Council of the European Union

Brussels, 9 December 2021
(OR. en)

Interinstitutional File: 2021/0411(COD)

14205/21
ADD 1

IXIM 260
ENFOPOL 460
JAI 1279
CODEC 1519
COMIX 576
IA 202

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	9 December 2021
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2021) 374 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the document DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA

Delegations will find attached document SWD(2021) 374 final.

Encl.: SWD(2021) 374 final

EUROPEAN
COMMISSION

Brussels, 8.12.2021
SWD(2021) 374 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the document

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA

{COM(2021) 782 final} - {SEC(2021) 420 final} - {SWD(2021) 377 final}

Table of contents

GLOSSARY

Term or acronym	*Meaning or definition*
CCWP	Customs Cooperation Working Party
CEA	Cost-Effectiveness Analysis
CISA	Convention Implementing the Schengen Agreement
CMS	Case Management System
EBCGA	European Border and Coast Guard Agency (Frontex)
EDPS	European Data Protection Supervisor
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EU	European Union
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
Europol	European Police Office
FL	Fuzzy Logic
FRA	Fundamental Rights Agency
JHA	Justice & Home Affairs
LEAs	Law Enforcement Authorities
LEWP	Law Enforcement Working Party
Naples II Convention	Convention on mutual assistance and cooperation between customs administrations
OCG	Organised Criminal Group(s)
OLAF	European Anti-Fraud Office
PCCC	Police and Customs Cooperation Centres
SAC	Schengen Associated Countries
SOC	Serious and Organised Crime
SFD	Swedish Framework Decision
SIENA	Secure Information Exchange Network Application
SIRENE	Supplementary Information Request at the National Entries
SPOC	Single Points of Contact
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

1. 1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

1.1. Background

Security and cross-border crime are, by definition, international issues. As set out in the EU Security Union Strategy, Europe faces **evolving and increasingly complex security threats**. These threats spread across borders and manifest themselves in organised crime groups that engage in a wide range of criminal activities. According to the EU Serious and Organised Crime Threat Assessment 2021 (SOCTA), more than 70% of organised crime groups are present in more than three Member States[1]. The 2021 SOCTA and the EMCDDA European Drug report[2] outline a number of areas where serious and organised crime appears to be on the rise[3]. At the same time, as set out in the December 2020 Counter-Terrorism Agenda, the EU remains on high terrorist alert[4].

The SOCTA also outlines ways in which serious crime is evolving. Notably, **technological advancements have created opportunities for new types of cross-border crime**, and for modernising traditional forms of crime. Linked to this, the increased use of digital technologies means there is no longer a need for a perpetrator to be in the same location as a victim. The Covid-19 pandemic has accelerated the rise in technology-facilitated serious and organised crime.

The **growing mobility of people within the EU** creates additional challenges in preventing and fighting all forms of criminal threats. In 2017, EU internal border regions covered approximately 40% of the EU's territory and were home to 30% of the population, i.e. 150 million people. Almost 2 million people commuted across borders, including 1.3 million cross-border workers[5]. In 2018, residents of the EU made in total 1.1 billion trips, either for business or privately – an increase of 11% since 2014. In 2019, 3.3% of the EU citizens of working age (20-64) had a nationality of an EU Member State other than the EU Member State of residence, compared to 2.4 % in 2009[6]. Despite the COVID-19 pandemic having reduced intra-EU mobility, flows of people will likely continue to be important in the near future.

The rapidly evolving criminal and terrorist landscape and the mobility of people suggest that **cross-border cooperation between law enforcement authorities in the EU and the Schengen area will remain crucial to tackle criminal offences**, and allow EU citizens to safely enjoy their rights of free movement in the future[7]. However, there are still obstacles for data exchange between law enforcement, which leads to blind spots and loopholes (for instance information not exchanged or exchanged too late) for criminals and terrorists that act in more than one Member State. The cross-border nature of crime requires Member States to be able to rely on one another through cross-border law enforcement cooperation, based on respect for fundamental rights.

Law enforcement cooperation is an area of shared competence between the EU and the Member States. Most of the EU legal framework underpinning law enforcement cooperation was designed 30 years ago through the 1990 Convention Implementing the Schengen Agreement

[1] Europol (2021) *Serious and Organised Crime Threat Assessment (SOCTA): A corrupting influence*.
[2] European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), *European drug report 2021 – trends and developments.*
[3] For example, the use of violence by criminals involved in serious and organised crime appears to be increasing; unprecedented quantities of cocaine are trafficked into the EU from Latin America and criminal groups are scaling up their capacities to produce and distribute synthetic drugs.
[4] COM(2020) 795 final.
[5] European Commission (2017), *Boosting Growth and cohesion in EU border regions*. link.
[6] Eurostat (2020) *EU citizens living in another Member State - statistical overview.* As of 8 April 2021: link.
[7] Complementary information can be found in annex 4.

(CISA)[8]. The Convention entails a number of obligations for contracting Parties regarding police cooperation at their common internal borders, at the external borders of the Schengen territory (land, international airports, and sea) and within the Schengen area in general to counteract any security deficit caused by the abolition of the checks at the internal borders.

The Commission and EU agencies support the Member States by providing means and tools for the exchange of information between national law enforcement authorities, such as the Schengen Information System (SIS), *inter alia* used to exchange data on wanted and missing persons and objects in real time, and the Prüm mechanism, aimed to step up the exchange of biometric and vehicle registration data information, between authorities responsible for the prevention and investigation of criminal offences.

The 2006 Swedish Framework Decision (SFD) complements these tools by introducing horizontal rules on the exchange of information between law enforcement authorities of EU Member States to conduct criminal investigations or criminal intelligence operations. The SFD sets out rules regarding time limits and standard forms for the exchange of any type of information or data held by law enforcement authorities (**principle of availability**), on prior request or spontaneously, ensuring that procedures for cross-border data exchanges are not stricter than those applying to exchanges at national level (**principle of equivalent access**). It also covers the channels of communication to be used. A response should be made within 8 hours where the request is urgent. In other cases, countries should respond within 14 days.

Europol, the EU law enforcement agency, supports EU Member States in their fight against terrorism, cybercrime and other serious and organised forms of crime, notably through the collection, analysis and exchange of information with Member States.

The **EU has also fostered greater cooperation between law enforcement bodies through the publication of recommendations and guidelines** (e.g. on national Single Point of Contact responsible for law enforcement exchange of information). Those seek to lay out the grounds for adopting common approaches to the access and the exchange of information within the EU. They also seek to clarify the implementation of binding rules[9].

1.2. Recent developments

In recent years, much progress has been made to improve the exchange of information between Member States and to close down the space in which terrorists and criminals operate.

The legislative framework on counterterrorism and information exchange was strengthened in the aftermath of the terrorist attacks in Europe. Following the migration crisis of 2015, the general architecture of Justice and Home Affairs (JHA) information systems and databases was overhauled with a focus on interoperability and dynamic convergence between security, borders and migration management. The mandates of JHA agencies are continuously being strengthened to allow them to provide enhanced support to Member States in their operational activities.[10]

Strategic documents underpin the Commission's efforts to improve the efficiency and effectiveness of law enforcement cooperation in the EU. These include the **Security Union strategy**[11], the new **counter-terrorism agenda** for the EU[12], the **EU Strategy to tackle Organised Crime 2021-2025**[13] and the new **Schengen Strategy**[14]. All stress the need to improve the timely access and

[8] It has been further complemented by a high number of bi-tri-multilateral agreements (60 were identified).
[9] Complementary information can be found in annex 5.
[10] In December 2020, the Commission tabled a legislative proposal to strengthen the mandate of Europol (COM(2020) 796 final). The mandate of the European Border and Coast Guard Agency was reinforced in November 2019 (see Regulation (EU) 2019/1896).
[11] COM(2020) 605 final.
[12] COM(2020) 795 final.
[13] COM(2021) 170 final.

smooth exchange of information for law enforcement purposes, both between Member States and with Schengen Associated Countries (SAC).

In spite of the progress made in recent years, important challenges remain, a very pressing one among these being that law enforcement authorities do not always effectively and efficiently exchange information with their partners in other Member States.

The **co-legislators have repeatedly called for further EU action** to address these challenges. The European Parliament resolution ofDecember 2020 on the EU Security Union Strategy stresses that "*measures in the framework of the Security Union Strategy must be sufficiently flexible to respond to constantly changing circumstances and criminal organisations changing their modus operandi*". The Council takes a comparable stance in the Council Conclusions of November 2020 on Internal Security and European Police Partnership, which asked the Commission "*to consider consolidating the EU legal framework to further strengthen cross-border law enforcement cooperation*"[15].

1.3. The Police Cooperation Code

In line with the call by President von der Leyen in her Political Guidelines[16] to "*leave no stone unturned when it comes to protecting our citizens*", the Commission Work Programme for 2021 announced a legislative initiative to "*modernise existing intra-EU law enforcement cooperation by creating an EU police cooperation code*"[17].

A proposal for setting up a **Police Cooperation Code on Information Exchange and Communication (PCC)** would aim at the codification of organisational and procedural aspects of information exchange and communication between law enforcement authorities in the EU.

It would deal with the cross-cutting 'horizontal' aspects of information exchange between Member States. This proposal would not touch upon the system-specific dimensions of individual systems or frameworks such as the Schengen Information System, Passenger Name Record (PNR) or Prüm**,** which address the processing of specific data categories for specific purposes and are therefore regulated by specific legal instruments.

The proposal for a PCC would **repeal and replace** the 2006 SFD. In doing so, the SFD will be "lisbonised", i.e. it will be turned into a legislative instrument to be adopted by both the Council and the European Parliament in the ordinary legislative procedure.

Moreover, a PCC proposal would form part of a **coherent package** with upcoming measures to reinforce **operational cross-border police cooperation** and the upcoming proposal revising the Automated Data Exchange Mechanism for Police Cooperation **("Prüm II")**. The "Prüm II" proposal will aim at strengthening the technical architecture of the Prüm exchange, broadening its scope of data categories and streamlining and accelarating its post-hit data exchange. The reinforced "Prüm II" proposal would provide specific rules and possibilities for the **automated** exchange of specific – and particularly important – data categories (e.g. fingerprints, DNA, facial images) within the overall framework and general rules for general information exchange that the Police Cooperation Code will provide.

A PCC proposal would fit together with the 2020 proposal revising the **Europol** mandate[18]. The latter aims at strenghening the agency's mandate on the processing of large and complex datasets, cooperation with privates parties, and the use of the Schengen Information System. A PCC proposal would build on and further develop Europol as a criminal information hub in the EU.

---

[14] COM(2021) 277 final.

[15] European Parliament resolution of 17.12.2020 on the EU Security Union Strategy (2020/2791(RSP)) and Council Conclusions 13083/1/20 REV 1, 24.11.2020 on *Internal Security and European Police Partnership*.

[16] Political Guidelines: https://ec.europa.eu/info/sites/info/files/political-guidelines-next-commission_en_0.pdf

[17] COM(2020) 690 final.

[18] COM(2020) 796 final.

As an important measure to enhance security within the EU, a PCC proposal would also contribute to a fully functioning and resilient **Schengen** area as set out in the Schengen Strategy. It would help ensure a high level of security within the territory of Member States and hence support a Schengen area without controls at internal borders. It would therefore complement the proposal announced in the June 2021 Schengen Strategy[19] to amend the Schengen Borders Code[20].

Whilst taking these complementary developments fully into account, this impact assessment focuses on the envisaged scope of a proposal for a Police Cooperation Code, namely **the 'horizontal' cross-cutting aspects of information exchange and communication between competent law enforcement authorities in EU Member States.**

[19] COM(2021) 277 final.
[20] Regulation (EU) 2017/458.

Intervention logic: Problems, problem drivers, objectives and options

High level problem: *A number of criminal markets are evolving and expanding while cross-border mobility is increasing*[21].

Core problem: *Law enforcement authorities do not always effectively and efficiently exchange information with their partners in other Member States.*

	Problems	Drivers	Objectives	Options
1	**Rules at national level impede the effective and efficient flow of information:** The **2006 Swedish Framework Decision is not fully implemented,** preventing law enforcement authorities from other Member States from receiving such information in an effective and efficient way.	• Law enforcement authorities do not fully apply the principles agreed under the 2006 Swedish Framework Decision. • There is no clear understanding of the data available for possible exchange from another Member State. • Deadlines are usually not met when a judicial authorisation is required to deliver the requested information. • The distinction between "urgent", "non-urgent" and "other cases" provided for in the Swedish Framework Decision is unnecessarily complex. • The Swedish Framework Decision is not aligned with the 2016 Law Enforcement Data Protection Directive.	To facilitate **equivalent access for law enforcement authorities** to information held in another Member State (similar to the access granted to information within a Member State), while complying with fundamental rights and data protection requirements.	• *Option 1.1*: N**ew flanking soft measures** (training, Commission guidance) • *Option 1.2:* Option 1.1 + **simplify the SFD use + improve clarity on the national data sets available for possible exchange** with law enforcement authorities of other Member States; • *Option 1.3:* Option 1.2 + provisions ensuring compliance with **deadlines** requirements by which data is to be made available to another Member State (including when a judicial authorisation is required).
2	**Structures at national level are not set up and equipped in a sufficiently efficient and effective manner:** Member States do **not always have the necessary structures** in place to exchange information effectively and efficiently with other Member States: Member States do not have the necessary structures in place to receive information requests from other Member States, channel them to the right authorities at national level, and provide the requested information in an effective and efficient way.	• Single Points of Contact (SPOCs), Police and Customs Cooperation Centres and other equivalent structures are set up differently, having different supervising authorities, roles, means and capabilities. • They are not always structured or manned appropriately, nor equipped with necessary information management tools. • There are delays in the judicial authorisation process in cases where this is needed. • Language barriers hamper the efficient cross-border exchange of information. • Limited training available for staff involved in information exchange and cooperation.	To ensure that all Member States have an effective functioning **Single Point of Contact** (SPOC), including when a **judicial authorisation** is required to provide the data upon request of another Member State, and ensuring its effective cooperation with **Police and Customs Cooperation Centres** (PCCCs).	• *Option 2.1:* Continue with Council non-binding guidelines on Single Points of Contact + **new flanking soft measures** (training, financial support, Commission guidance); • *Option 2.2:* **approximation of minimum standards** on the composition of the Single Points of Contact (including when a **judicial authorisation** is required), its functions, staffing and IT systems, and its cooperation with regional structures such as Police and Customs Cooperation Centres + flanking soft measures (as in option 2.1); • *Option 2.3:* **harmonisation of rules** on the composition of the Single Points of Contact (including when a **judicial authorisation** is required), its functions, staffing and IT systems, and its cooperation with regional structures such as Police and Customs Cooperation Centres + flanking soft measures (as in option 2.1).

[21] Complementary information on high level issues and their links with the core problems can be found in annex 4.

3	**The free choice of communication channel(s) between Member States causes recurrent duplication of requests:** Member States' law enforcement authorities use a variety of different channels to send information request to other Member States and respond to them, which hampers effective and efficient exchange of information.	Member States have not agreed on a single channel of information exchange between their law enforcement authorities for cases with an EU dimension, leading to duplication of requests, undue delays and occasional information loss, and also depriving their competent authorities from Europol's support even though they call on the Agency to be the EU criminal information hub and to deliver intelligence-led products.	To **remedy the proliferation of communication channels** used for law enforcement information exchange between Member States **while empowering Europol** as the EU criminal information hub for offences falling within its mandate (unless otherwise regulated by EU law).	• *Option 3.1:* Continue with Council non-binding guidelines and Recommendations to put Europol in copy when using SIENA[22] in cases within Europol' mandate + new **flanking soft measures** (training, financial support); • *Option 3.2:* Obligation to **use SIENA as preferred communication channel** + obligation to put Europol in copy when using SIENA in cases within Europol's mandate + flanking soft measures (as in option 3.1) • *Option 3.3:* **obligation to use SIENA by default for all bilateral information exchange** (unless otherwise regulated by EU law) + obligation to put Europol in copy when in cases within Europol's mandate, both after the end of a **transition period and with Internal Security Fund support for the SIENA roll-out** + flanking soft measures (as in option 3.1)

[22] Europol's "Secure Information Exchange Network Application".

2. 2. PROBLEM DEFINITION

The evolution of the EU security landscape and the increased cross-border mobility call for more effective and efficient exchange of information between Member States. Noted inefficiencies stem from three vertical problems.

2.1. Problem 1: Rules at national level impede the effective and efficient flow of information

2.1.1. 2.1.1. What is the problem?

Member States' Law Enforcement Authorities (LEAs) are involved in daily cross-border information exchanges related to operations against criminal offences[23].

Yet, rules at national level impede the effective and efficient flow of information. While EU measures are supposed to ensure access to information, their scope is often unclear and law enforcement authorities face difficulties in interpreting and implementing relevant EU provisions. As a case in point, the 2006 Swedish Framework Decision is found unclear and complex, thereby hampering the full implementation of the principles of availability/equivalent access of relevant information in a cross-border context[24]. As a consequence, the Framework Decision is not fully implemented and rules at national level continue to impede the flow of information.

Council Framework Decision 2006/960/JHA ('Swedish Framework Decision' - SFD)[25]

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

- preventing, detecting and investigating offences or criminal activities which correspond to or are equivalent to those referred to in the European arrest warrant, or
- preventing an immediate and serious threat to public security. The designated authorities are obliged to reply within at most eight hours in urgent cases, as long as the requested information or intelligence is directly accessible to law enforcement authorities.

Information may not be provided if:

- national security is at stake,
- current investigations may be jeopardised,
- the request pertains to an offence punishable by a term of imprisonment of one year or less under the law of the requested Member State,
- the competent judicial authority withholds access to the information.

[23] Survey: Q 31, 83% (n=53) of LEAs respondents reported information sharing took place always or very frequently in relation to drugs, 73% (n=38) in relation to illegal immigration and 68% in relation to both terrorism (n=26) and cybercrime (n=34). See Annexes 2, 6 & 9 .

[24] The SFD has been regularly and thoroughly monitored and evaluated as part of the Schengen evaluation and monitoring process carried out for the past 6 years in field of police cooperation. The Schengen evaluation and monitoring process consist of questionnaires and one-week on-site visits (announced or unannounced) by an expert team involving national experts from other Member States, Commission representatives and experts from EU Agencies. The evaluation team inquires into the practical application of the SFD by national police authorities in their daily work, e.g. how the national police authorities request information from other Member States, and how they respond to such requests that they receive from other Member States. The evaluation team can directly address relevant persons and has access to all areas, premises and documents required for the evaluation. All Schengen countries have been evaluated from 2015 to 2019 (26 countries). A new evaluation cycle started in 2020 (starting with countries evaluated in 2015). Over 30 evaluations have thus been carried out in field of police cooperation over the past 6 years. The country reports drawn up following each evaluation analyses the qualitative, quantitative, operational, administrative and organisational aspects and list any deficiencies identified during the evaluation. The country reports offer sound and first-hand information on the application of the SFD in the Member States, making the SFD one of the best evaluated policies in the justice and home affairs domain, and providing a very solid knowledge base for evidence-based law-making.

[25] 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, OJ L 386/89, 29.12.2006.

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

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

The content of these categories depends on national legislations. The type of information available from each Member State is set out in national sheets (Council guidelines)[26]. Data is to be shared with Europol insofar as the information or intelligence exchanged refers to an offence or criminal activity within the Europol mandate. Information and intelligence will be processed in accordance with the relevant Europol handling codes. SIENA, (Europol's Secure Information Exchange Network Application) supports the exchange of information in accordance with the 'Swedish Framework Decision'.

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

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

The requesting Member State may choose between any of the existing channels for international law enforcement communication (SIRENE[27], Europol, INTERPOL, bilateral contact points). The replying Member State normally uses the same channel as used for the request. If, however, the requested Member State replies, for legitimate reasons, through another channel, the requesting authority is informed of this change. The language used for the request and supply of information shall be the one applicable for the channel used.

2.1.2. 2.1.2. What are the problem drivers?

As indicated above, at EU level, the principles for the exchange of law enforcement information and intelligence of cross-border relevance are laid down in the 2006 Swedish Framework Decision, notably through its two key principles of availability and equivalent access.

This means that:

- a law enforcement officer in one Member State in need of information and intelligence in order to carry out his duties can obtain it from another Member State; and that
- the law enforcement authorities in the Member State that holds this information and intelligence will make it available for the declared purpose, taking account of the needs of investigations pending in that Member State; and that
- once information and intelligence is available in a Member State, it should be shared across borders under the same conditions which govern information sharing at national level, meaning that the rules applied in a cross-border case **are not stricter** than those applying to data exchanges at national level ("principle of equivalent access")[28].

In practice, as evidenced in the Schengen evaluations in the field of police cooperation, ***the Swedish framework Decision is hardly used***, as the availability of many options for cooperation or information exchange limits its added value, and it overlaps with the Convention Implementing the Schengen Agreement (CISA), with many articles worded in a similar way[29]. The envisaged proposal will address this discrepancy by expanding the scope of the SFD to "*preventing and detecting criminal offences*", thereby fully superseding Articles 39 and 46 CISA and hence providing the necessary legal clarity.

[26] Council document 5825/20 ADD 1 REV 1, 2.12.2020, *Manual on Law Enforcement Information Exchange*.

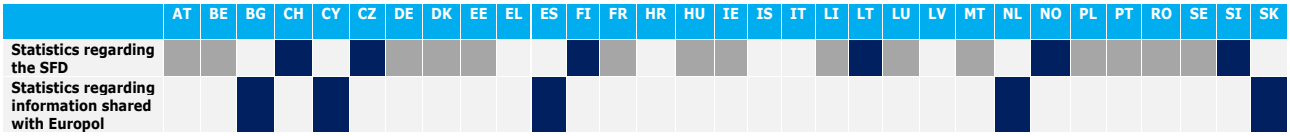
[27] Supplementary Information REquest at the National Entry.

[28] See Council document 6261/17, 4 July 2017, *ibidem* p. 31.

[29] A number of Member States indicated that the different scope of the SFD and the CISA (respectively "conducting criminal intelligence operations" and "preventing and detecting criminal offences") makes it unclear if and to what extent the CISA (Art. 39 and 46) is still applicable, despite that the SFD was expected to replace the CISA as the key legal basis for information sharing relevant to law enforcement cooperation. This results in a limited contribution of the SFD towards simplification and streamlining of the EU framework. They also questioned the need to have two pieces of legislation (the SFD and the CISA) instead of just one piece of legislation with a broader and more comprehensive scope. 7 Schengen evaluation reports.

The quantification of information exchange and its breakdown per communication channel was not possible for lack of national and comparable data. Indeed, 17 countries have reported not to produce complete and comparable statistics regarding the information requests exchanged pursuant to the SFD, while seven indicated to keep statistics and five to do so only for information shared with Europol[30].

Collection of statistics concerning information exchange



**Blue cells: statistics are collected. Grey cells: no data available*

Source: EY/RAND Study' elaboration based on desk research

Deadlines are usually not met when a judicial authorisation is required to deliver the requested information.

Indeed, the more authorities are concerned, the more procedural steps have to be followed, hence the need for additional time to cope with all procedures[31]. Representatives from national judicial authorities have pointed out that the EU legal bases for information exchange in law enforcement cooperation is complex, creating burdensome, laborious and unclear processes to be followed[32].

This issue is further exacerbated by the fact that what is regarded as an information request for police officers in one country might be regarded as an information request for judicial authorities in another country, depending on the rules at national level. Hence, different authorities may be concerned depending on the specific national institutional framework, further undermining the overall efficiency of the process[33]. Furthermore, there is no obligation to have a judicial authority functionally available 24/7 within the national Single Point of Contact (SPOC – national information hub centralising the reception, processing and the sending of the information – in and out), thereby slowing down the judicial authorisation process, where it is needed.

The distinction between "urgent", "non-urgent" and "all other" cases provided for in the SFD and the SFD forms to be used (on a voluntary basis) for information exchange is unclear and (unnecessarily) complex.

The SFD does not define "urgent cases", "non- urgent cases" and "all other cases", which are deductively identified as those not fitting the "urgency criteria". Such a deductive process takes time. Some guidance on the possible understanding of "urgency" is offered by Council (non-binding) guidelines[34], which, however, has not led to a convergence of national practices.

Moreover, **the forms for submitting and requesting information** included in the SFD are rarely used[35]. They are considered time-consuming and labour intensive, and the Member States prefer free-text messages[36]. Hence, although the SFD forms were expected to boost a standardised and efficient exchange of information, their limited use results in a limited harmonisation of communication procedures.

[30] Council Document 14755/1/12, *Swedish Framework Decision (SFD) implementation – Assessment of compliance pursuant to Article 1(2)*.
[31] Council Document 14755/1/12.
[32] Survey: Q 15, 3 national judicial authorities' representatives.
[33] Huybreghts, G. (2015), *The Schengen Convention and the Schengen acquis: 25 years of evolution*. ERA Forum.
[34] Council Document 9512/1/10, REV 1, 17.12.2010, *Guidelines on the implementation of Council Framework Decision 2006/960/JHA of 18 December 2006*.
[35] 15 Schengen evaluation reports. Technical workshop held on 24 March.
[36] Council Document 14755/1/12, *Swedish Framework decision (SFD) implementation - Assessment of compliance pursuant to Article 11(2)*. Available at: link. Technical workshop held on 24 March 2021.

The Swedish Framework Decision is not aligned with the 2016 Law Enforcement Data Protection Directive.

The exchange of personal data pursuant to the SFD is not aligned with the 2016 Law Enforcement Data Protection Directive (LED)[37]. Indeed, Article 8 SFD states that the use of the information and intelligence exchanged must be subject to the national data protection provisions of the Member State receiving the information, according to the same rules as if they had been gathered in that Member State.

Moreover, when providing information and intelligence, the competent law enforcement authority may impose additional conditions that are in accordance with its national law on their use by the receiving competent law enforcement authority. The Commission committed to "*make a legislative proposal, which as a minimum will entail an amendment of Council Framework Decision 2006/960/JHA to ensure the necessary data protection alignment, in the last quarter of 2021*"[38].

In practice, law enforcement authorities do not have a clear understanding of the data available for possible exchange with their counterparts in other Member States.

The content of these data depends on national legislations. The type of information available from each Member State is set out in national fact sheets (compiled in Council guidelines)[39]. Yet, the awareness of these national fact sheets remains limited. This results in unnecessary wide requests leading to lengthy processing time. In other instances, data that would have been needed is not included in the exchange while unnecessary one is provided.

2.1.3. 2.1.3. How will the problem evolve without intervention?

Member States alone would not be able to ensure the full implementation of the principles of availability and equivalent access to information. This means that the current uncertainties with regard to the applicable legislation and the data available for possible exchange between the Member States would remain and continue to negatively affect the effective and efficient sharing of information, thereby leaving the impacts in the evolution of the EU security landscape and in the increased cross-border mobility essentially unaddressed. In practice, there would continue to be a lack of clarity on what data are available in different Member States. The respect of deadlines for urgent information requests would remain unlikely when a judicial authorisation is required. The distinction between urgent and non-urgent cases/all other cases, and the forms to be used for information exchange will remain (unnecessarily) complex.

Without intervention, the 2006 Swedish Framework Decision will remain unaligned with the 2016 Law Enforcement Data Protection Directive (LED). This means that even though Fundamental Rights would remain adequately safeguarded, improvement would not be brought forward.

2.2. Problem 2: Structures at national level are not set up and equipped in a sufficiently efficient and effective manner

2.2.1. 2.2.1. What is the problem?

Member States do not always have the necessary structures in place to exchange information effectively and efficiently with other Member States. Where Single Point Of Contacts (SPOCs), Police and Customs Cooperation Centres (PCCCs) and other equivalent structures at national level

[37] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences and on the free movement of such data.

[38] COM(2020)262, *Way forward on aligning the former third pillar acquis with data protection rules.*

[39] Council document 5825/20 ADD 1 REV 1, 2.12.2020, *Manual on Law Enforcement Information Exchange.*

exist they do not always play their coordination role and lack resources to face the increasing number of requests.

Notably, SPOCs, PCCCs and other equivalent structures often have outdated IT infrastructure. They are not always equipped with the necessary information management tools (e.g. a case management system with a common dashboard and automatic data upload and cross-check).

National and regional information hubs (SPOC and PCCC)

Nearly all Member States have implemented the policy of channeling as much information exchange as possible through a single point of contact. The Single Point of Contact (SPOC) is the national "one-stop shop" for international law enforcement cooperation, gathering under the same management structure all main international law enforcement communication channels (INTERPOL, Europol and SIRENE[40]). Such innovation was introduced as an attempt to reconcile Member States' fragmented law enforcement authorities' landscape with the growing need to jointly tackle cross-border threats of shared competence (e.g. drug trafficking). At the nexus of cross-border information exchange and national coordination between different law enforcement authorities, the SPOC concept greatly facilitates information flows.

The understanding of what defines a SPOC varies among the Member States. The 2014 Council (non-binding) draft guidelines tentatively indicate how SPOCs can be structured to maximise the use of resources, avoid overlaps and make cooperation with other Member States more efficient, expedient and transparent[41]. From these guidelines, Member States should select the solution appropriate for their situation in view of the common and agreed aim of enhancing international cooperation, and consider appropriate ways of informing other Member States about the solution selected with a view to the exchange of best practices. This Council non-binding guidance has not led to a sufficient convergence of national practices.

Information (mostly concerning petty crimes) is notably exchanged through Police and Customs Cooperation Centres (PCCC), set up in border regions between two to four European countries, thus alleviating the national SPOC from an overflow of requests. 59 PCCCs have been set up across most Member States and Schengen Associated Countries. Similar duties are ensured by other equivalent bodies, such as police (only) cooperation centres or police and border guards cooperation centres. These PCCCs (regional information hub) are not always under the umbrella of the national SPOC, preventing the SPOC from having a full picture of information exchanged and preventing possible links.

2.2.2. 2.2.2. What are the problems drivers?

SPOC do not always play their coordination role and lack resources to face the increasing number of information requests.

Member States are free to decide which law enforcement authorities and services are represented within their SPOCs[42]. Although different manuals and national factsheets have been produced in order to facilitate a harmonised approach to the way national SPOCs are organised[43], there are still significant differences across countries as regards the structures at national level[44].

For example, in some countries the SPOC includes the Europol National Unit (ENU), the Supplementary Information Request at the National Entry (SIRENE) bureau and the INTERPOL National Central Bureau, while in other countries these units are not included. Such differences lead to confusion when it comes to the cross-border exchange of information.

[40] Each state operating the Schengen Information System (SIS) has set up a national SIRENE Bureau, operational 24/7, that is responsible for any supplementary information exchange connected to SIS alerts.

[41] Council document 10492/14, *Draft Guidelines for a SPOC for international law enforcement information exchange.*

[42]7 Schengen evaluation reports. Technical workshop held on 24 March 2021.

[43] Council Document 10492/14; Council Document 12093/19, *Draft Council Conclusions on establishing a 'Heads of SPOC' network*; Council Document 5825/20 ADD 1 REV 1, *Manual on Law Enforcement Information Exchange*.

[44] At the time of their Schengen evaluations (carried out between 2016 and 2019), 3 countries were not considered to have a SPOC in place, while, in one, the SPOC was still not operational. Some of the countries consider the SPOC to be the front-office, others see it as the entire structure comprising the three main international police communication channels (INTERPOL, Europol and SIRENE). Such a structure may also contain other strategic or support services. Whereas one country reported that its SPOC was run by a staff of 7, another country indicated that its SPOC was run by 287 persons (they are also acute differences between similar size countries showcasing the diversity of Member States approaches and the related efficiency of their IT architecture).

Thus, when a request for information is addressed to a specific Law Enforcement Authority (LEA) or a dedicated service within a LEA, the requesting Member State does not know in advance whether this entity is included or not within the SPOC of the receiving Member State. This leads to a risk of duplication of requests, which are sent both to the SPOC and to the specific service. Moreover, SPOCs face a high workload notably due to the practice of "fishing" and difficulties in the choice of the most appropriate communication channels to be used to exchange information[45].

Additionally, the SPOCs – and in some cases also the PCCCs[46] – lack resources to timely and effectively address the increasing number of requests they receive[47]. The increasing amount of information requests has not been accompanied by a proportionate increase of the resources allocated to manage these requests[48]. The lack of sufficient resources allocated to the SPOCs is particularly challenging in cases of urgent requests for information[49].

Pursuant to Article 4 of the Swedish Framework Decision (SFD), urgent requests for information shall be addressed within 8 hours. This timeframe is not critical *per se* and it seems well suited to share information, which is necessary to carry out the investigation. However, if several urgent requests are received at the same time, enough officials would need to be available to manage them in parallel, and this is problematic since human resources within the SPOCs are limited. This is particularly challenging since the SFD does not envisage an automated tool for issuing reminders of the information requests.

Hence, timely responses depend on the SPOC's capacity to monitor and track the deadlines in the Case Management Systems[50]. There is often a lack of a modern information management architecture that would alleviate tensions on limited human resources.

SPOC's staff

	AT	BE	BG	CH	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK
SPOC staff		89						30			22	35			74		10	287	7	10		33	40						54	29	

**Blue cells: number of SPOC's staff. White cell: no data available. Grey cells: no Schengen evaluation report available.*
Source: EY/RAND study' elaboration based on Schengen evaluation reports

Examples found in Schengen evaluations in the field of police cooperation (2015-2019)

- In three countries, the total number of messages exchanged through all channels used by the SPOC has been increasing over the past years and was not mirrored by a comparable increase in the number of available staff, leading to challenges to cope with all requests for information;

- In one country, the human resources allocated to the national SPOC are deemed insufficient to properly address all requested exchanges of information;

- In one country, the number of SPOC staff has decreased recently despite a sizable increase in the number of messages exchanged.

Information from (i) different units within the SPOCs and (ii) from the PCCCs (and equivalent structures in the border area) is not always integrated in the SPOC information management system.

[45] Fishing means that one or several Member State' law enforcement agencies may receive the same information request via several channels without any clear link to a specific case (catch all fishing request), thus leading to duplication of work. Technical workshop held on 24 March.

[46] Council document 14623/17, 27.11.2017 - *Information Management Strategy (IMS): action list No 5 and proposal for action list No 6 - State of play of "PCCC: European dimension" (Action No 7).*

[47]5 Schengen evaluation reports. ICMPD (2010) Study on the status of information exchange amongst LEAs in the context of existing EU instruments. Available at: link.

[48] Comparative analysis of the Schengen evaluation reports. See complementary information in annex 5.

[49] 5 Schengen evaluation reports. Technical workshop held on 24 March 2021.

[50] Survey: Q 41, 69% (n=99) of LEAs respondents reported that differences between countries in the capacity to regularly monitor the different communication channels (e.g. SIENA, SIS/SIRENE, EIS and INTERPOL) as well as in the response time to requests sent via these platforms hamper cross-border law enforcement cooperation.

In some Member States there is **no integration of information** included in databases owned by the different law enforcement authorities, which form part of the same SPOC and/or the PCCC. The lack of integration of information collected and stored by different law enforcement authorities results in a risk of duplications of both uploads and searches of information, hence reducing the overall efficiency of information exchange[51].

Direct and user-friendly access to all relevant EU and international databases and platforms is not the norm in the SPOCs and the PCCCs. The specific national law enforcement authorities (LEAs) entitled to access and use EU and international databases and platforms vary between the Member States.

An additional issue hampering a smooth cross-border exchange of information is that the SPOCs and the PCCCs do **not** always **have direct** and user-friendly **access to all relevant EU and international databases and platforms**, limiting their capacity to effectively support cross-border exchange of information[52], thus hampering cross-border law enforcement cooperation[53]. As regards the PCCCs, out of 59 PCCCs active in Europe, only 14 are connected to Europol SIENA[54]. Besides the PCCCs, this consideration also applies to regional and local level law enforcement authority investigation departments that most of the times do not have access to SIENA[55].

Examples found in Schengen evaluations in the field of police cooperation (2015-2019)

- One country reported that the customs Liaison Official at Europol is the only national customs staff granted with direct access to the Europol Information System;
- One country reported to have no Case Management System (CMS) in place at the international police in the unit responsible for all matters relating to international police cooperation and communication within the police;
- In one country, national LEAs do not have direct access to the national identity document registry;
- In one country**,** the national police database is not linked to the national case management system;
- In one country, the search criteria for the national police database do not fully mirror those for accessing the data included in the SIS II database. For this reason, officials have difficulties to retrieve information from the different databases, especially when they lack specific information such as the passport nationality or document type, which may be required by one information system and not by the other;
- In one country**,** each national police force has its own database which is not accessible to and interoperable with databases used by other police forces: in order to check whether a person or object has been registered in a specific database, officials from each agency have to perform separate searches in their corresponding databases, each accessible from different workstations. Hence, the risk of waste of time and duplication of information and related searches;
- In one country, incoming requests for information are managed by the international police, which consists of different units, each having its own case management system. When the request is received, the overarching unit forwards it to the different units; this double-step process takes time, and this could represent a hurdle in the case of urgent requests;
- Similar issues are reported also in another two countries, where manual double-checking by officials is performed to avoid duplications of information and requests;
- Moreover, duplications are particularly challenging where, like in one country, there are no available electronic means for automatically identifying cases of duplications of information between the workflow systems;

[51] 9 Schengen evaluation reports. Interviews: 11 representatives from four EU bodies. European Confederation of Police (EuroCOP) supporting Commission's initiative to streamline and consolidate existing instruments for cross-border police cooperation (2020). Survey: Q 29, 34% (n=38) of LEAs respondents pointed out that the lack of coordination between SPOCs and PCCCs hampers law enforcement cooperation.

[52] 21 Schengen evaluation reports. Survey: Q 44, 71% (n=101) of LEA respondents reported that access to SIENA, SIRENE, EIS, and INTERPOL exchange channels and databases differs between countries to a moderate, high degree, or very high degree.

[53] Survey: Q 41, Survey: Q 41, 71% (n=101) of LEAs that responded to the online survey reported that the different tools for which the access to SIENA, SIS/SIRENE and INTERPOL exchange channels and databases is regulated between countries hamper cross-border law enforcement cooperation through the platforms listed above from a moderate to a very high degree.

[54] Council document 14629/17, *State of play of the roll-out of SIENA regarding PCCCs - Outcome of questionnaire*.

[55] 17 Schengen evaluation reports. Interviews: 2 EU Agency representatives. 4 Member States' representatives at the Technical Workshop held on 24 March 2021.

- In one country, requests and messages received through i24/7, SIS, SIRENE and SIENA are entered into the SPOC's case management system. However, the information included in the messages is not automatically cross-checked against the national databases and this means that the checks have to be performed manually;
- In one country, limited interoperability is further exacerbated by the fact that international information exchanges at the local or regional levels are not systematically reported to the SPOC undermining its coordination role.

National LEAs have limited awareness and knowledge of relevant databases.

Cross-border information sharing is further hampered by the **national LEAs' limited awareness** and knowledge of **relevant databases**. Notably, the majority of Member States reported that national LEAs' officials are not completely aware of all the law enforcement databases available to them or they are not sufficiently experienced and proficient in their use[56].

The SPOCs often face IT capacity issues when dealing with the increasing requests for urgent information.

This is further challenged by the fact that the SPOCs and the PCCCs are **not** always **equipped with the necessary information management tools**, preventing an efficient tracking/filing of information in cross-border cases[57].

For instance, some SPOCs have limited access to relevant national databases[58]. Since they cannot access directly the databases of other law enforcement authorities, they need to ask officials within those authorities to collect and share the information. This delays the overall exchange process[59]. Difficulties related to the steps needed for the SPOCs to obtain the relevant information included in national databases are further exacerbated by the actual limited interconnectivity between national law enforcement databases[60].

Main features of SPOC's Case Management System

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK
Model	A	D		B	E	A	D	E	A	A	E	C	D	D						D	B	A	D		E		B	E	C	
CMS in place	Yes	Yes			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes		Yes	Yes		Yes	Yes	Yes
CMS linked with LEAs	No				No		Yes		No		No	No	Yes	No		Yes	Yes		Yes	Yes	Yes	No	No			No		No	Yes	Yes
CMS linked with PCCC	No	No			Yes		Yes		No		No	No	No	No			Yes			No			No		No	No			Yes	Yes
CMS linked with SIRENE II					Yes		Yes		No	Yes	No		Yes	Yes		No	Yes		Yes		Yes	No	No		Yes	Yes		Yes	Yes	Yes
CMS linked with Interpol					Yes		Yes		No	Yes	No		Yes				Yes		Yes		Yes	No	No		Yes	No		Yes	Yes	Yes
CMS linked with Europol					No		Yes	No	No		No		Yes	No		No	Yes		Yes		Yes	No	No		Yes	No		No	Yes	No
Cross-check functions					No				No		No	No		Yes		No	Yes		Yes	No	No		No		No				No	Yes
Automatic upload														No					Yes											Yes
Notification of deadlines						No		No	No		No	Yes					Yes		No			No	No		No	No				
Statistical functionality							No					No					Yes											No		

Source: EY/RAND Europe Study's elaboration based on desk research (dark grey cells indicate that no information is available)

The use of rudimentary search tools hampers the adoption of transliteration and "fuzzy logic" search.

[56] 24 Schengen evaluation reports. Technical workshop held on 24 March 2021.
[57] 10 Schengen evaluation reports.
[58] 5 Schengen evaluation reports. SWD/2020/327 final. Available at: link.
[59] Council Document 14755/1/12.
[60] 17 Schengen evaluation reports. Technical workshop held on 24 March 2021. Commission Staff Working Document SWD/2020/327 final. Available at: link.

Furthermore, the exploitation of the full potential of existing databases is hindered by the **use of rudimentary search tools,** which prevent the adoption of transliteration[61] techniques and "fuzzy logic"[62] search functions. The lack of transliteration and fuzzy logic search options within national databases and information systems prevents officials to get a full picture about the person they are looking for in the systems through a unique query. As a result, officials have to carry out a new search for each personal detail they are investigating, resulting in an increased workload, which slows down the search process (e.g. inversion of first and last name, different spelling used for the same individual notably stemming from different languages, alphabets and diacritic accents).

Examples found in Schengen evaluations in the field of police cooperation (2015-2019)

- In one country, a transliteration issue was identified when some letters were entered differently or in case some letters were left out at the end of the name, as the system was not able to find matches in the databases;
- In one country, issues were reported related to transliteration and fuzzy logic searches in the national application used for mobile access to police databases. In particular, when there is some uncertainty if a given word corresponds to the surname or name of a suspect, the system is not able to search both fields at the same time, which means that an official has to make the search twice;
- In one country, the same problem was identified with reference to the interconnection with SIS: due to the lack of fuzzy logic instruments, some SIS hits were missed;
- In one country, the need to repeat a search was raised, as the on-site team noted that the inversion of the name/surname is not possible, and a second search must be carried out;
- In one country, if a record includes special characters, the system will not be able to identify it unless these characters are included in the search term. Moreover, there were differences depending on the tool used as fuzzy logic searches were not possible on the fixed stations or on mobile devices;
- In one country, none of the information systems that have been assessed included a "fuzzy logic" search capability;
- In one country, the absence of a universal search tool incorporating fuzzy logic results in that law enforcement officials have to repeat a search several times in order to ensure that all the relevant records are considered, which increases the risk of missing possible matches.

There is limited availability of training for law enforcement staff involved in cross-border information exchanges and cooperation.

Training concerning **cross-border law enforcement cooperation** is **not** held on a **regular basis at national level** and does not always take into account the latest changes in the EU law enforcement legislative framework in a timely manner (e.g. new EU or Schengen-related legislative initiatives)[63]. In practice, this implies that training for staff involved in cross-border cooperation is often based on informal mentoring by experienced colleagues, which has a negative impact on the number of officials who possess the necessary skills to properly manage all the different procedures and information tools required[64]. Moreover, this training is often voluntary, thus leaving room for heterogeneous skills between police officials, and it is not always systematic for newcomers in the SPOCs and PCCCs[65].

Language barriers hamper the efficient cross-border exchange of information.

Finally, **language barriers** were reported by some Member States as hampering the cross-border exchange of information[66]. Officials engaged in cross-border cooperation are not always proficient in English and this has a twofold drawback. **First,** since EU official communication channels

[61] Transliteration is the process of representing words/names from one language using the alphabet or writing system of another language (multilingual name recognition). E.g. the letter "o" can be 'ò', 'ó', 'ô, 'õ', 'ö', 'ø' depending on the language/alphabet used. 8 Schengen evaluation reports.

[62] A fuzzy database is a database which is able to deal with uncertain or incomplete information using fuzzy logic. i.e. the ability to find matches even when a person' name is misspelled. 10 Schengen evaluation reports.

[63] 9 Schengen evaluation reports. Survey: Q 59, 58% (n=67) of LEAs respondents confirmed that the lack of knowledge and training among law enforcement practitioners about how to apply for or implement investigative tools act as barrier for effective cross-border cooperation.

[64] COM/2020/779 final. Available at: link.

[65] 8 Schengen evaluation reports.

[66] 12 Schengen evaluation reports. Survey: Q 34, 35 LEAs' representatives reported that language barriers are among the main issues they face when sharing information.

requires the exchange of information in a language that can be understood by the receiving Member State, officials who are not proficient in English or in the language of the requesting country prefer to exchange information via informal channels (e.g. email, etc.). **Second,** even when official channels are used, information is often reported in a rudimentary English. Thus, officials receiving a request for information often need to take time to translate it[67].

2.2.3. 2.2.3. How will the problem evolve without intervention?

Whilst it remains possible that the SPOCs and PCCCs will over time incrementally update and improve their information management systems, these developments would not be aligned between the Member States and the current efficiency and effectiveness gaps are expected to remain. The varied competences of the SPOCs across the EU would continue to hamper the efficient and effective exchange of information, notably because adequate access to key databases and platforms would not be ensured in all SPOCs and PCCCs. Moreover, some SPOCs would continue to have insufficient resources to address the information requests received within the deadlines in all cases.

The latest cycle of Schengen evaluations in the field of police cooperation revealed, in a number of Member States, deeply engrained internal coordination issues between different law enforcement authorities, preventing the proper functioning of their national SPOC/PCCCs.

Such internal issues have been proven to significantly hinder the efficient and effective functioning of the SPOC/PCCCs and hence the exchange of information between Member States. For example, some national SPOCs/PCCCs do not have a direct access to relevant national databases, nor benefit from a modern information architecture, thereby preventing necessary cross-match with EU and International databases.

Furthermore, designing IT upgrades can be complex and the implication far reaching rendering an efficient internal coordination even more essential. A general finding of the Schengen evaluations points to the need to address national/domestic structures, processes and procedure in order to improve the exchange of information between Member States in the framework of EU law.

Member States would not ensure appropriate and uniform level of training in intra-EU cross-border cases, in foreign languages and in the adequate use relevant databases and communication channels either. Law enforcement authorities will not effectively and efficiently exchange information with their partners in other Member States, thereby leaving the impacts in the evolution of the EU security landscape and in the increased cross-border mobility essentially unaddressed.

2.3. Problem 3: The free choice of communication channel(s) between Member States causes recurrent duplication of requests

2.3.1. 2.3.1. What is the problem?

Member States' law enforcement authorities use a variety of different channels to exchange information, leading to recurrent duplication of requests and creating confusion due to the number of information systems that can be used[68]. **Three main channels** are used for cross-border information exchange, each based on national units in each Member State that use a related communication tool:

[67] Some IT features allow for an automatic "rough" translation service.

[68] 1 Schengen evaluation report. technical workshop held on 24 March 2021. Q 41, 87% (n=57) of LEAs' respondents reported that the high number of communication channels for EU information exchange overburdens the officials involved in cross-border cooperation.

- SIRENE Bureaux can, following a hit on an alert in Schengen Information System (SIS), obtain supplementary information from the Member State that issued the alert. They operate 24/7 and follow the procedures of the SIRENE Manual.
- Europol National Units (ENUs) exchange information with Europol. They may also exchange information bilaterally on crime outside Europol's mandate and without involving Europol. ENUs can exchange information directly or through Europol Liaison Officers, who are part of an ENU but stationed at Europol headquarters. A secure communications tool, SIENA[69], has been developed by Europol for exchanges with Europol and between Member States.
- INTERPOL National Central Bureaux, operating 24/7, exchange information with INTERPOL as well as bilaterally without involving INTERPOL. National Central Bureaux use the I-24/7 communication tool developed by INTERPOL.

Other channels include bilateral Liaison Officers (stationed in other Member States and typically used in more complex cases) and PCCCs.

Member States use different channels to different extents to request, send and receive information, which hampers effective and efficient exchange of information. This was also confirmed by a number of stakeholders who also pointed out that the use of different tools at the same time contributes to the duplication of requests. Such cases of duplications of requests due to the use of different channels concerning the same piece of information were also reported during the technical workshop held on 24 March 2021[70].

On top of noted duplications, the use of different communication channels leads to the Europol Secure Information Exchange Network Application (SIENA) to being underused in spite of its tailored features and strong data security infrastructure. Even when Member States use Europol SIENA they can choose not to involve Europol in their bilateral exchanges even though the information exchanged falls under the Europol mandate. This significantly hinders Europol' ability to fulfil its support function, thereby creating an important information gap.

There are also **differences at national level as regards the access to EU instruments**. In some Member States all Law Enforcement Authorities (LEAs) have access to SIENA, in other ones, access to SIENA is only granted to a single national authority that coordinates the information exchange thereby hampering its full use[71]. Consequently, most of the times, regional and local investigation services do not have access to SIENA. This is particularly important considering that SIENA seems to be one of the preferable tools to share sensitive and confidential information since it allows to securely exchange data.

This issue was also raised in the recent evaluation of the EU Policy Cycle 2018-2021[72]. Notably, the effectiveness of SIENA was hindered by the fact that national stakeholders regularly have to firstly share information with the central authority which in turn shares it with other countries. This

[69] Secure Information Exchange Network Application. SIENA is Europol's secure communication system, Europol and its cooperation partners exchange operational and strategic crime-related information and intelligence, including operational data on persons. SIENA is a messaging system offering different message types for different purposes, including data exchange in accordance with the Swedish Framework Decision.

[70] 2 Member States' representatives at the Technical workshop held on 24 March 2021. Interviews: 1 EMPACT Driver. Moreover, the information received often includes details and data, which are not necessary to address the specific request. This results in unnecessary time to process all answers to the same request. Moreover, participants in the workshop confirmed that the information is not always exchanged using the appropriate channels and tools (e.g. a request from one Schengen country to another to locate a person is sent via I-24/7 and not through the SIRENE).

[71] In some Member States, investigators can use SIENA directly, shortening the information exchange process.

[72] EY, RAND (2020) Evaluation Study on the EU Policy Cycle/EMPACT 2018-2021. (Unpublished).

double-tier process delays the overall process, with possible negative impact on international investigations where timely information sharing is crucial for success[73].

Ideally, the SPOC should ensure that a request is sent through one channel only. The SPOC Front desk is crucial in choosing the most appropriate and relevant channel by gathering all requests ("in" or "out") dealt with by the SPOC, before dispatching them to the relevant desk (SIRENE Bureau, INTERPOL National Central Bureau, Europol National Unit, and bilateral liaison officers)[74]. So far, a number of **national SPOC use internal guidelines** recommending or requiring the specific use of a communication channel for specific purpose, thereby ensuring consistency and avoiding duplication of requests. **Other SPOCs rely on officers' habits and personal preferences**. Such leeway result in inefficiencies in a cross-border context. Council guidelines did not led to a convergence of national practices either[75].

The current proliferation of information exchange channels has also meant that different Member States have invested in different information exchange channels, thus not always matching the investments made in other Member States and hence hindering and effective use of the investments made domestically. Some Member States lack the necessary funding. Correspondingly, the present proposal will be flanked with financial support via the national programmes under the EU Internal Security Fund.

2.3.2. 2.3.2. What are the drivers?

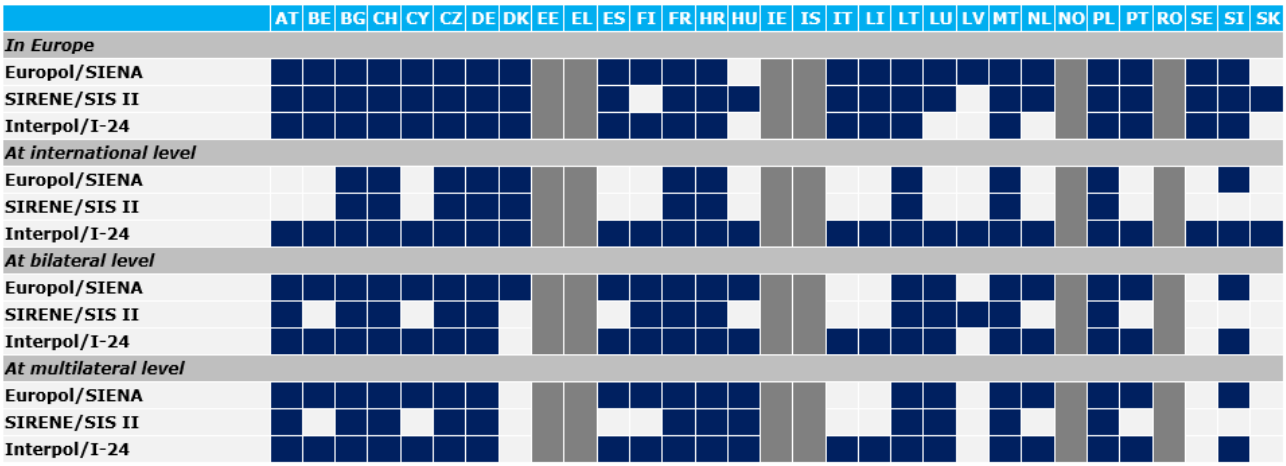
Member States have not agreed on a single channel of information exchange between their law enforcement authorities for cases with an EU dimension. The **choice of channel is only partly regulated by EU law**: SIS requests for supplementary information must be made via SIRENE Bureaux,[76] and information exchange with Europol via ENUs.[77] Otherwise the choice is up to Member States[78].

There is **not a clear rationale behind the choice of one tool instead of the other**[79]. Some Member States have moved towards more systematic use of the Europol channel. Others continue to rely a good deal on the INTERPOL channel for intra-EU cooperation, the attraction of which seems to lie partly in its traditional central role in international police cooperation, partly in its perceived ease of use, and partly on Member States officers' habits and personal preferences[80].

The **limited training** hampers the efficient use of available tools for exchanging information by national law enforcement officials. As regards the **PCCCs,** out of 59 PCCCs active in Europe in 2017, only nine were connected to SIENA[81] (against 14 PCCCs in 2021, thereby indicating slow progress).

[73] Survey for the Evaluation study on the EU Policy Cycle 2018-2021: 5 EMPACT Drivers and 11 Action Participants.
[74] Provided all channels are available to a SPOC and the SPOC is able and ready to use all channels appropriately.
[75] Council document 5825/20, 2.12.2020, *Manual on Law Enforcement Information Exchange*.
[76] SIS requests for post-hit supplementary information must be done via SIRENE Bureaux.
[77] Europol National Unit. Information exchange with Europol must be done via ENUs.
[78] Comparative analysis of the Schengen Evaluation Reports. Survey: Q 40, LEAs respondents agreed that although SIENA is the most frequently used tool (77%, n=128), all used INTERPOL I24/7 to a high or very high extent (INTERPOL: 52%, n=87).
[79] Comparative analysis of the Schengen Evaluation Reports.
[80] Survey: Q 2 SPOC's representatives, 1 PCCC representative. 1 Schengen evaluation report.
[81] Council document 14629/17, *State of play of the roll-out of SIENA regarding PCCCs*.

Communication channel used for police cooperation



**Blue cells: both channels are used indifferently. Light grey cells: preferred channel of communication. Dark grey cells: No Schengen evaluation report available*
Source: EY/RAND Europe Study's elaboration based on a questionnaire on the developments since the update of the SPOC guidelines in 2014

2.3.3. 2.3.3. How will the problem evolve without intervention?

The planned changes to SIENA that are currently envisaged by Europol are expected to lead to some clear improvements with regard to the cross-border exchange of information, notably due to its anticipated doubling of end-users.

Yet, Member States would only slowly update their IT information management system to integrate these upgrades. Member States are also expected to continue to send requests to multiple countries at the same time via parallel channels to "fish" for information, leading to duplication of work. Member States will remain free to choose not to copy Europol in their exchanges via Europol SIENA even when this concerns an offence falling under the Europol mandate. The qualitative and quantitative information flow towards Europol would thus only increase in a piece-meal manner across the European Union, hampering Europol's ability to support Member States in their cross-border investigations.

In the absence of further intervention, formal and informal processes that have been established over the years are expected to remain intact. This means that stakeholders are expected to continue to use ad hoc processes. One example is, of course, not sending an information request via SIENA, but simply calling the official counterpart in another country or requesting information via an informal email. Informal practices have been and remain an important part of law enforcement cooperation today. This being said, such traditional ways of working may no longer prove adequate in the future. More specifically, while they may work well between Member States where frequent contacts and cooperation are established, this may not be the case with other Member States. Existing Council guidelines did not manage to ensure a satisfactory convergence of national practices. Updated guidance is thus unlikely to achieve further results.

Without intervention, law enforcement authorities will continue not to effectively and efficiently exchange information with their partners in other Member States, thereby leaving the impacts in the evolution of the EU security landscape and in the increased cross-border mobility essentially unaddressed.

3. 3. WHY SHOULD THE EU ACT?

3.1. Legal basis

A legislative proposal following this impact assessment would be based on Article 87 (2) of the Treaty on the Functioning of the European Union (TFEU).

3.2. Subsidiarity: Necessity of EU action

The objective of improving information flows between relevant law enforcement authorities and with Europol, cannot be sufficiently achieved by the Member States acting alone. Owing to the cross-border nature of crime, the Member States are obliged to rely on one another. This can be better achieved at the level of the Union.

Despite the existence of a number of national and regional measures in place that aim to strengthen national capacity to deploy coordinated actions against common threats and challenges, Member States alone would not be able to ensure the full implementation of the principles of availability and of equivalent access to information. Member States would not overcome current differences among SPOCs (and in its relation with PCCCs), which hinder the efficient exchange of relevant information across countries. They would not ensure appropriate and uniform level of knowledge of and capacity to use relevant databases and communication channels.

The EU is better equipped than individual Member States to ensure the coherence of actions taken at the national level, address the divergence of practices, prevent duplications and uncertainties and eventually ensure an efficient counter-action to cross-border crime. The need for EU intervention is widely supported by Law Enforcement Authorities (LEAs) answering the survey with 82% (n=131) of respondents reporting a need for EU action from a moderate to a very high extent.

3.3. Subsidiarity: Added value of EU action

EU action in response to the identified problems is expected to bring added value for the entire EU with a ripple effect on Schengen Associated Countries, and therefore to its citizens. Common EU level rules, standards and requirements facilitating these information exchanges on cross-border crime between law enforcement authorities will generate significant **economies of scale** while ensuring high-level **data security and data protection standards**.

Additionally, common standards allow for the automation of information exchange workflows, releasing law enforcement officers from a number of labour-intensive/time-consuming manual activities, **thereby increasing the efficiency and effectiveness of national practices**.

Law enforcement cooperation at EU level does not replace different national policies on internal security. It does not substitute the work of national law enforcement authorities. Quite the contrary, EU level action supports and reinforces national security policies and the work of national law enforcement authorities, helping them to enforce the law against criminals and terrorists that act across borders. Differences in the legal systems and traditions of the Member States, as acknowledged by the Treaties[82], remain unaffected by this EU level support. The envisaged proposal, a Directive, would introduce an **obligation of result**. In full line with the subsidiarity principle, Member States will remain free to determine the most appropriate means to achieve the prescribed results.

4. 4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1. General objective

Law enforcement work is inherently an information-based activity. The successful prevention, detection and investigation of criminal offences, require a fast, streamlined and systematic access to all relevant information.

[82] Article 67(1) TFEU.

The general objective of the initiative is to ensure the timely access and the smooth exchange of necessary information, thereby enabling effective and efficient cooperation between law enforcement authorities to counter the cross-border dimension of criminal action while ensuring a high level of protection of fundamental rights and personal data.

4.2. Specific objectives

The specific policy objectives of this initiative respond to the three problems identified in chapter 2:

- To facilitate **equivalent access for law enforcement authorities** to information held in another Member State, while complying with fundamental rights and data protection requirements;
- To ensure that all Member States have an effective functioning **Single Point of Contact** (SPOC), including when a **judicial authorisation** is required to provide the data upon request of another Member State, and ensuring its effective cooperation with **Police and Customs Cooperation Centres** (PCCCs)[83];
- To **remedy the proliferation of communication channels** used for law enforcement information exchange between Member States **while empowering Europol** as the EU criminal information hub for offences falling within its mandate (unless otherwise regulated by EU law)

5. 5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

5.1. Baseline representing current situation

The baseline is a "no policy change" scenario **(option 0).** This implies:

- No additional regulatory intervention is implemented by the EU to the exception of the alignment the 2006 SFD with the 2016 Law enforcement data Protection Directive[84];
- No specific flanking support measures are undertaken by the EU, such as awareness raising, training, funding etc. in order to improve access to and exchange of information between Law Enforcement Authorities;
- No further technical changes are implemented by the EU, e.g. in relation to technical means to access and share information via SIENA, apart from what is already planned.
- However, the Commission committed to ensure the alignment of the 2006 SFD with the 2016 law enforcement data protection Directive (LED). Consequently at the very least, a targeted amendment would be necessary.

As a result, law enforcement authorities will not effectively and efficiently exchange information with their partners in other Member States and with Europol, causing operational hurdles in the daily law enforcement practices.

In addition, differences with regard to the efficiency and effectiveness of SPOCs, PCCCs and other equivalent structures are expected to continue to exist and hamper the level playing field between Member States.

Europol is making efforts to improve SIENA. The planned changes are expected to lead to some improvements with regard to the cross-border exchange of information already in the baseline scenario[85].

[83] This will also require that the PCCCs have the necessary structures, staffing and IT systems.

[84] Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

If no further action is taken (other than the ones already agreed or underway), LEAs will likely face additional challenges in keeping pace with criminal groups in the near future. LEAs are expected to take advantage of and use new technologies to cope with evolving criminal patterns.

5.2. Description of policy options

5.2.1. 5.2.1. Objective I: Facilitate equivalent access for law enforcement authorities to information held in another Member State, while complying with fundamental rights and data protection requirements

Policy option 1.1: New flanking soft measures (training, Commission guidance)

The problem described in chapter 2 will be addressed, to the extent possible, via support measures aiming to improve awareness, the implementation of EU provisions as well as national capabilities through dedicated funding via the Internal Security Fund (ISF).

This could cover training, Commission guidance (e.g. on the use of communication channels, on SPOCs, on PCCCs and on information exchange, the provision of a matrix concerning which information channel should be used in what cases, and the provision of information concerning what data are available in the Member States). Europol would be asked to speed up the SIENA roll-out.

As a result of the lisbonisation of the SFD, possible future guidelines will no longer be developed by the Council but by the European Commission. These new guidelines will require an active support from the Member States given national specificities and related technicalities.

Policy option 1.2: Option 1.1 + simplification in the use of the SFD + improve clarity on the national data sets available for possible exchange

Based on the Council guidance, the Schengen evaluations in the field of police cooperation, and on the Study' findings, the policy option 1.2 will cover Option 1.1, extended to the revision of the Swedish Framework Decision with a view to clarify and simplify its use, thereby improving the implementation of the principles of availability and of equivalent access.

This would be achieved through:

- *Adaptations to the SFD* to remove references to "other" cases and also remove the forms for information exchange (two annexes of the SFD);
- *Commission Guidelines* clarifying the data sets available for possible exchange;
- *Clarification of the scope* of operations to which the SFD applies[86].

Policy option 1.3: Option 1.2 + provisions ensuring compliance with deadlines requirements by which data is to be made available to another Member State (including when a judicial authorisation is required)

Based on the Council guidance, the Schengen evaluations in the field of police cooperation, and on the Study' findings, the policy option 1.3 will cover option 1.2 and extend the revision of the Swedish Framework Decision to ensuring compliance with deadlines requirements by which data is to be made available to another Member State (including when a judicial authorisation is required).

[85] See Europol's plan concerning the extension of SIENA access: https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena

[86] i.e., the explicit coverage of the prevention and detection of criminal offences (as in CISA).

5.2.2. 5.2.2. Objective II: Ensure that all Member States have an effective functioning Single Point of Contact (SPOC), including when a judicial authorisation is required to provide the data upon request of another Member State, and ensuring its effective cooperation with Police and Customs Cooperation Centres (PCCCs)

Policy option 2.1: Continue with Council non-binding guidelines on Single Points of Contact + new flanking soft measures (training, financial support, Commission guidance)

Based on the Council guidance, the Schengen evaluations in the field of police cooperation, and on the Study findings, the policy option 2.1 will limit itself to **supporting measures** to improve the effective and efficient role of SPOCs/PCCCs and any other relevant structures.

Recommendations (Commission Guidance – 'soft law') would be made with a view to support Member States in setting up and developing *common requirements for modern case management systems* (CMS). This would include:

- **Guidance** on a list of possible common requirements for the functionalities of the Case Management System (CMS), e.g.:
  - Degrees of urgency should be linked with a deadline (e.g. when a deadline draws near, automated alerts should be triggered);
  - Selection (in a multiple-choice list by the requesting Member State) and cancellation of the degrees of urgency should be done manually;
  - One CMS for receiving, sending and dispatching messages (follow up, manage, store and exploit the international exchange of information). The Universal Message Format (UMF) is to be used[87];
  - The Case Management System (CMS) should be able to import and export incoming messages from e-mail, documents or web applications to reduce the number of registration acts to the minimum;
  - Clear identification of the case and its components: within the case (unique case number), all documents and acts should be clearly identified. The CMS should be able to make links between persons/objects; per item – per act; author, date and time. This should be done automatically on the basis of the user profile;
  - Automation of data cross-check, e.g. through improved search tools and the adoption of transliteration and "fuzzy logic" search;
  - further coordination between the SPOCs and the PCCCs (and other relevant bodies) through the interconnectivity between their respective CMSs;
  - Generation of necessary statistics for national analytical needs.
- **Guidance** on accreditation of the CMS (security needs, security check for data access, data protection, handling codes, confidentiality, access rights by different units and to EU databases);
- **Guidance** on quality control: Through subject-based registration and the use of structured and mandatory fields and multiple-choice lists, certain quality requirements can be met beforehand without needing to conduct additional checks afterwards;
- **Guidance** on availability of technical support;
- Training on CMS use.

Updating existing Council guidelines in view to achieve further approximation of practices will require an active support from the Member States given national specificities and related technicalities. IT upgrades would require financial supports.

[87] The UMF defines standards for cross-border information exchange between information systems, authorities or organisations. This ensures an effective data processing across information systems.

Policy option 2.2: ***Approximation of minimum standards*** **on the composition of the Single Points of Contact (including when a judicial authorisation is required), its functions, staffing and IT systems, and its cooperation with regional structures such as Police and Customs Cooperation Centres + new flanking soft measures (as in option 2.1)**

Based on the Council' guidance, the Schengen evaluations in the field of police cooperation, and on the Study' findings, the policy option 2.2 will ensure the *approximation of common minimum requirements* regarding the SPOCs/PCCCs' (and any other relevant bodies) environment (structure, composition, role, IT capabilities and staffing). These common minumum requirements **('hard law')** will cover:

- *Establishment of the SPOC as a "one stop shop" for LEA cooperation through common minimum standards. A SPOC should*:
  - Be, at the minimum, informed about all international law enforcement cooperation requests dealt with at national level, and, in addition, be established as the preferred hub to handle intra-EU law enforcement cooperation requests;
  - Operate 24/7 (including when a judicial authorisation is required);
  - Have full access to all relevant EU and international law enforcement databases (i.e. Schengen Information System (SIS), Europol databases, INTERPOL databases and software applications;
  - Be connected to Europol SIENA (for intra-EU cases), INTERPOL I24/7 (for cases involving third countries having no access to Europol SIENA) and SIS;
  - Involve staff in the SPOC who have full access to all relevant national case management systems (including those managed by customs and border guards where relevant);
  - Ensure that all relevant information from the Police and Customs Cooperation Centres (PCCCs) is integrated in the SPOC information system;
  - Have arrangements for indirect (e.g. on a hit/no hit basis), but quick, effective and efficient access to relevant databases of other authorities or bodies (including customs, border guards and tax authorities where relevant);
  - Ensure further coordination between the SPOCs and the PCCCs and other relevant entities through the interconnectivity between the national SPOC and the national PCCCs (and any other equivalent bodies) Case Management Systems.

- *Establishment of new provisions on the skills of law enforcement officials working primarily on international cases:*
  - Provision on appropriate English skills as a criterion ("entry criterion") for specific roles within certain law enforcement agencies working primarily on international cases;
  - Provision on mandatory training on EU law enforcement cooperation for officials in specific roles relevant for cross-border law enforcement and at specific levels (e.g. newcomers/senior officials).

- *Establishment of flanking soft measures in the form of training measures:*
  - Establishment of an awareness raising and training campaign within the EU law enforcement community;
  - CEPOL to provide training material to law enforcement agencies (e.g. on how to use EU databases efficiently). The training material should focus on aspects common to all the Member States. The Member States would need to prepare additional training on the specificities in the individual country;
  - CEPOL to provide voluntary induction training on cross-border law enforcement;
  - Expansion of the existing CEPOL practice to provide online courses on an ad-hoc basis on new EU level developments;

- Performance of a regular review of the training content provided by CEPOL.

- *Establishment of common minimum requirements for Case Management Systems (CMS) for the SPOCs/PCCCs and other equivalent bodies* (see policy option 2.1 where these measures would only be proposed as non-binding guidance).

Policy option 2.3: *harmonisation* of rules on the composition of the Single Points of Contact (including when a judicial authorisation is required), its functions, staffing and IT systems, and its cooperation with regional structures such as Police and Customs Cooperation Centres + new flanking soft measures (as in option 2.1)

Based on the Council' guidance, the Schengen evaluations in the field of police cooperation, and on the Study' findings, the policy option 2.3 will ensure the *harmonisation* of rules regarding the SPOCs/PCCCs' (and any other relevant bodies) environment (structure, composition, role, IT capabilities and staffing).

This option will cover the same measures as described in policy option 2.2. The **legal provisions would however be more precise** where relevant. Such harmonisation would be carried out through a proposal for a Regulation and would consequently offer the advantage to **impose an "EU model" for information exchange.**

Contrary to option 2.2, where Member States would retain the possibility to chose how to best implement **common minimum requirements** and decide to go beyond them where they see fit, the harmonisation by means of a Regulation would bind Member States **not only regarding the objectives to be achieved but also with regards to the means to achieve them**.

Consequently, the impact of options 2.2 and 2.3 on Member States would thus differ considerably. The Regulation would also be directly applicable.

Measures covered by option 2.3 (Regulation) and not by option 2.2 (Directive) would notably seek to define a detailed check list of features for SPOCs, PCCCs and for their Case Management System (beyond com mon minimum requirements); e.g.:

- Requirement to set up a front desk at SPOC to determine which office/contact point will deal with the incoming request;
- Requirement to determine the priority level of the request at the Front Desk;
- Empower the SPOC management to impose an arbitrage in case of disagreement between law enforcement authorities composing the SPOC;
- Requirement to set up the SPOC in a secure working environment, including high level of security and safety of the premises and is equipped with back-up power systems;
- Requirement for the SPOC to use of the Universal Message Format as a standard for structured, cross-border information exchange;
- mandatory development of fuzzy search (notably multi-category search, partial search, any name search) and transliteration tools;
- automated attribution of a single registration number to every case, unique for the involved cooperation channels such as SIRENE, INTERPOL, Europol, etc.;
- Case Management System able to import and export incoming messages from e-mail, documents or web applications to reduce the number of registration acts to the minimum. The same could apply to the exportation of generated messages;
- Requirements regarding the training of staff...

5.2.3. 5.2.3. Objective III: To remedy the proliferation of communication channels used for law enforcement information exchange between Member States while empowering Europol as the EU criminal information hub for offences falling within its mandate (unless otherwise regulated by EU law)

Policy option 3.1: Continue with Council non-binding guidelines and Recommendations to put Europol in copy when using SIENA[88] in cases within Europol' mandate + new flanking soft measures (training, financial support)

Policy option 3.1 will limit itself to supporting measures to improve the effective and efficient use of SIENA. They will mandate Europol with training in the use of SIENA and support Member States' effort notably through funding. The following *non-legislative* improvements to SIENA would also be recommended:

- Establishment of new, simpler and more user-friendly forms (e.g. design and accessibility, types of information required and clarifications and wording, multiple-choice alternatives, removal of references to "other cases") and implementation of these in SIENA. The forms should include factual reasons for the information request;
- Extension of the functionalities of SIENA, such as the introduction of an automated display of a hit/no hit indication (plus a possibility to request further information).

Updating existing Council guidelines in view to achieve further approximation of practices will require an active support from the Member States given national specificities and related technicalities.

Policy option 3.2: Obligation to use SIENA as the preferred communication channel + obligation to put Europol in copy when using SIENA in cases within Europol's mandate + new flanking soft measures (as in option 3.1)

Policy option 3.2 will clarify existing guidelines on the preferred channels of communication. These provisions will cover:

- *Establishment of the information channel to be used:* Establishment of SIENA as the *preferred channel* of communication for information exchange in an intra-EU context, while maintaining Member States' possibility to choose another communication channel. INTERPOL I24/7 should be used in cases where third countries are involved in the exchange of information. SIENA would need to be monitored 24/7 at national level. There would also be an obligation to put Europol in copy in cases concerning information exchange within Europol's mandate.

Policy option 3.3: obligation to use SIENA by default for all bilateral information exchange (unless otherwise regulated by EU law) + obligation to put Europol in copy when in cases within Europol's mandate, both after the end of a transition period and with Internal Security Fund support for the SIENA roll-out + new flanking soft measures (as in option 3.1)

With Policy option 3.3, Europol SIENA will become the mandatory channel of communication by default for police cooperation[89] between EU Member States[90] (excluding those situations where other channels are required by EU law, e.g. SIS). This means that for cases that only have an EU

[88] Europol's "Secure Information Exchange Network Application".
[89] This would not affect the work and cooperation of intelligence services.
[90] Member States will no longer be able to choose another communication channel. Exceptions would be considered under clearly defined circumstances.

dimension or in relation to which it is not (yet) clear if they also concern third countries, SIENA should be used as channel for information exchange[91].

This obligation will only come into force after a necessary transition period allowing the full roll-out of SIENA to all relevant end users. Funding will be made available to support Member States necessary IT upgrades. Additional (flanking) measures correspond to policy option 3.1.

5.3. Options discarded at an early stage

Following the consultation of stakeholders, the Commission discarded[92] the option of expanding legislative changes to the 1998 Naples II Convention on mutual assistance and cooperation between customs administrations. This decision has been taken in view of necessity and proportionality considerations, customs cooperation being mostly of administrative nature.

Customs administrations are nevertheless fully covered as competent authorities under the objectives of this initiative with a view to improve cooperation between relevant law enforcement authorities (notably against tax crimes e.g. tobacco smuggling):

- *Objective I:* Customs administrations are competent under the Swedish Framework Decision. Its revision by means of a Directive thus covers its use by customs administrations;
- *Objective II:* customs administrations are to become part of the SPOC where this is not yet the case and where relevant. This includes necessary access to relevant customs databases and case management system (also in Police and Customs Cooperation Centres – where they exist);
- *Objective III:* customs administrations, as part of the SPOC, are to use Europol SIENA by default when engaging with another Member State and copy Europol when concerning an offence within Europol's mandate.

6. 6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

This chapter assesses all policy options identified in section 5.2 against the baseline options identified in section 5.1. Given that the baseline scenario is evidently unsuited to address the problems identified in chapter 2 (problem definition), this impact assessment will not assess the baseline scenario any further[93].

These impacts cover a wide range of parameters, including effectiveness, efficiency, EU added value, proportionality and coherence. These criteria are further elaborated upon regarding the combined preferred option.

No direct environmental and economic impacts were clearly identified per policy option. Nevertheless, the following high-level impacts could be mentioned:

[91] SIENA is used by 20.000 SIENA end-users (originating from 2.300 law enforcement authorities). 1.3 million SIENA messages were exchanged in 2020. The number of SIENA messages only continues to increase. In the first six months of this year, SIENA has experienced a strong increase of 26% when compared to the same period last year (note that COVID has not slowed down the exchanges).

[92] Additional discarded options can be found in annex 7.

[93] The baseline scenario is expected to, one the one hand, have a small positive impact as regards the achievement of the horizontal objective. It will have no identified impact on objective I (alignment with the LED excluded). Regarding objective II, the current differences between the national set-ups are expected to continue to exist and hamper the level playing field between Member States. Regarding objective III, Europol is expected to make further improvements to SIENA, potentially doubling the number of users. However, this will not adequately address the current and expected future challenges.

- **Environmental impact:** A small negative impact is expected on the environment due to the expected increase in electricity consumption in relation to computers and servers used for information exchange.
- **Economic impact:** Immediate economic impacts of any of the above options will be limited to the design, development and operation of the new processes. The costs will fall to the EU budget and to Member State authorities operating the systems. They will vary depending on the Member States national specificities and needs. ISF[94] funding will be made available to support Member States necessary IT upgrades. The proposed measures may have a positive impact on **small and medium-sized enterprises** given the need for IT-related products. An indirect positive economic impact could be found in a more effective fight against counterfeited good, thereby better protecting SMEs' intellectual property rights.

6.1. Fundamental Right expected impacts

The provisions on data protection and privacy contained in the 2006 Swedish Framework Decision (SFD) are outdated. The full alignment with the 2016 Data Protection Law Enforcement Directive (LED) is a legal obligation. This is relevant with regard to Article 7 (Respect for private and family life) and Article 8 (Protection of personal data) of the EU Charter of Fundamental Rights. In line with that, the Commission committed in a 2020 Communication to "*make a legislative proposal, which as a minimum will entail an amendment of Council Framework Decision 2006/960/JHA to ensure the necessary data protection alignment, in the last quarter of 2021* [95].

The sharing of information between Law Enforcement Authorities has a potential impact on Fundamental Rights. This concerns the Articles 2 (Right to life), 3 (Right to the integrity of the person), 6 (Right to liberty), 17 (Right to property) and 45 (Freedom of movement and of residence) of the EU Charter of Fundamental Rights.

Data protection impact: EU institutions and Member States are bound to the Charter of Fundamental Rights of the EU when they implement EU law (Article 51(1) of the Charter). The options presented in this impact assessment need to be balanced with the obligation to ensure that interferences with Fundamental Rights that may derive from them are limited to what is strictly necessary to genuinely meet the objectives of general interest pursued, subject to the principle of proportionality (Article 52(1) of the Charter).

Exchange of information has an impact on the right of protection of personal data. The latter is established by Article 8 of the Charter and Article 16 of the Treaty on the Functioning of the European Union. As underlined by the Court of Justice of the EU[96], the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society. Data protection is closely linked to respect for private and family life, protected by Article 7 of the Charter, and in Article 8 of the European Convention on Human Rights.

---

[94] Internal Security Fund 2021-27. With an overall budget of EUR 1.9 billion, the Internal Security Fund, will finance actions in the field of fight against terrorism and radicalisation, serious and organised crime, cybercrime and the protection of victims. Member States will implement the largest share of the allocation through multiannual national programmes. In addition to this, the Commission will also implement actions of particular EU value; the Union actions.

[95] COM(2020)262, *Way forward on aligning the former third pillar acquis with data protection rules.* As per this Communication, the alignment of the SFD with the 2016 Law Enforcement Data Protection Directive will:

- specify the types of personal data that can be exchanged;
- further clarify the safeguards: in particular the requirement of a necessity and proportionality assessment of each information exchange;
- make reference to the applicability of the Law Enforcement Data Protection Directive and the high level of protection that is provides.

[96] Court of Justice of the EU, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert (2010).

No potential harmful effect of the policy options on other Fundamental Rights has been identified, as the impact of these policy options is limited to impacts on the right to the protection of personal data.

The **Law Enforcement Data Protection Directive 2016/680 (LED)**[97] **already applies** to personal data processing activities carried out on the basis of the SFD. The revision of the Swedish Framework Decision will ensure its explicit alignment with the LED. It will contain a new provision stating that the legal instrument is **without prejudice to the LED**. The application of the Law Enforcement Data Protection Directive remains a matter of national competence when applying EU law. Concerning data protection, national law transposing the Law Enforcement Data Protection Directive are applicable to data exchanges between Member States.

The SFD will be aligned with the 2016 Law Enforcement Data Protection Directive (as part of the baseline scenario) thereby ensuring the high level of data protection provided by the wider EU data protection regime. While maintaining the specific data protection safeguards already provided for in the SFD, the alignment with the Law Enforcement Data Protection Directive will provide the necessary safeguards for the cooperation between police authorities in the EU.

Taken together, this will provide all the necessary safeguards. As the Law Enforcement Data Protection Directive provides the required level of data protection in the Union, there is no need to go beyond it. Instead, the alignment will ensure full consistency with the wider EU data protection rules.

Each of the options meet an objective of general interest, which is the safeguarding of the internal security of the European Union. Therefore, for each option, the impact on Fundamental Rights is assessed based on **necessity** of the measure and **its proportionality** to the objective.

The impacts are assessed on a scale ranging from 'highly positive impact' (+++) to 'highly negative impact' (---), with intermediate scores: 'significant positive impact' (++), 'significant negative impact' (--), 'low positive impact' (+), 'low negative impact' (-), 'neutral – no impact' (0).

More specifically, it should be noted that various elements considered under this legal proposal may have different impacts on fundamental rights, as outlined below.

Legal barriers

Adaptations to the 2006 Swedish Framework Decision, notably Article 8 on data protection, to ensure alignment with the LED are expected to positively impact safeguarding **citizens' fundamental rights**.

Moreover, a number of additional, targeted procedural safeguards would be introduced by the new legislative instruments which may have a **positive impact on the citizens' right to the protection of personal data**:

- The establishment of new provisions ensuring compliance with the deadlines by which data are to be made available to another Member State may have a positive impact on citizens' Fundamental Rights. Indeed, possible suspects who are being wrongfully accused of crimes are expected to be cleared faster. This is expected to improve safeguarding, for instance, the citizens' right to liberty, freedom of movement and of residence;
- The provision on training and updated guidance for officials in relation to the access to and exchange of information may increase the efficiency of law enforcement cooperation processes. This is also expected to contribute to potentially clear citizens from wrongful charges in a swifter fashion;

[97] Directive (EU) 2016/680, OJ L 119, 4.5.2016.

- The clear establishment of SIENA as the mandatory information channel to be used by default is expected to have a positive impact by minimising the opportunities for officials to "fish" for specific information that could compromise suspects' Fundamental Rights. Furthermore, the use of SIENA for information exchange between Member States will improve the safeguard of data protection standards given the state-of-the-art security and built-in data protection parameters SIENA offers;

- A modern SPOC, equipped with a proper information management architecture, will be able to track access to databases thereby ensuring proper use.
- The removal of references to "other" cases in the SFD is also expected to positively impact on safeguarding fundamental rights, as it may contribute to reducing the likelihood of unsolicited information about citizens is being exchanged between Member States. Moreover, by removing the category "other" cases, all cases would either be "urgent" or "non-urgent". This is expected to speed up the process of requesting information and, thus, could have a positive impact on citizens' Fundamental Rights.

Technical barriers

At the technical level, there are potential risks to Fundamental Rights in relation to the use of Case Management Systems (CMSs) by SPOCs. The measures considered aims to address existing risks by introducing common requirements for the functionalities of the CMSs run by SPOCs, e.g. establishing one CMS for receiving, sending and dispatching messages. This is expected to reduce the number of cases in which case management is distributed across several platforms and layers which, in turn, is expected to reduce the risk of officials unduly being able to access and exchange information.

Moreover, improvements with regard to the clear identification of the case and its components in the CMS are expected to positively impact on citizens' Fundamental Rights. The likelihood of confusing cases and, as a consequence access and exchange unsolicited information is expected to be more limited than in the baseline scenario.

The introduction of a need for an accreditation of Member States' CMS with regard to security needs, security check for data access, data protection, handling codes, confidentiality, access rights by different units and to EU databases is expected to positively impact Fundamental Rights. Law enforcement authorities' IT systems are a prime target for hackers and, thus, under constant scrutiny with regard to their security and potential to ensure citizens' privacy. Therefore, the accreditation of CMS satisfying certain technical minimum quality criteria is expected to add an additional safeguard for IT systems being compromised by criminals. Other safeguards are ensured by the Member States as per their transposition of the **Law Enforcement Data Protection Directive 2016/680 (LED)**.

Structural barriers

At the structural level, the measures envisaged ensure that SPOCs are, at the minimum, informed about all international law enforcement cooperation requests dealt with at national level, and, in addition, established as the preferred hub to handle intra-EU law enforcement cooperation requests. The increased ability and role of the SPOCs to coordinate law enforcement cooperation is expected to have a positive impact on citizens' Fundamental Rights, since cases can be administered more swiftly and discretely without multiple authorities being unduly involved in the processes.

At the same time, however, providing SPOCs via the involvement of different types of eligible law enforcement officials with full access to EU and international law enforcement databases could be regarded by some stakeholders (e.g. Non-Governmental Organisations) as an excessive measure in view of providing law enforcement authorities with only the necessary access to information. Similar to the argumentation in relation to the legal and technical barriers, additional and updated training on EU law enforcement cooperation (including by CEPOL) is expected to increase citizens'

Fundamental Rights thus effectively and efficiently mitigating the risk of unnecessary and disproportionate access to personal data.

Problem 1: Rules at national level impede the effective and efficient flow of information

6.2. Objective I: Facilitate equivalent access for law enforcement authorities to information held in another Member State, while complying with fundamental rights and data protection requirements

Policy Option 1.1: New flanking soft measures (training, Commission guidance)

Expected impact of policy option 1.1
1. Impact on citizens and businesses [+]
• **Low positive impact** to the security of the European citizens and societies. The simplification/clarification in both the scope and the use of the Swedish Framework Decision and supporting soft measures would **marginally** support Member States to more effectively counter any forms of criminal offences. This would also **marginally** reduce undue delays in the information sharing.
2. Impact on national authorities [+]
• **Low positive impact** on national authorities, which could **marginally** contribute to efficiently combat criminal offences, because of the simplification/clarification in the scope and use of the Swedish Framework Decision and the adoption of supporting soft measures. • A **low** negative impact would be a **possible marginal** workoad increase for national SPOCs.
3. Impact on EU bodies [+]
• The adoption of supporting soft measures would **marginally** contribute to increase the quality and quantity of information shared with Europol.
4. Effectiveness in meeting the policy objectives [+]
• This policy option would **marginally** address the objective of facilitating the implementation of the principle of equivalent access to information and intelligence held in another Member State while complying with fundamental rights and data protection requirements. If the later would be fully covered such would be the case for the former. • The better respect of deadlines, including when a judicial authorisation is required, would **not** be ensured.
5. Efficiency in meeting the policy objectives [++]
• This option may generate **cost** at EU and Member States. • The extent of these costs may vary depending on the nature and scale of the soft measures. • Some of these costs would already be covered by relevant EU agencies as part of their support functions to Member States (e.g. training). They don't outweight benefits.
6. Legal feasibility [++]
• This policy option will require changes to the 2006 Swedish Framework Decision. It ensures the respect of the conferral of powers and of fundamental rights.
7. technical feasibility [+++]
• This policy option would be technically feasible. Member States would need to take the necessary steps to ensure the implementation of updated guidances and related trainings.
8. Coherence with other measures [+]
• This policy option would **marginally** complement other Commission initiatives such as the Commission proposals for a new Schengen border code, for Prüm II on automated information exchange and for Europol.

Policy option 1.2: Option 1.1 + simplification in the use of the SFD + improve clarity on the national data sets available for possible exchange

Expected impact of policy option 1.2
1. Impact on citizens and businesses [++]

• **Significant positive impact** to the security of the European citizens and societies. On top of option 1.1, the simplication in the use of the SFD and improved clarity on the national data sets available to law enforcement authorities of other Member States would **significantly** support Member States to more effectively counter any forms of criminal offences. This would also **moderately** reduce undue delays in the information sharing.
2. Impact on national authorities [++]
• **Significant positive impact** on national authorities, which could **significantly** contribute to efficiently combat criminal offences, because of the swifter information exchange. • A **moderate** negative impact would be a **possible moderate** workoad increase for national SPOCs.
3. Impact on EU bodies [++]
• On top of option 1.1, the simplication in the use of the SFD and improved clarity on the national data sets available for possible exchange would s**ignificantly** contribute to increase the quality and quantity of information shared with Europol.
4. Effectiveness in meeting the policy objectives [++]
• This policy option would s**ignificantly** facilitate the implementation of the principle of equivalent access to information and intelligence held in another Member State while complying with fundamental rights and data protection requirements. • The respect of deadlines, including when a judicial authorisation is required, will **not** be ensured.
5. Efficiency in meeting the policy objectives [++]
• As option 1.1 + option 1.2 which would generate **costs** for a number of **Member States.** • These costs will vary significantly depending on the national solution considered by the concerned Member States. They don't outweight benefits.
6. Legal feasibility [++]
• This policy option will require changes to the Swedish Framework Decision. It ensures the respect of the conferral of powers and of fundamental rights.
7. technical feasibility [+++]
• This policy option would be technically feasible. Member States would need to take the necessary steps to ensure the implementation of new legal provisions.
8. Coherence with other measures [++]
• This policy option would **significantly** complement other Commission initiatives such as the Commission proposals for a new Schengen border code, for Prüm II and for Europol.

Policy option 1.3: Option 1.2 + provisions ensuring compliance with deadline requirements by which data is to be made available to another Member State (including when a judicial authorisation is required)

Expected impact of policy option 1.3
1. Impact on citizens and businesses [+++]
• **Highly positive impact** to the security of the European citizens and societies. On top of option 1.2, provisions ensuring compliance with deadlines requirements by which data is to be made available to another Member State, including when a judicial authorisation is required, would **highly** support Member States to more effectively counter any forms of criminal offences. This would also cleary reduce undue delays in the information sharing.
2. Impact on national authorities [+++]
• **Highly positive impact** on national authorities, which could **highly** contribute to efficiently combat criminal offences, because of the provisions ensuring compliance with deadlines, including when a judicial authorisation is required. • A **significant** negative impact would be a **possible significant** workoad pressure for national SPOCs to deliver in a timely fashion.
3. Impact on EU bodies [+++]
• On top of option 1.2, the the provisions ensuring compliance with deadlines, including when a judicial authorisation is required would **highly** contribute to facilitate the timely support of Europol.
4. Impact on fundamental rights [++]

• **Siginificant** positive impact. • Compliance with the deadlines by which data are to be made available to another Member State is often not ensured. One of the negative consequences could be that citizens who are (wrongfully) subject to criminal investigations are not cleared from pending charges as swiftly as possible. This option would address that.
5. Effectiveness in meeting the policy objectives [+++]
• **Highly positive impact.** This policy option would **clearly** address the objective of facilitating the implementation of the principle of equivalent access to information and intelligence held in another Member State while complying with fundamental rights and data protection requirements. The better respect of deadlines, including when a judicial authorisation is required, would be ensured.
6. Efficiency in meeting the policy objectives [++]
• As option 1.2 + option 1.3 which would generate **costs** for a number of **Member States.** • These costs would vary significantly depending on the solution adopted by the concerned Member States to ensure the functional availability of a judicial authority. They don't outweight benefits.
7. Legal feasibility [++]
• This policy option will require changes to the Swedish Framework Decision. It ensures the respect of the conferral of powers and of fundamental rights.
8. technical feasibility [+++]
• This policy option would be technically feasible. Member States would need to take the necessary steps to ensure the implementation of new legal provisions.
9. Coherence with other measures [+++]
• **Highly positive impact.** This policy option would **clearly** complement other Commission initiatives such as the Commission proposals for a new Schengen border code, for Prüm II and for Europol.

<u>Problem 2:</u> Structures and IT systems at national level are not set up and equipped in a sufficiently efficient and effective manner

6.3. Objective II: Ensure that all Member States have an effective functioning Single Point of Contact (SPOC), including when a judicial authorisation is required to provide the data upon request of another Member State, and ensuring its effective cooperation with Police and Customs Cooperation Centres (PCCCs)

<u>Policy option 2.1:</u> Continue with Council non-binding guidelines on Single Points of Contact + new flanking soft measures (training, financial support, Commission guidance)

Expected impact of policy option 2.1
1. Impact on citizens and businesses [+]
• **Low positive impact** to the security of the European citizens and societies. The adoption and development of soft measures would **marginally** support Member States to more effectively counter any forms of criminal offences. This would also **marginally** reduce undue delays in the information sharing.
2. Impact on national authorities [+]
• **Low positive impact** on national authorities, which could **marginally** contribute to efficiently combat criminal offences, because of the adoption and development of support measures. • A **low** negative impact would be a **possible marginal** workoad increase for national SPOCs however marginally offset by the improvements the soft measures would bring.
3. Impact on EU bodies [+]
• The adoption and development of support measures would **marginally** contribute to increase the quality and quantity of information shared with Europol.
4. Impact on fundamental rights [+]
• **Low positive impact.** Possible guidance on the implementation of the 2016 law enforcement data protection Directive (LED) at national level would **better** safeguard the Right to respect for private and family life and the Right to protection of personal data. They would not have additional capabilities in data processing.
5. Effectiveness in meeting the policy objectives [+]

• This policy option would **marginally** address the objective of an effective functioning of the SPOCs, PCCCs (and any other equivalents bodies). • Given national specificities, actual progress would essentially be left to Member States' ability and wilingness to diligently follow up on updated guidances. • Member States developments may not be aligned, thereby further deepening existing differences in the functionning of the SPOC, PCCCs and any other equivalent bodies.
6. Efficiency in meeting the policy objectives [++]
• This option may generate **cost** at EU and Member States. • The extent of these costs may vary depending on the nature and scale of the soft measures. • Some of these costs would already be covered by relevant EU agencies as part of their support functions to Member States (e.g. training). They don't outweight benefits.
7. Legal feasibility [0]
• This policy option would require no legal changes. It is de facto in line the conferral of powers and with the respects of fundamental rights.
8. technical feasibility [+]
• This policy option would be technically feasible. Its extent would depend on the level of ambition and on the technical requirements needed at national level.
9. Coherence with other measures [+]
• This policy option would **marginally** complement other Commission initiatives such as the Commission proposals for a new Schengen border code, for Prüm II and for Europol.

Policy option 2.2: ***Approximation of minimum standards*** **on the composition of the Single Points of Contact (including when a judicial authorisation is required), its functions, staffing and IT systems, and its cooperation with regional structures such as Police and Customs Cooperation Centres + new flanking soft measures (as in option 2.1)**

Expected impact of policy option 2.2
1. Impact on citizens and businesses [++]
• **Significant positive impact** to the security of the European citizens and societies. The approximation of common minimum standards in the functioning of the SPOCs, PCCCs and any other equivalent bodies would **significantly** support Member States to more effectively counter any forms of criminal offences. This would also **significantly** reduce undue delays in the information sharing.
2. Impact on national authorities [++]
• **Significant positive impact** on national authorities, which could significantly contribute to efficiently combat criminal offences, because of what the approximation of common minimum standards would bring in the functioning of the SPOCs, PCCCs and any other equivalent bodies. It would also facilitate the link with judicial authorities whenever judicial authorisation is needed. • A negative impact would be a **likely** workoad increase for national SPOCs however offset by the improvements the approximation of common minimum standards would bring.
3. Impact on EU bodies [++]
• The adoption and development of support measures would **significantly** contribute to increase the quality and quantity of information shared with Europol. • The adoption and development of **flanking soft measures** (training, financial support, guidance) would be essential.
4. Impact on fundamental rights [++]
• **Significant positive impact.** Since SPOCs are not always informed about all international law enforcement cooperation requests dealt with at national level, there is a risk that procedures are being duplicated or "fly below the radar" which, for instance, can be a risk in relation to the rights to privacy since the same information can be requested a number of times. Minimum requirements regarding the functioning of the SPOC will also improve the efficiency and effectiveness of information sharing thereby more swiftly contribute to establishing a possible offender implication (or lack thereof).
5. Effectiveness in meeting the policy objectives [++]
• This policy option would **significantly** address the objective of an effective functioning of the SPOCs, PCCCs

(and any other equivalents bodies).
6. Efficiency in meeting the policy objectives [++]
• As option 2.1 + option 2.2 which would generate **costs** for a number of **Member States.** • These costs would vary significantly depending on the effectivenss and efficiency of the national SPOCs and PCCCs (if any). • This would essentially cover possible IT upgrades. They don't outweight benefits.
7. Legal feasibility [++]
• This policy option would require **new provisions** regarding the functioning of the SPOCs, PCCCs and any other equivalent bodies. These provisions ensure the respect of the conferral of powers and of fundamental rights (approximation of common minimum standards. Member States are free to go beyond as they see fit).
8. Technical feasibility [+]
• Even though this policy option would be technically feasible, the extent of this approximation would vary significantly from one Member State to the next depending on national needs. • The adoption and development of **flanking soft measures** (training, financial support, guidance) would be essential.
9. Coherence with other measures [++]
• This policy option would **significantly** complement other Commission initiatives such as the Commission proposals for a new Schengen border code, for Prüm II and for Europol.

<u>Policy option 2.3:</u> *Harmonisation* of rules on the composition of the Single Points of Contact (including when a judicial authorisation is required), its functions, staffing and IT systems, and its cooperation with regional structures such as Police and Customs Cooperation Centres + new flanking soft measures (as in option 2.1)

Expected impact of policy option 2.3
1. Impact on citizens and businesses [+++]
• **Highly positive impact** to the security of the European citizens and societies. The harmonisation of rules concerning the functioning of the SPOCs, PCCCs and any other equivalent bodies would **highly** support Member States to more effectively counter any forms of criminal offences. This would also **clearly** reduce undue delays in the information sharing.
2. Impact on national authorities [+++]
• **Highly positive impact** on national authorities, which could significantly contribute to efficiently combat criminal offences, because of the harmonisation of rules concerning the functioning of the SPOCs, PCCCs and any other equivalent bodies would bring. It would also facilitate the link with judicial authorities whenever judicial authorisation is needed. • A negative impact would be a **likely** workoad increase for national SPOCs however offset by the improvements the harmonisation of rules would bring.
3. Impact on EU bodies [+++]
• The harmonisation of rules concerning the functioning of the SPOCs, PCCCs and any other equivalent bodies would **highly** contribute to increase the quality and quantity of information shared with Europol. • The adoption and development of **flanking soft measures** (training, financial support, guidance) would be essential.
4. Impact on fundamental rights [+++]
• **Highly positive impact.** Since SPOCs are not always informed about all international law enforcement cooperation requests dealt with at national level, there is a risk that procedures are being duplicated or "fly below the radar" which, for instance, can be a risk in relation to the rights to privacy since the same information can be requested a number of times. Harmonisation of requirements regarding the functioning of the SPOC will also improve the efficiency and effectiveness of information sharing in a standardised fashion, thereby more swiftly contribute to establishing a possible offender implication (or lack thereof).
5. Effectiveness in meeting the policy objectives [+++]
• **Highly positive impact.** This policy option would **clearly** address the objective of an effective functioning of the SPOCs, PCCCs (and any other equivalents bodies).
6. Efficiency in meeting the policy objectives [++]

• The costs of option 2.3 would be fairly comparable to those of option 2.2. • These costs would essentially cover IT upgrades. They don't outweight benefits.
7. Legal feasibility [-]
• This policy option would **not** be fully aligned with the subsidiarity principle and existing national legal traditions.
8. technical feasibility [---]
• This policy option would **not** be technically feasible given the **major technical**, legal and financial implications. • The adoption and development of **flanking soft measures** (training, financial support, guidance) would be essential.
9. Coherence with other measures [+]
• **Highly positive impact.** This policy option would **clearly** complement other Commission initiatives such as the Commission proposals for a new Schengen border code, for Prüm II and for Europol.

Problem 3: The free choice of communication channel(s) between Member States causes recurrent duplication of requests

6.4. Objective III: To remedy the proliferation of communication channels used for law enforcement information exchange between Member States while empowering Europol as the EU criminal information hub for offences falling within its mandate (unless otherwise regulated by EU law)

Policy option 3.1: Continue with Council non-binding guidelines and Recommendations to put Europol in copy when using SIENA[98] in cases within Europol' mandate + new flanking soft measures (training, financial support)

Expected impact of policy option 3.1
1. Impact on citizens and businesses [+]
• **Low positive impact** to the security of the European citizens and societies. The adoption and development of support measures would **marginally** support Member States to more effectively counter any forms of criminal offences. This would also **marginally** reduce undue delays in the information sharing.
2. Impact on national authorities [+]
• **Low positive impact** on national authorities, which could **marginally** contribute to efficiently combat criminal offences, because of the adoption and development of support measures. Updated guidance could reduce the recurrent duplication of request across several communication channels.
3. Impact on EU bodies [+]
• The adoption and development of support measures would **marginally** contribute to increase the quality and quantity of information shared with Europol via SIENA.
4. Impact on fundamental rights [+]
• **Low positive impact** through soft measures aiming at improving the choice of the communication channel, thereby possibly reducing the duplication of requests across several communication channels. Law enforcement authorities will remain free to consider what types of information should be made available for possible exchange. They would not have additional capabilities in data processing.
5 Effectiveness in meeting the policy objectives [+]
• This policy option would **marginally** address the objective of setting up a default communication channel for law enforcement exchange between Member States. • Actual progress would essentially be left to Member States' ability and wilingness to diligently follow up on updated guidances.
6. Efficiency in meeting the policy objectives [++]

[98] Europol's "Secure Information Exchange Network Application".

- This option may generate **cost** at EU and Member States.
- The extent of these costs may vary depending on the nature and scale of the soft measures.
- Some of these costs would already be covered by relevant EU agencies as part of their support functions to Member States (e.g. training, SIENA roll-out). They don't outweight benefits.

7. Legal feasibility [0]

- This policy option would require no legal changes. It is de facto in line the conferral of powers and with the respects of fundamental rights.

8. technical feasibility [++]

- Even though this policy option would be technically feasible, favouring the use of Europol SIENA as channel of communication between Member States for offences falling within the Europol mandate, through guidelines, would require the full roll-out of SIENA to all relevant end-users.
- Significant technical and financial support will be needed.

9. Coherence with other measures [+]

- This policy option would **marginally** complement other Commission initiatives such as the Commission proposals for a new Schengen border code, for Prüm II and for Europol.

Policy option 3.2: Obligation on Member States to use SIENA as the preferred communication channel + obligation to put Europol in copy when using SIENA in cases within Europol's mandate + new flanking soft measures (as in option 3.1)

Expected impact of policy option 3.2

1. Impact on citizens and businesses [++]

- **Significant positive impact** to the security of the European citizens and societies. The obligation to use use SIENA as the preferred communication channel while putting Europol in copy when this concerns its mandate would **significantly** support Member States to more effectively counter any forms of criminal offences.

2. Impact on national authorities [++]

- **Significant positive impact** on national authorities, which could **significantly** contribute to efficiently combat criminal offences, because of the obligation to use communication channels for the same purpose while putting Europol in copy when this concerns its mandate.
- This would **significantly** address the issue of duplication of requests through several communication channel, thereby saving offciers' valuable time.

3. Impact on EU bodies [++]

- The obligation to use SIENA as the preferred communication channel while putting Europol in copy when this concerns its mandate would **significantly** contribute to increase the quality and quantity of information shared with Europol via SIENA. It would also improve the security of information as compared to ad hoc exchanges of information.
- This would likely have a negative impact on Europol' workload.

4. Impact on fundamental rights [++]

- **Significant positive impact** through provisions aiming at improving the choice of the communication channel, thereby reducing the duplication of requests across several communication channels (clarify existing guidelines in a (binding) legal proposal, notably making of SIENA the preferred channel of communication for intra-EU cooperation). It would also improve accountability as compared to ad hoc exchanges of data.
- The use of different information channels in addition to SIENA does not ensure as efficiently as possible law enforcement processes. Thus, citizens may face undue processing time in case they are wrongfully subject to a criminal investigation. This option would partly address that. Law enforcement authorities will remain free to consider what types of information should be made available for possible exchange. They would not have additional capabilities in data processing.

5. Effectiveness in meeting the policy objectives [++]

- This policy option would **partly** address the objective of setting up a default communication channel for law enforcement exchange between Member States.

6. Efficiency in meeting the policy objectives [++]

- As option 3.1 + option 3.2 which would generate **cost** for a number of **Member States.**
- These costs would vary significantly depending on the effectiveness and efficiency of the SIENA access at

national level. This would essentially cover possible IT upgrades. • At the same time, under this policy option, Europol could more efficiently support Member States in preventing and combatting criminal offences, because of the economies of scale of performing such tasks at EU level. They don't outweight benefits.
7. Legal feasibility [++]
• This policy option would require legal changes. They would ensure the respect of the conferral of powers and of fundamental rights.
8. technical feasibility [++]
• Even though this policy option would be technically feasible, favouring the use of SIENA as channel of communication between Member States for offences falling within the Europol mandate would require the full roll-out of SIENA to all relevant end-users. • This would require significant technical and financial support.
9. Coherence with other measures [++]
• This policy option would **significantly** complement other Commission initiatives such as the Commission proposals for a new Schengen border code, for Prüm II and for Europol (see Schengen Strategy).

<u>Policy option 3.3:</u> obligation to use SIENA by default for all bilateral information exchange (unless otherwise regulated by EU law) + obligation to put Europol in copy when in cases within Europol's mandate, both after the end of a transition period and with Internal Security Fund support for the SIENA roll-out + new flanking soft measures (as in option 3.1)

Expected impact of policy option 3.3
1. Impact on citizens and businesses [+++]
• **Highly positive impact** to the security of the European citizens and societies. The obligation to use SIENA while copying Europol for offences within its mandate would **highly** support Member States to more effectively counter any forms of criminal offences.
2. Impact on national authorities [+++]
• **Highly positive impact** on national authorities, which could **highly** contribute to efficiently combat criminal offences, because of the obligation to use communication for the same purpose while putting Europol in copy when this concerns its mandate. • This would **fully** address the issue of duplication of requests through several communication channel.
3. Impact on EU bodies [+++]
• The obligation to use SIENA by default while copying Europol for offences within its mandate would **highly** contribute to increase the quality and quantity of information shared with Europol via SIENA. It would also improve the security of information as compared to ad hoc exchanges of information. • This would likely have a negative impact on Europol' workload.
4. Impact on fundamental rights [+++]
• **Highly positive impact** through provisions aiming at improving the choice of the communication channel, thereby ending the duplication of requests across several communication channels (clarify existing guidelines in a (binding) legal proposal). • The use of different information channels in addition to SIENA does not ensure as efficiently as possible law enforcement processes. Thus, citizens may face undue processing time in case they are wrongfully subject to a criminal investigation. This option would address that. They would not have additional capabilities in data processing. • Given the high level of security of SIENA, its use by default would more effectively and efficiently safeguard data protection. It would also improve accountability as compared to ad hoc exchanges of data.
5. Effectiveness in meeting the policy objectives [+++]
• **Highly positive impact.** This policy option would **fully address** the objective of setting up SIENA as default communication channel for law enforcement exchange between Member States for offences within Europol mandate.
6. Efficiency in meeting the policy objectives [++]
• Option 3.3 would **not** generate **additional cost** in comparison with **Option 3.2.** • At the same time, under this policy option, Europol could **highly efficiently** support Member States in preventing and combatting criminal offences, because of the economies of scale of performing such tasks at

EU level. They don't outweight benefits.
7. Legal feasibility [++]
• This policy option would require legal changes. They would ensure the respect of the conferral of powers and of fundamental rights.
8. technical feasibility [++]
• Even though this policy option would be technically feasible, making of SIENA channel of communication by default between Member States for offences falling within the Europol mandate would require first the full roll-out of SIENA to all relevant end-users. • This would require technical and financial support. • That is why such provision would only enter into force after a transition period allowing the SIENA full roll-out.
9. Coherence with other measures [+++]
• **Highly positive impact.** This policy option would **clearly** complement other Commission initiatives such as the Commission proposals for a new Schengen border code, for Prüm II and for Europol.

7. 7. HOW DO THE OPTIONS COMPARE?

7.1. Objective I: Facilitate equivalent access for law enforcement authorities to information held in another Member State, while complying with fundamental rights and data protection requirements

Comparative assessment for objective I			
	option 1.1	**option 1.2**	**option 1.3**
1. impact on citizens and businesses	+	++	+++
2. impact on national authorities	+	++	+++
3. impact on EU bodies	+	++	+++
4. impact on Fundamental Rights	n/a	n/a	++
5. effectiveness in meeting the policy objectives	+	++	+++
6. efficiency in meeting the policy objectives	++	++	++
7. legal feasibility	0	++	++
8. technical feasibility	+++	+++	+++
9. coherence with other measures	+	++	+++
Preferred policy option			**X**

The policy options are cumulative in the sense that policy option 1.2 builds on policy option 1.1, and policy option 1.3 builds on policy option 1.2.

Policy option 1.3 is the preferred option[99]. Under this policy option, not only the 2006 Swedish Framework Decision (SFD) will be aligned with the 2016 Data Protection Law Enforcement Directive (LED), but its use will be simplified. The data sets available for possible exchange will also be clarified. Furthermore, the revision of the deadline requirements, even when a judicial authority is involved, will improve the timely access to information. Flanking measures will be defined by a supporting informal expert group set up by the Commmission. This policy option will have a positive ripple effect on Schengen Associated Countries.

Indeed, as part of the online survey conducted within the framework of this study, almost all Heads of SPOCs of the EU Member States and Schengen Associated Countries confirmed that the existing barriers lead to increased time needed for investigations, as well as – in the worst case – discontinued investigations. Moreover, according to the survey respondents, delays were estimated to typically be of two to four weeks in almost half of the cases in which delays occurred. Even

[99] Additional information on the impacts of policy options on Member States can be found in annex 9.

longer delays were reported to be experienced in the largest part of the rest of the cases experiencing delays. Such delays are clearly hampering the efficient implementation of law enforcement operations in intra-EU cross-border cases.

Efficiency and effectiveness. Policy option 1.3 is more efficient and effective than the **policy options 1.1 and 1.2.** Limiting the revision of the SFD to a necessary alignment with the LED (baseline scenario) would represent a missed opportunity to also address additional well known issues hampering the full use of the SFD. Given the cumulative nature of these 3 options, options 1.2 (simplication in the use of the SFD) would significantly improve on option 1.1 while falling short of addressing the need for timely access to necessary information (option 1.3). These issues have been persistently noted in the Schengen evaluation country reports in the field of police cooperation. Council guidelines (non-binding) have not led to a necessary convergence of national practices (while recent Council Conclusions insisted on the need to support the "*development of smooth and swift information exchange*").

Under **policy option 1.1**, the identified uncertainties and inefficiencies in the intra-EU law enforcement cooperation, including the current incoherencies between different legislative instruments both at the EU level and between the Member States are expected to remain and eventually to increase.

Political feasibility. Policy option 1.3 is politically feasible. A number of Member States with a less efficient SPOC may express concerns at their ability to meet deadline requirements when the involvement of a judicial authority is required. For this reason, **policy options 2.1, 2.2 and 2.3** recommend (option 2.1) and require (option 2.2 and 2.3) the functional availability of a judicial authority, as it is already the case in more effective and efficient SPOCs (see options 2.2 and 2.3 below).

Coherence and proportionality. Policy option 1.3 is in full coherence with past and envisaged initiatives, notably the proposals on Europol, Prüm II and on the Schengen Border Code. **Policy option 1.3** is also **proportionate** to the identified problem and do not go beyond what is necessary to achieve the specific objective.

7.2. Objective II: Ensure that all Member States have an effective functioning Single Point of Contact (SPOC), including when a judicial authorisation is required to provide the data upon request of another Member State, and ensuring its effective cooperation with Police and Customs Cooperation Centres (PCCCs)

Comparative assessment for objective II			
	option 2.1	**option 2.2**	**option 2.3**
1. impact on citizens and businesses	+	++	+++
2. impact on national authorities	+	++	+++
3. impact on EU bodies	+	++	+++
4. impact on Fundamental Rights	+	++	+++
5. effectiveness in meeting the policy objectives	+	++	+++
6. efficiency in meeting the policy objectives	++	++	++
7. legal feasibility	0	++	-
8. technical feasibility	+	+	---
9. coherence with other measures	+	+++	+
Preferred policy option		**X**	

The policy options are partially cumulative in the sense that policy option 2.2 builds on policy option 2.1, and policy option 2.3 builds on policy option 2.2 **for the sole flanking soft measures.**

Policy option 2.2 is the preferred option[100]. Under this policy option, national and regional information hubs will benefit from the necessary approximation of commun minimum standards. This will cover the functionning, staffing, and IT information systems, while ensuring the interconnectivity between the national information management architecture with regional ones (if any). This will significantly improve the efficiency and effectiveness of these information hubs at national and regional levels (inter-agency cooperation) but also at EU level (cooperation between national SPOCs). This will also have a positive ripple effect on Schengen Associated Countries. Flanking measures will be defined and implemented to support Member States accordingly.

Under **policy options 2.2 and 2.3**, Member States will be required to monitor SIENA 24/7 and to ensure the functional availability of a judicial authority. This good practice, identified in a number of Member States, has been noted to significantly improve the SPOC ability to respond to urgent requests in a timely manner.

Efficiency and effectiveness. While some countries do not seem to work with a modern Case Management System (CMS) in relation to cross-border law enforcement cooperation, other countries have systems in place that are seamlessly interoperable and integrated with Europol SIENA. Thus, the measures identified in **policy option 2.2** are expected to contribute to level the playing field in terms of technical progress of law enforcement cooperation between countries and, thereby, facilitate the access to and exchange of information. The approximation of common minimum requirements will ensure coordinated future developments, thereby facilitating and enhancing internal and EU cooperation. Indeed, data can be exchanged in a more structured and swifter way (e.g. via the Universal Message Format).

A large majority of Member States participants to the 2nd technical workshop held in May 2021 indicated that the envisaged measures centred on national Case Management System for SPOCs would have a (very) positive impact on cross-border law enforcement cooperation[101].

Elements of the **policy option 2.1** (non-binding guidance) are expected to make a small positive contribution to improving the efficiency of cross-border law enforcement cooperation. **Yet,** this would not provide an adequate response from an efficiency perspective. Under **policy option 2.1,** the identified differences and inefficiencies in the functioning of SPOCs across the EU would remain, hampering the efficient exchange of information, notably due to an inadequate access to key databases and platforms in all SPOCs. The limited interconnectivity between different systems (e.g. due to vast differences between various 'in-house solutions' used in the EU), as well as the limited functionalities of the Case Management System (CMS) in various Member States are also expected to remain and continue to hamper cross-border information exchange in the future.

The plethora of existing databases, channels and systems, as well as the extent to which and how they are used in practice by officials is expected to continue to hamper the efficiency of law enforcement cooperation in the EU. Fragmentation concerning the associated legal, technical and structural requirements at the EU and national levels, as well as established informal practices are expected to continue to be the main reasons for this.

Moreover, some SPOCs have insufficient resources to address the information requests received within the deadlines in all cases. There is also a need to further ensure that law enforcement authorities involved in intra-EU cross-border cases are better trained on recent developments and possess adequate language skills to communicate with their peers. Whilst it remains possible that the SPOCs and PCCCs will over time incrementally update and improve their information management systems, these developments would not be aligned between the Member States and the current barriers are expected to remain.

[100] Additional information on the impacts of policy options on Member States can be found in annex 9.
[101] See complementary information in annex 10.

Political feasibility. Unlike policy option 2.3, **policy option 2.2** is politically feasible. The lack of effective and efficient functioning of national and regional information hubs (where they exist) have been persistently noted in the Schengen evaluation country reports in the field of police cooperation. Council guidelines (non-binding) have not led to a necessary minimal convergence of national practices (while recent Council Conclusions insisted on the need to support the "*further development of relevant structures and platforms*").

This approximation of common minimum standard, notably stemming from the Heads of SPOC network[102], express a wide consensus at expert level. Ensuring the harmonisation of rules (option 2.3) on issues not covered by EU provisions so far will not be supported by Member States given their far-reaching structural and financial implications.

Coherence and proportionality. Policy option 2.2 is in full coherence with past and envisaged initiatives notably the proposals on Europol, Prüm II and on the Schengen Border Code. **Policy option 2.2** is also **proportionate** to the identified problem and do not go beyond what is necessary to achieve the specific objective.

A full harmonisation of rules **(option 2.3)** do not meet the **proportionality test**. Indeed, passing from Council non-binding guidance to a fully-fledged harmonisation by EU law would not be feasible given the major technical, legal and financial implications. The approximation of core minimum standards is considered less invasive while still being conducive to achieving the objective II.

7.3. Objective III: To remedy the proliferation of communication channels used for law enforcement information exchange between Member States while empowering Europol as the EU criminal information hub for offences falling within its mandate (unless otherwise regulated by EU law)

Comparative assessment for objective III			
	option 3.1	**option 3.2**	**option 3.3**
1. impact on citizens and businesses	+	++	+++
2. impact on national authorities	+	++	+++
3. impact on EU bodies	+	++	+++
4. impact on Fundamental Rights	+	++	+++
5. effectiveness in meeting the policy objectives	+	++	+++
6. efficiency in meeting the policy objectives	++	++	++
7. legal feasibility	0	++	++
8. technical feasibility	+++	++	++
9. coherence with other measures	+	++	+++
Preferred policy option			**X**

The policy options are partially cumulative in the sense that policy option 3.2 builds on policy option 3.1, and policy option 3.3 builds on policy options 3.2 **for the sole flanking soft measures.**

Policy option 3.3 is the preferred option[103]. Under this policy option, Member States will be required to exchange information between them via SIENA (unless otherwise regulated by EU law) while putting Europol in copy when this concerns an offence within Europol's mandate. Such

[102] Council Conclusions 12825/19, 8.10.2019 on *establishing European network of Heads of SPOC for international law enforcement information exchange*.
[103] Additional information on the impacts of policy options on Member States can be found in annex 9.

requirement will only enter into force after a necessary transition period ensuring the full roll-out of SIENA at national level. This will also have a positive ripple effect on Schengen Associated Countries.

Flanking soft measures will be defined and implemented to support Member States accordingly. Compared to the status quo, where Member States use different communication channels and often do not involve Europol in their bilateral exchanges, this will also significantly increase the amount of information that Member States will share with Europol on cross-border crime, and hence close an important information gap.

The main difference between **policy option 3.2 and 3.3** lies in SIENA being the "preferred" channel of communication, thereby still leaving room for Member States not to implement this option if they so decide, and SIENA being the channel of communication "by default" for intra-EU communication.

Policy option 3.2 will still allow Member States leeway in the choice of the communication channel in predefined cases, thereby promoting the use of Europol SIENA as the preferred channel of communication where relevant. The **policy option 3.2** will thus seek to clarify existing Council guidelines on the choice of the appropriate channel in a (binding) legal text. **Policy option 3.3** ensures a more coherent approach, one giving the Europol channel a central role. Member States could still be allowed to use an alternative channel in exceptional circumstances (to be understood restrictively).

Efficiency and effectiveness. One result of Member States having a free choice of channel (apart from the legal requirements relating to SIRENE Bureaux and Europol National Units) is that they use different channels to different extents also depending from officers' habits and personal preferences. Some Member States have moved towards more systematic use of the Europol channel (SIENA). Others continue to rely a good deal on the INTERPOL channel.

It is important to note that the Member States have divergent views in relation to the use of SIENA as default channel of communication. Some Member States have pointed out that it is important for their own purposes to be able to decide based on the case at hand in a rather flexible manner via which channel information should be exchanged. For instance, it is not always clear in practice to determine whether a specific case is only related to the EU or also has an international component. In such a case, making SIENA the default channel via which information is exchanged may lead to double work if the case turns out to be of international nature in relation to which INTERPOL I24/7 should rather have been used.

However, the choice of the Europol channel (SIENA) is justified by its advantages. SIENA can be used for direct bilateral exchanges, but also facilitates sharing of information with Europol in line with legal requirements of the Europol Regulation and the Swedish Framework Decision. SIENA messages are structured, can handle large data volumes and are exchanged with a high level of data protection and security. The Europol Liaison Officers community is an additional benefit as they can be asked to intervene where necessary to facilitate the understanding and effectiveness of information exchange.

Europol indicated that the definition of SIENA as the default channel (while putting Europol in copy) instead of as a preferred channel **(policy option 3.2)** is in particular expected to further facilitate the access to and exchange of information and, inevitably, lead to a strong increase of the number of messages exchanged via SIENA. The yearly number of messages exchanged via SIENA is estimated to increase to up to 3.86 million messages in 2030 (against 1.3 million in 2020).

Option 3.1 is expected to, one the one hand, have a small positive impact as regards the achievement of this objective, since Europol is expected to make further improvements to SIENA, potentially doubling the number of users.

However, the extent to which the potential efficiency gains may actually materialise largely depends on Member States' commitment to the improvement of law enforcement cooperation and their willingness to implement (common) changes within their national systems. The current differences between the national set-ups are expected to continue to exist and hamper the level playing field between Member States. Member States will remain free **not** to put Europol in copy of their exchanges via SIENA even when concerning offences falling into the agency' mandate.

Under **policy option 3.1**, the identified uncertainties and inefficiencies in the intra-EU law enforcement cooperation, including the current duplication of requests in various communication channels both at the EU level and between the Member States are expected to remain and eventually to increase, causing undue delays and additional workload.

For example, the practice of 'fishing' is likely to remain, meaning that a number of Member States or national LEAs may receive the same information request without any clear link to a specific case, thus leading to duplication of work. Therefore, it is expected that the efficiency of future law enforcement cooperation will considerably lag behind its potential.

Political feasibility. A number of Member States favours an approach that leaves wide flexibility to use different channels. While considered politically feasible[104], the **policy option 3.3** is likely to be closely analysed by the Member States.

Coherence and proportionality. While possibly more readily acceptable by a number of Member States, the **policy option 3.2** is considered to be only partially **coherent** with other EU measures, notably the Europol Regulation and **Council Document 5503/21**[105] on the use of SIENA as a primary communication channel. Because the policy option 3.2 will leave Member States more leeway, it is considered to falling short of the necessity requirement, while **policy option 3.3** is considered **proportionate** to the identified problem and do not go beyond what is necessary to achieve the specific objective.

Policy option 3.3 is fully in line with a decade-long political commitment to make of Europol the "*hub for information exchange between the law enforcement authorities of the Member States, a service provider and a platform for law enforcement services*"[106].

In coherence with this 2009 European Council strategic guidance, a 2021 Council Presidency Document also states: "*applying SIENA as the default communication channel would add to the streamlining of law enforcement information exchange, and increase the level of security in the context of police cooperation in the Union. By the same token, it would enable that efforts be focused on the development of a single instead of numerous solutions, thus fostering the objective of reaching enhanced EU internal security*"[107].

8. 8. PREFERRED POLICY OPTION: A GAME CHANGER FOR LAW ENFORCEMENT COOPERATION

Options 1.3, 2.2 and 3.3 form the preferred option.

[104] Based on the Study' findings: If SIENA was established as the preferred/default channel for information exchange, this would imply changes for **4 countries who currently prefer the I-24/7 channel**. For those 17 countries which are indifferent between communication channels establishing SIENA as the preferred/default channel would imply smaller changes as for those who clearly prefer the I-24/7. For 5 countries which use SIENA as the preferred communication channel, no change is expected.

[105] Council Document 5503/21, *Secure communication channel in law enforcement cooperation – SIENA.*

[106] European Council, "The Stockholm Programme", OJ C 115, 4.5.2010, p. 1–38. The European Council also invited the Commission to "*examine how it could be ensured that Europol receives information from Member States law enforcement authorities so that the Member States can make full use of Europol capacities*".

[107] Council Document 5503/21, 28.1.2021, *Secure communication channel in law enforcement cooperation – SIENA.*

Taken together, the preferred policy option will streamline, clarify, develop and modernise cross-border law enforcement cooperation while better safeguarding Fundamental Rights. It will also step up Europol support to Member States in countering evolving threats. The preferred policy option, a game changer, will ensure a strong convergence of national practices regarding the effective and efficient functionning of SPOC, through common minimum standards.

This choice reflects the best cumulative score of these options as regards to relevance, added value, effectiveness, efficiency, coherence and proportionality. It draws the lessons from the past and, at the same time, is sufficiently ambitious. The approximation of common minimum (ambitious) standards will ensure a sufficient degree of convergence of national practices and ultimately deliver effective and efficient information flows. It respects the views of the Member States concerning the role of information exchange in addressing criminal offences while at the same time respecting also the legitimate expectations of the EU citizens and businesses as to contribute to the effective and efficient safeguard of the Schengen area as one of the main enablers of the freedom of movement of persons and goods[108].

8.1. Overview of the preferred policy option

specific objectives	preferred policy options
Objective I: Facilitate equivalent access for law enforcement authorities to information held in another Member State, while complying with fundamental rights and data protection requirements	***Policy option 1.3:*** Option 1.2 + provisions ensuring compliance with **deadlines requirements** by which data is to be made available to another Member State **(including when a judicial authorisation is required)**
Objective II: Ensure that all Member States have an effective functioning Single Point of Contact (SPOC), including when a judicial authorisation is required to provide the data upon request of another Member State, and ensuring its effective cooperation with Police and Customs Cooperation Centres (PCCCs)	***Policy option 2.2: Approximation of minimum standards*** **on** the composition of **the Single Points of Contact** (including when a judicial authorisation is required), its functions, staffing and IT systems, and its cooperation with regional structures such as **Police and Customs Cooperation Centres +** new flanking soft measures (training, financial support, Commission guidance)
Objective III: To remedy the proliferation of communication channels used for law enforcement information exchange between Member States while empowering Europol as the EU criminal information hub for offences falling within its mandate (unless otherwise regulated by EU law)	***Policy option 3.3:*** **obligation to use SIENA by default** for all bilateral information exchange (unless otherwise regulated by EU law) **+ obligation to put Europol in copy** when in cases within Europol's mandate, both after the end of a **transition period and with Internal Security Fund support** for the SIENA roll-out+ new flanking soft measures (training, financial support)

The most positive **cumulated** impacts of the preferred policy option are expected to stem from establishing the SPOC as a "one stop shop" for law enforcement cooperation in all Member States. Additionally:

- The requirement to have full access to EU and international law enforcement databases (e.g. by involving staff in the SPOC who have full access) will constitute a key step forward, as the current uneven access to relevant databases by the SPOCs have a negative impact on the speed to which information can be exchanged.
- The requirement to have a judicial authority functionally available will imply that those cases where a judicial authorisation is required can be handled more swiftly than what is currently the case, meaning that deadlines can be more readily met also in these cases. At present, deadlines are almost always exceeded when a judicial authorisation is required.
- The requirement for the SPOC to be, at the minimum, informed about all international law enforcement cooperation requests dealt with at national level will lead to better (statistical) information concerning the information exchanges and thus constitute an important basis for

[108] See Complementary information on political feasibility in annex 10.

better informed future action. It will also mean that the SPOC will have better possibilities to assist with information exchanges.

- The requirement to set up a Case Management System (CMS) with common minimum features at SPOC and ensure its interconnection with the PCCCs' CMSs, will significantly improve both the efficiency and effectiveness of national, regional and EU level inter-agency cooperation.
- The establishment of Europol SIENA as the default (rather than the preferred) channel of communication will add to the streamlining of law enforcement information exchange.
- A key enabler to achieve the specific objectives is the establishment of appropriate training and financial support.

The consultation process revealed some political red lines for Member States. If the preferred options took note of them, the main reason for excluding a full harmonisation of the functioning of the SPOC by means of a Regulation stems, first and foremost, from the wide divergence of practices, legal traditions and existing set up in place at national level. The policy options would have therefore remained the same irrespective of their **political feasibility**.

Ensuring the harmonisation of rules (Regulation) through a detailed check list of necessary features (option 2.3) on issues not covered by EU provisions so far will not be supported by Member States given their far-reaching structural and financial implications. Such harmonisation may also be considered going beyond would be strictly necessary to achieve the main goal of this initiative. It would thus not pass the proportionality, necessity and subsidiarity tests.

Even though the political feasibility of new measures in the area of law enforcement cooperation is generally challenging, the preferred policy responds to calls for actions from the co-legislators. It will notably meet the objectives of the Council Conclusions of November 2020[109] calling on:

- the Member States to: "*take all necessary steps to further strengthen operational cross-border law enforcement cooperation by effectively implementing existing instruments and, where appropriate and necessary, by consolidating, simplifying and extending the legal foundations [and] swiftly improve means for regular or ad hoc exchange of information*".
- The Commission to support: "*the development of smooth and swift information exchange, further development of relevant structures and platforms; to consider consolidating the EU legal framework to further strengthen cross-border law enforcement cooperation*" [and]
- "*to duly take into account – when assessing options for a proposal for a European Police Cooperation Code and while upholding the principle of national sovereignty, the existing standards for the protection of fundamental rights, existing legal systems in Member States and the decisive role of the host state – the value and success of local, regional, bi- and multilateral law enforcement cooperation between Member States".*

Stakeholders' high-level support for the policy options

Stakeholders in the Member States	Public authorities					NGOs & civil society
	Law Enforcement Authorities			Judicial Authorit	Data Protect. Authorit	
Topics	SPOCs	PCCCs	Other			
Overarching topics						
Access to and exchange of information						
Specific topics						
Legislative improvements						

[109] Council Document 13083/1/20, *Council Conclusions on Internal Security and European Police Partnership,* link

Stakeholders in the Member States / Topics	Public authorities					NGOs & civil society
	Law Enforcement Authorities			Judicial Authorit	Data Protect. Authorit	
	SPOCs	PCCCs	Other			
Provision of clarifications						
Introduction of new requirements						
Streamlining of existing requirements						
Alignment of different legal instruments						
Technical improvements						
Definition of technical requirements & functionalities						
Establishment of quality control mechanisms						
Structural improvements						
Establishment of organisational requirements						
Establishment of governance requirements						
Other improvements						
Provision of training						
Provision of awareness raising						
Provision of funding						

Source: EY/RAND Europe Study's elaboration

Cells that are marked in darker green denote a stronger positive impact on the different types of stakeholders. This table is not based on official positions provided by the Member States.

Based on the study' findings and initial feedback at political level[110], there is a general trend towards high-level support among stakeholders. Law Enforcement Authorities (LEAs) seem to be more supportive of the elements of the policy options than judicial authorities. With specific regard to data protection authorities, it is crucial to note that the support is contingent on the extent to which the protection of personal data is safeguarded throughout all measures foreseen under the policy options.

Generally spoken, Non-Governmental Organisations and civil society organisations are supportive of the policy options as long as fundamental rights are safeguarded, and LEAs do not come into the possession of excessive, unjustified amounts of information about citizens and businesses that do not concern actual criminal investigations and/or legal proceedings before Court.

The preferred policy option is also coherent with:

- the **EU Security Union Strategy for the period 2020 to 2025**[111], which points to the need to improve intra-EU operational law enforcement cooperation;
- the **Counter-Terrorism Agenda**[112], which calls for a more effective interoperability of EU information;
- the **EU Strategy to tackle organised Crime 2021-2025**[113], which is focused on boosting law enforcement and judicial cooperation;
- the new **Schengen strategy**[114], which points to the need for police officers to cooperate effectively and by default across Europe;
- the 2020 **Council Conclusions on Internal Security and European Police Partnership**[115], which calls for the consolidation and improvement of available law enforcement instruments;

[110] Informal Council COSI meeting of 7-8 July 2021.
[111] Commission (2020), *EU security union strategy* - COM/2020/605 final, link.
[112] Commission (2020) *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond,* link.
[113] Commission (2020) *A EU Strategy to tackle organised Crime 2021-2025,* link.
[114] Commission (2021), COM(2021) 277 final, *A strategy towards a fully functioning and resilient Schengen area.*
[115] Council Document 13083/1/20, *Council Conclusions on Internal Security and European Police Partnership,* link.

- the **Commission Recommendation (EU) 2017/820**[116], which invites Member States to strengthen cross-border police cooperation;
- the **Commission Staff Working Document SWD/2020/327 final**[117], which highlights the need to address the deficiencies and the recurrent issues affecting law enforcement cooperation, and;
- the **Council Document 5503/21**[118] on the use of SIENA as a primary communication channel.

The high-level issues and core problems stemming from them as well as their likely future development are addressed by the preferred policy option in line with the **subsidiarity** and **proportionality** principles.

8.2. Preferred policy option cumulated advantages and disadvantages

Main advantages	Main disadvantages
• Expected to facilitate to a large extent the swift exchange of data via one main channel and, thus in turn contribute to the ability to more effectively fight SOC. • Establishes a level playing field between countries from a technical perspective by introducing common functional requirements for CMS and ensures that countries adequately reflect the practical importance of SPOCs and PCCCs within their national set-ups. • Has a large positive impact on increasing the coherence of the legislative framework at both the EU and national levels. • The policy option is expected to contribute in a largely positive way to safeguarding fundamental rights.	• Necessitates investments, including for IT-and staff-related investments at both the EU and national levels. • Increases need for training of officials.

Overall, it is expected that the preferred policy option will have a very significant impact on the **effectiveness** of EU cross-border law enforcement cooperation. The preferred policy option will contribute to **efficiently** reduce specific types of **costs** related to law enforcement cooperation, while at the same time contribute to increasing others.

It can be expected that different Member States will be affected by reduced/increased costs to varying degrees depending on how much aligned their current national set-up already is with the measures envisaged under the preferred policy option. However, **reliable quantitative data on costs are largely missing**[119].

8.3. Main types of costs expected to be reduced/increased with the preferred policy option

Main types of costs increased	Main types of costs decreased
To ensure the efficient access to and exchange of necessary information among law enforcement authorities in an intra-EU context	
EU level: • EU funding (e.g. through Internal Security Fund) and financial support, as well as budget for procuring studies. • Costs in relation to awareness raising and training (incl. by CEPOL).	*EU level:* • n/a *Member State level:* • Reduced working time due to better information to act on (solving cases instead of managing them). • Reduced waiting time / time delays (e.g. due to waiting for information from LEAs in other countries).

[116] Commission Recommendation (EU) 2017/820 of 12 May 2017 on proportionate police checks and police cooperation in the Schengen area. Available at: link.
[117] Commission Staff Working Document on the Functioning of the Schengen Evaluation and Monitoring Mechanism SWD/2020/327 final. Available at: link.
[118] Council Document 5503/21, 28.1.2021, *Secure communication channel in law enforcement cooperation – SIENA*.
[119] Complementary information can be found in Annex 3.

Main types of costs increased	Main types of costs decreased
Member State level: • Necessitates investments at MS level, including for IT- and staff-related investments. • Increased budgetary spending by MS on officers' training.	• Less time needed for case management. • Fewer resources needed for case management, i.e. more resources spent on "solving cases".

While highly depending from the specificities of each national IT set-up and legal parameters, an estimation of possible costs has been provided by Europol. These costs, deemed acceptable, are **proportionate** to the identified problem and do not go beyond what is necessary to achieve the specific objective (see below). The Annex 3 provide further details on the methodology issues to estimate anticipated costs. Given the lack of data, these costs are considered **rough estimations**.

The costs associated with the development of SIENA and CMS

The direct operational costs for SIENA are 1 to 1,2 million EUR per year. This figure does not factor in hardware, helpdesk, infrastructure, business product management activities, training, etc. However, these items could be estimated at around 0,5 million in addition.

For a CMS, an estimation of costs is difficult, as they are largely depending on system complexity, number of users, functionalities, licenses, infrastructure, etc. However, it can be estimated that, without infrastructure and hardware costs, the respective costs should be at least 150,000 EUR.

The assumptions above are also presented in the following table.

Estimation of costs for SIENA and CMS[120]

MS package estimate[121]			
CMS for 10 MS	10 x 150.000	EUR 1,5 million	***Total***: EUR 2,5 million (one-time investment needed)
SIENA integration in CMS for 20 MS	20 x 50.000	EUR 1 million	

Source: Data provided by Europol

Based on the estimation above, the set-up of Case Management Systems and their SIENA integration in **PCCCs** not yet equipped could possibly cost **EUR 9 million** (one-off).

This cost is broken down as follow:

- Out of the 59 identified PCCCs, 14 are already connected to SIENA;
- The SIENA connection to a possible maximum of 45 PCCCs would cost EUR 2,250 million (45x EUR 50.000);
- The set-up of CMSs in a maximum of 45 PCCCs would cost EUR 6,750 million (45x EUR 150.000);
- Hence a total of EUR 9 million (2,250 + EUR 6,750 million) for PCCCs;
- This would be considered as a maximum one-off cost given that a number of PCCCs are already connected to the SPOC CMS. Hence the SIENA integration in the SPOC CMS would de facto cover the SIENA integration in the connected PCCCs.

The necessary IT upgrades in both SPOCs and PCCCs could thus amount to a maximum one-off grand total of **EUR 11,5 million** (2.5 + 9 million).

These costs (one-off investment), deemed acceptable, are **proportionate** to the identified problem and do not go beyond what is necessary to achieve the specific objective. As Member States are in any case pursuing a modernisation of their IT systems (also in the context of the interoperability of

[120] Respectively only 10 and 20 Member States would be considered here (other Member States being adequately equipped).

[121] The information provided should be used carefully. It should be understood as "in case a CMS is needed for 10 Member States, then costs would be…" and "in case SIENA would need to be integrated into the CMS in 20 Member States, the costs would be…" etc. Thus, the table does not provide actual costs but rather refers to actual costs under specific circumstances.

EU information systems), this provides a good opportunity for cost effective implementation of the envisaged changes. These costs do not cover training needs. As for IT upgrades, the training costs are highly depending from the specificities of each national IT set-up and legal parameters.

The costs at national level should be covered by Member States' programmes under the Internal Security Fund.[122] The Internal Security Fund includes the specific objective to "improve and facilitate the exchange of information" and to "improve and intensify cross-border cooperation".[123] When preparing their national programmes, Member States are invited to include in their national programmes activities relevant to the upcoming Police Cooperation Code, with explicit reference to SPOCS and PCCCs, and the connection to SIENA.

With a view to maximising the main advantages of the preferred policy option, and to minimise the main disadvantages to the extent possible, various success factors have been identified:

- Provide sufficient funding and financial support to Member States in order to facilitate high-level political support for the preferred policy option, as well as to ensure the necessary financial commitment;
- Leverage and streamline existing IT-solutions (e.g. developed by Europol) in order to avoid Member States diverging at the technical level;
- Provide sufficient funding and co-develop awareness raising campaigns targeted at EU law enforcement officials in relation to cross-border matters;
- Provide sufficient funding and co-develop specific training relevant for the subject matter covered by the preferred policy option and leverage existing training opportunities provided by CEPOL;
- Closely collaborate with Member States in order to take advantage of proven operational practices;
- Take appropriate action in unison with the Member States in order to identify and streamline good practices concerning the implementation of the preferred policy option; and
- Continuously collect relevant statistics and monitor the implementation of the preferred policy option to enable swift action in case diverging implementation practices occur.

9. 9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

The evaluation of impacts will depend on the information to be received from the Member States. For this reason, the Directive Proposal would contain **provisions on collection of data indicators** on the quantity of information requested, sent, received; the number of urgent requests, the number of urgent requests replied on time and a breakdown by communication channels at SPOC, at PCCCs (if any) and at any other equivalent structures.

The responsibility for the collection of the relevant monitoring data should be in the hands of national authorities. The development of a modern information management architecture, as per the Directive proposal, will greatly facilitate the data collection exercise at no additional cost by the SPOCs.

Subsequently, the monitoring of these activity indicators will be used to inform on the application of the Directive proposal. **Three** and five **years** after the transpositon deadline, , the Commission intends to submit to the European Parliament and the Council two reports. **The first,** assessing the extent to which the Member States have taken the necessary measures to comply with this

[122] Regulation (EU) 2021/1149.
[123] See Articles 3(2)(a) and (b) of Regulation (EU) 2021/1149.

Directive; **the second,** assessing its results against its objectives and the continuing validity of the underlying rationale and any implications for future options.

Aside from this legal proposal, the Commission, acting by virtue of its administrative autonomy, will set up an expert group composed by experts from each Member State, to advise and support the Commission in the monitoring and application of the Directive, including in the preparation of Commission guidance papers.

Main indicators for the monitoring of the preferred policy option contained in the Directive proposal

	Implementation ("outputs")	**Application ("results & impacts")**
Timely access to and smooth exchange of information	• Number of non-urgent/urgent messages sent/received, refused/accepted, fully/partially answered • Number of cases initiated/closed • Number of staff in SPOCs/PCCCs • Number of requests from non-proprietary CMS/databases • Capital/operational expenditures, e.g. in relation to IT and training	• Level of security in the EU • Number of interactions (in-) directly leading to positive outcomes[124] • Level of awareness and knowledge among officials • Degree of smoothness of law enforcement cooperation

ANNEX 1: PROCEDURAL INFORMATION

1. LEAD DG, DECIDE PLANNING/CWP REFERENCES

The lead DG is the Directorate-General for Migration and Home Affairs (DG HOME). The agenda planning reference is PLAN/2020/8314 - HOME - EU police cooperation.

The Commission Work Programme for 2021 announced a legislative initiative to "modernise existing intra-EU law enforcement cooperation by creating an EU police cooperation code[125].

2. ORGANISATION AND TIMING

The inception impact assessment was published on 28 September 2020[126] and open for feedback for a period of 8 weeks, until 16 November 2021[127].

[124] Depending on the type of case, this could mean e.g. apprehensions and arrests.
[125] COM(2020) 690 final, (19.10.2020), https://ec.europa.eu/info/publications/2021-commission-work-programme-key-documents_en

An Inter-Service Sterring Group (ISSG), composed of representatives from SG, SJ, HOME, JUST, TAXUD and OLAF was set up. The ISSG met four times:

- Comment on and validation of the **Terms of Reference for the Study** underpinning this Impact Assessment and **Consultation strategy**, 30 October 2020;
- Comment on and validation of the Study' **Inception Report**, 17 February 2021;
- Comment on and validation of the Study' **Interim Report**, 29 April 2021;
- Comment on and validation of the Study' **Final Report**, 21 June 2021.

The Inter-service Group on the Security Union discussed a draft text of the impact assessment on 9 July 2021. It was composed of representatives from SG, SJ, HOME, JUST, TAXUD, BUDG, EAC, CNECT, NEAR, MOVE, ECHO, ENV, EMPL, ENER, DEFIS, DIGIT, FISAM, FPI, GROW, HR, RTD, SANTE, TRADE, INPTA, REGIO, MARE, CERT-EU, ESTAT, JRC OLAF, EEAS.

The comments made by the ISG were integrated in the draft Impact Assessment.

3. CONSULTATION OF THE RSB

On 19 August 2021, the Directorate-General for Migration and Home Affairs submitted the draft impact assessment to the Regulatory Scrutiny Board, in view of a hearing that took place on 22 September 2021.

The opinion of the Regulatory Scrutiny Board was positive[128]. The following comments were made:

Comments made by the RSB	Amendments following RSB comments
The report should clarify how the initiative will articulate with the Automated Data Exchange Mechanism for Police Cooperation (Prüm II) and the Convention Implementing the Schengen Agreement (CISA). It should also clarify that the initiative aims to propose a Directive to update and replace the pre-Lisbon Swedish Framework Directive (adopted by both the Council and the European Parliament in the ordinary legislative procedure)	This was ensured accordingly, see: - added rationale on Prüm II p. 6. - added rationale on CISA p.10 (footnote 24) and p.11.
The problem analysis should be reinforced with anonymised evidence from the Schengen evaluation reports. The report should also explain why Member States do not or cannot address certain shortcomings themselves, e.g. ill-equipped national authorities, lack of common binding procedures	This was ensured accordingly, see: - added tables p. 12, 15, 17. - added boxes p. 15, 16, 18. - added rationale p. 20-21.
Regarding personal data protection, the report should explain how the alignment with the 2016 Law Enforcement Data Protection Directive will provide the required level of data protection in the Union	This was ensured accordingly, see: - added rationale p. 31-32.
The political feasibility of the policy options should not determine their substantive assessment but rather be considered when comparing options. The criteria of legal and technical feasibility should be used to screen the options to be retained for further in-depth analysis. Only feasible options should be kept. Any difference in terms of their performance should then be reflected via the standard assessment criteria of effectiveness, efficiency and coherence. The Board notes the estimated costs	This was ensured accordingly, see: - amended tables pp. 34 to 44, p. 46. - added rationale pp. 27-28, p. 50.

[126] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12614-EU-police-cooperation
[127] EU police cooperation code – tackling cross-border serious & organised crime (europa.eu)
[128] Ref. Ares(2021)58622323 – 27/09/2021.

and benefits of the preferred option in this initiative, as summarised in the attached quantification tables. Some more technical comments have been sent directly to the author DG.	

4. EVIDENCE, SOURCES AND QUALITY

The impact assessment is notably based on the stakeholder consultation (see annex 2). The Commission applied a variety of methods and forms of consultation, ranging from consultation on the Inception Impact Assessment, which sought views from all interested parties, to targeted stakeholders' consultation by way of a questionnaire, experts' interviews and targeted thematic stakeholder workshops, which focused on subject matter experts, including practitioners at national level. Taking into account the technicalities and specificities of the subject, the Commission emphasised in targeted consultations, addressing a broad range of stakeholders, at national and EU level.

In this context, the Commission also took into account the findings of the "*Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation*", which was commissioned by DG HOME and developed by the contractor based on desk research and the following stakeholder consultation methods: scoping interviews, questionnaire and online survey, semi-structured interviews, case-studies and two online workshops (see annex 2).

ANNEX 2: STAKEHOLDER CONSULTATION

This annex provides a synopsis report of all stakeholder consultation activities undertaken in the context of this impact assessment.

1. CONSULTATION STRATEGY

The aim of the consultation was to receive relevant input from stakeholders to enable an evidence-based preparation of the future Commission initiative on a improving law enforcement cooperation between Member States.

The stakeholders' consultation took place between September 2020 and July 2021 and encompassed, primarily, targeted stakeholders by way of the Study and two workshops hosted by the Commission with Member States and Schengen Associated Countries' representatives.

To do this, the Commission services identified relevant stakeholders and consulted them throughout the development of its draft proposal. The Commission services sought views from a wide range of subject matter experts, national authorities, civil society organisations, and from members of the public on their expectations and concerns relating to strengenting law enforcement cooperation in the EU.

During the consultation process, the Commission services applied a variety of methods and forms of consultation. They included:

- the consultation on the Inception Impact Assessment, which sought views from all interested parties;
- targeted stakeholder consultation by way of a questionnaire;
- expert interviews; and
- targeted thematic stakeholder workshops that focused on subject matter experts, including practitioners at national level. Taking into account the technicalities and specificities of the subject, the Commission services focused on targeted consultations, addressing a broad range of stakeholders at national and EU level.

The Commission also took into account the findings of the "*Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation*", which was commissioned by DG HOME and developed by the contractor based on desk research and the following stakeholder consultation methods: scoping interviews, questionnaire and online survey, semi-structured interviews, case-studies and two online workshops.

The aforementioned diversity of perspectives proved valuable in supporting the Commission to ensure that its proposal address the needs, and took account of the concerns, of a wide range of stakeholders. Moreover, it allowed the Commission to gather necessary data, facts and views on the relevance, effectiveness, efficiency, coherence and EU added value of the proposal.

Taking into consideration the Covid-19 pandemic and the related restrictions and inability to interact with relevant stakeholders in physical settings, the consultation activities focused on applicable alternatives such as online surveys, semi-structured phone interviews, as well as meetings via video conference.

A public consultation as part of our consultation strategy for the new legislative proposal was carried out.

2. CONSULTATION ACTIVITIES (SUMMARY)

2.1. Feedback on the Inception Impact Assessment

A call for feedback, seeking views from any interested stakeholders, on the basis of the Inception Impact Assessment was organised from 28 September to 16 November 2020. The consultation, sought feedback from public authorities, businesses, civil society organisations and the public, was open for response from 4 May 2020 to 09 July 2020. Participants of the consultation were able to provide online comments and submit short position papers, if they wished, to provide more background on their views. **4 contributions** were received[129]. They were integrated as part of the study' findings.

2.2. Consultations that took place during the study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation

The Commission contracted an external consultant to conduct a study. It took place from January to August 2021. It involved desk research, and stakeholder consultations by way of scoping interviews, targeted questionnaires, a survey, semi-structured interviews, case-studies, a public consultation and two *ad hoc* workshops.

2.3.1. Feedback on the public consultation

The public consultation was carried out from 19 April to 14 June 2021. **20 contributions** were received[130]. They were integrated as part of the study' findings.

2.3.2. Targeted consultation by way of a questionnaire

An online survey in the form of questionnaires made accessible to targeted stakeholders via the EUSurvey[131] tool was also held as part of the Study. The objective of this consultation was to receive feedback, comments and observations on the challenges identified for the legal proposal. The questionnaires were tailored to different stakeholders.

239 contributions were received. They served as foundation for the study' findings.

2.3.3. Member State experts' consultation by way of meetings

In the course of the consultation undertaken as part of the Study, the contractor organised two workshops held on 24 March and 25 May 2021 to which representatives of the Member States, Council Secretariat and Commission were invited[132].

Ad hoc workshop of 24 March 2021

On 24 March 2021, the contractor organised an ad hoc workshop. The objective was to have an exchange of views with and between Member States and Schengen associated countries on their current challenges when engaging in cross-border law enforcement cooperation.

The 27 Member States, 3 Schengen associated countries, the European Anti-Fraud Office (OLAF) and Commission Directorate-Generals participated in the workshop.

Ad hoc workshop of 25 May 2021

[129] EU police cooperation code – tackling cross-border serious & organised crime (europa.eu)
[130] See the results' analysis in Annex 2.
[131]
[132] See summaries of the meetings in Annex 8.

On 25 May 2021, the contractor organised an ad hoc workshop. The objective was to have an exchange of views with and between Member States and Schengen associated countries on possible options addressing identified challenges and their respective impacts.

Council working groups

The Commission also made use of the Law Enforcement Working Party (LEWP)[133] meetings of 22 February and 16 March 2021 to brief Member States on its preparatory work and relevant technical deliberations, in the context of strengthening law enforcement cooperation, and explore Member States' views on the problems and potential solutions. The same was done at the Customs Cooperation Working Party (CCWP)[134] of 23 March 2021.

Head of Single Point Of Contact (SPOC) meeting of 26 May 2021

On 26 May 2021, the contractor presented the findings from the questionnaire sent to national Single Point of Contact (SPOC) with a view to gather additional opinions and rationale.

2.3.4. Semi-structured interviews

The consultation conducted as per the Study, included targeted bilateral and multilateral semi-structured interviews with stakeholders on the basis of formalised and open-ended questions allowing for open and in depth discussions. These interviews were conducted from March to June 2020 via teleconferencing. They included in particular relevant EU agencies, services and Commission Directorates-general, national experts and academics.

3. STAKEHOLDER PARTICIPATION

Stakeholders consulted[135] included:

- EU institutions, agencies and bodies;
- law enforcement authorities in the Member States (e.g. police, customs);
- judicial authorities in the Member States;
- data protection authorities;
- non-governmental organisation, academias, civil society.

The feedback on the Inception Impact Assessment included responses from members of the public, and non-governmental associations with an interest in this field.

4. METHODOLOGY AND TOOLS

Given the small number of results in the public consultation results have been proceed manually.

Debate and answers to the surveys, interviews, case-studies, and ad hoc workhops involved the reading of the consultation responses in full, the drafting of minutes and the noting of any issues and concerns. They were factored in as part of the Study on which this impact assessment is based.

5. RESULTS

5.1. Consultation on the Inception Impact Assessment

This public consultation on the Inception Impact Assesssment received four answers. Two from members of the public, one from a private company and one from a European police trade unions association. All the responses have been published in full online[136].

[133] Law Enforcement Working Party (LEWP) is a Council preparatory body, which handles work relating to legislative activities as well as cross-border policing and related operational issues.

[134] The Customs Cooperation Working Party handles work regarding operational cooperation among national customs administrations and with a view to increasing their enforcement capabilities.

[135] See the list of stakeholders consulted in Annex 2.

The European police trade unions association indicated that: "*obtaining relevant information quickly at the time when it is needed is essential*". "*Under the current fragmented legal framework for law enforcement, information received by national police forces is not readily accessible by officers on the ground*". It supported: "*the Commission's initiative to streamline and consolidate existing instruments for cross-border police cooperation*".

The private company, involved in cyber-security issue, indicated "*the possibility to provide police with the possibility for a transfer of the investigation from the jurisdiction of the victim to that of the police in the jurisdiction of the suspect*" as an avenue to be explored.

A member of the public mentioned the relevance of the European Arrest Warrant. The last answer was irrelevant.

6. HOW THE RESULTS HAVE BEEN TAKEN INTO ACCOUNT

The results of the consultation activities have been incorporated throughout the impact assessment in each of the sections in which feedback was received. The consultation activities were designed to follow the same logical sequence as the impact assessment, starting with the problem definition and then moving on to possible options and their impacts.

Using the same logical sequence in the consultation activities as in the impact assessment itself, facilitated the incorporation of the stakeholders' feedback – where relevant – into the different sections of the impact assessment.

Exhaustive presentation of the consultation activities as part of the support study

This document presents the exhaustive findings from the consultation activities carried out as part of the *Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation*.

Objectives and types of stakeholders consulted

As part of the study, various consultations, both with key stakeholders and the public at large, were carried out. The aim of these consultations was to provide the European Commission with factual evidence concerning possible problems and additional measures in the area of intra-EU law enforcement cooperation. A wide range of stakeholders operating both at the EU and the national levels was consulted, using a combination of different consultation tools. The stakeholders can be organised into a number of general categories described in the Table below.

Categories of stakeholders involved

Stakeholder category	
EU Agencies, Bodies and Networks	European Commission
	EU bodies with relevant expertise
	LEWP members
National authorities	National LEAs
	National judicial authorities
	National data protection authorities
Mixed EU level and national level stakeholders	EMPACT Support Managers
	EMPACT Drivers
Other	Members of the Academia and think tanks
	Members of the general public

Source: EY/RAND Europe Study's elaboration

Consultation methods and tools

[136] EU police cooperation code – tackling cross-border serious & organised crime (europa.eu)

The following consultation methods were used as part of the study:

- Online survey with LEAs, data protection authorities and judicial authorities;
- Interviews with:
  - EU bodies;
  - EMPACT actors;
  - Member State representatives (case studies);
  - Academia;
- Focus groups with representatives of Member States that cooperate within the framework of bi-/tri-/ multilateral agreements; and
- Technical workshops with representatives of Member States and Schengen Associated Countries, as well as EU-level stakeholders.

In addition to these methods, in line with its *Better Regulation Guidelines*, the European Commission implemented a *Public Consultation* (PC) of all relevant stakeholders interested, including members of the general public. The consultation was hosted on the European Commission's website (ec.europa.eu) in all EU official languages. The PC ran for eight weeks, from 19 April 2021 to 14 June 2021. In total, 20 replies were received.

Online survey with LEAs, judicial authorities and data protection authorities

An **online survey** was deployed using the contractor's survey tool. The survey targeted national LEAs, national judicial authorities (specifically, Eurojust national desks and European Judicial Network contact points) and national data protection authorities. The consultation ran for eight weeks, from 5 March 2021 to 30 April 2021. In total, 239 responses were received: 216 from national LEAs' representatives, 13 from national judicial authorities and 10 from national data protection authorities.

Interviews with EU bodies, EMPACT actors, Member States, and Academia

In total 48 individual **interviews** were conducted with key stakeholders. These included:

- 20 interviews with EU bodies;
- 10 interviews with EMPACT drivers and two group interviews with EMPACT support managers (in total 21 interviewees); and
- 4 interviews with academics and members of think tanks.
- 12 group interviews with Member State representatives for the case studies.

The interviewees were selected in agreement with the Commission. The interviews were conducted online, for most part via Teams. The interviews were used to collect data on the problems, possible solutions and the impacts of these.

The **interviews with EU bodies, academia and think tanks** were focused on collecting expert views on gaps and deficiencies affecting the current EU framework for law enforcement cooperation, as well as qualitative and quantitative information concerning possible impacts of additional measures. The interviews with members of academia served to provide relevant inputs based on their knowledge and past research on cross-border police cooperation.

The involvement of **EMPACT support mangers and operational action plan (OAP) drivers** helped gaining a better understanding on the state play in the use, implementation and effectiveness of cross-border law enforcement cooperation measures/practices and investigative tools with regard to each specific priority crime area of the EU Policy Cycle, in order to understand whether there are measures/tools that are particularly used and effective in certain crime areas, but not in others. In other words, this data collection exercise allowed the Study Team to change the angle of the

analysis from the legal basis (EU/national/international) to the area of utilisation of specific measures/tools (i.e. priority crimes).

In addition**, interviews with national LEAs** were performed at the end of phase 1 of the study in order to follow up on specific findings and issues identified during the assessment of the problems.

To account for possible national differences in the assessment of the impacts of the policy options, the Study Team undertook case study interviews with national stakeholders from a selected number of Member States to better comprehend the heterogeneity of the institutional and regulatory law enforcement frameworks in the Member States and SAC, and related impacts of the options. Within this framework, an additional **12 interviews with 26 participants from five countries (Austria, France, Slovenia, Sweden and Switzerland)** were conducted to provide Member State-level deep dives concerning the expected impacts of the policy options in their country.

Focus groups with representatives of Member States and SAC

In order to collect first-hand information on the use, practical implementation and effectiveness of four relevant bi/tri/multilateral agreements (i.e. the Benelux agreement; DE-CZ agreement; CH-FR agreement; and Nordic countries agreement), the Study Team organised **four separate focus groups** convening the parties involved in each agreement. The focus groups allowed the Study Team to develop an in-depth understanding of the content and scope of said agreements, as well as of their practical implications, including both strengths and weaknesses. The Study Team collected the necessary information to understand whether the agreements are outdated/underused or, on the opposite, whether they include measures on cooperation mechanisms or investigative tools that are innovative or have proved to be particularly effective in combating cross-border crime. The focus groups involved a total of 48 participants. Each group included participants from each Member State and SAC who has signed the agreement and included stakeholders from different agencies (for example, police, customs, and other specialist departments).

Technical workshops with representatives of Member States and SAC

Two full-days technical workshops were organised and animated by the Study Team. Each workshop involved close to 200 participants. The objectives of each workshop were as follows:

- The **first technical workshop** took place on 24 March 2021 in Phase 1 of the study and involved representatives from DG HOME, DG JUST, the Council, Europol and Cepol, as well as representatives from all EU Member States and SAC. The participants were asked to provide their feedback on the nature and scale of identified problems, the EU dimension of the problems and the effective need for further EU action, thus allowing the Study Team to fine-tune the problem definition and the analysis of the evolution of the problem in the absence of any additional EU action. The first technical workshop also allowed the Study Team to cross-check information collected through other sources and collect missing data and information to develop a more complete evidence-base. Finally, this meeting was also used by the Study Team to discuss and explore possible policy options addressing identified problems to be taken into consideration.
- The **second technical workshop** took place on 24 May 2021 in phase 2 of the study. This workshop involved the same types of stakeholders as the first workshop, namely representatives from DG HOME, DG JUST and the Council, as well as representatives from all EU Member States and SAC. The participants involved in this workshop had the possibility to both give their feedback on the preliminary content of the policy options to address the current problems affecting cross-border law enforcement cooperation and to provide additional information on the likely impacts of the options, thus allowing the Study Team to fine-tune the definition of the options and the assessment of their impacts.

Each workshop included:

- **Plenary sessions** for the discussion of the study interim findings and preliminary results; and
- **Break-out sessions** in smaller groups according to information exchange.

In addition to both technical workshops, the study team gave a presentation at the law enforcement working party (LEWP) meeting on 16 March 2021. The presentation focused on the study's objectives and methodology. This synopsis report does not include a detailed summary of this meeting since the study team was only present for its own presentation.

Exhaustive results of the consultation activities carried out as part of the support Study

This chapter presents the main findings derived from the various consultation methods.

Online survey with LEAs, judicial authorities and data protection authorities

As indicated above in section 1, in total 239 responses were received to the online survey: 216 responses were received from national LEAs' representatives, 13 from national judicial authorities and 10 from national data protection authorities.

Measures/practices existing at EU and national levels including investigative tools

As concerns the **existence of bi-/tri-/multilateral agreements** concerning law enforcement cooperation, almost all of the survey respondents among LEAs (98%, n=62[137]) confirmed that their country is part of at least one agreement with one or more countries. Moreover, numerous LEAs also confirmed that the agreements in many cases go beyond the provisions in EU instruments (n=19). A lower number of respondents indicated that they address specific legal challenges countries may face when cooperating on specific topics or using specific tools (n=5). A very limited number of respondents stated that the agreements they have entered into with other countries were an affirmation of cooperation, which either already existed prior to Schengen or is based on cultural values (n=3). Furthermore, according to a limited number of respondents, the perceived added value of the agreements included the clear outlining of rules and competencies (n=5), and fast information exchange and additional competencies beyond what is outlined in EU documents (n=3). Three respondents explained in this regard that the agreements in their country had more added value when they were created, compared to now, but that there is still value in them now. One respondent described the agreements as a daily manual for their tasks.

The online survey also included questions on **data protection in relation to bi-/tri-/multilateral agreements**, which were targeted at data protection authorities. Two thirds of the respondents from this stakeholder group (66% (n=6) confirmed that they had previously been asked to advise or comment on a bi-/tri- or multilateral agreement their country is part of. More than two thirds (70%; n=7) stated that there are no differences in breaches between the implementation of multilateral agreements and the implementation of other cross-border cooperation matters.

[137] The number of responses ("N") denotes the number of valid answers for a specific question, not the number of replies to the survey overall. Therefore, 62 responses can e.g. refer to a share of 98% of respondents whereas, at the same time, 131 responses can also correspond to a share of 82%. The "N", thus, also always needs to be understood in view of the specific questions and number of answers given to a particular question – not the overall number of respondents to the survey.

Finally, according to the judicial authorities that responded to the survey, 9% (n=1) of the respondents stated that **judicial authorities** always need to be **involved in the authorisation of investigative tools**, while 27% (n=3) confirmed an occasional involvement. However, equally many respondents (37%; n=4) stated that no involvement of judicial authorities is required, while 27% (n=3) indicated that they do not know. Regarding the **supervision of investigative tools**, 43% (n=3) stated that judges or prosecutors are involved in supervising the measures, while an even higher number (57%; n=4) stated that they are not.

The need to harmonise investigative tools and for EU action

The **need for EU intervention** in the field of **cross-border exchange of and access to information** is widely supported by the LEAs answering the survey, with 82% (n=131) of the respondents reporting a need for EU action from a 'moderate' to a 'very high' extent. The percentage of those supporting EU intervention to **strengthen operational cooperation for public order and safety** was somewhat lower, with 52% (n=44), reporting a need to intervene from a 'moderate' to a 'high' extent. Similarly, 54% (n=83) of LEAs answering the survey reported a strong need for EU intervention to **improve operational cooperation to fight SOC**.

The problem definition

Considering the issue of **access to and exchange of necessary information** among law enforcement authorities, LEAs answering the survey stated that information exchanges related to operations against SOC are frequent, and those related to **public safety** are frequent as well, although slightly less so. However, the majority of LEAs responding to the survey (82%, n=98) reported to have experienced some problems when sharing information with other countries, such as time delays to receive the information request (30% of the responses, n=82). As pointed out (62% of the responses, n=98), such issues are mainly due to the fact that the foundational EU legal framework is not consolidated in all areas, it is spread across several legislative instruments and allows for significant flexibility to the Member States and SAC regarding the implementation of relevant EU provisions.

Interviews

EU bodies

Interviews conducted in Phase 1

In the first phase, interviews with EU bodies were conducted to explore the functioning of current law enforcement cooperation practices, including current problems and the need for EU action (CEPOL, EDPS, EJN, EJTN, EMCDDA, EPPO, EUCPN, Eurojust, Europol, FRA, OLAF).

Policy objectives

Representatives from EU bodies expressed the need to develop instruments setting common standards and ensuring:

- A convergence of LEAs towards a common understanding of the use of tools;
- A common and shared assessment of threats affecting the EU;
- A common practice to gather information from all EU Member States in a similar way and have comparable data available;

On a more operational level, guidelines for information sharing were seen as flexible instruments as they allow Member States to maintain "room for manoeuvre" and adapt them to their specific

needs. Non-binding documents were seen as a compromise reached at the political level, as it is hardly possible to commit 27 Member States to only one binding still more effective document.

Stakeholders agreed that the interoperability of databases is an important aspect to be addressed with the aim to ease cross-border cooperation and to overcome the current issues related to the presence of divergent approaches.

According to EU bodies' representatives, EU should also implement measures and mechanisms to compel Member States to share information with each other and with the relevant EU agencies. The final outcome should be the implementation of an automated process to access databases, in order to have a centralised system that every Member State and third countries can benefit from.

Regarding data protection, it was seen as important that the legislative framework of data protection is up to date to integrate new forms of cooperation resulting from technological innovation (artificial intelligence or big data). Legislative interventions concerning data protection should address:

- Limited quality of data quality stored in databases;
- Difficulties comparing data retrieved from different databases as they are stored differently;
- Children's fundamental rights as part of cross border investigations;
- Sharing of sensible data with third countries, which may not apply EU standards concerning data protection.

Interviews conducted in Phase 2

As second round of interviews with EU bodies were conducted in phase 2 of the assignment (CEPOL, EDPS, EJN, EPPO, EUCPN/ENAA, Europol, FRA, OLAF).

The interviews served to gather additional detailed information concerning:

- Possible EU measures to address current problems affecting cross-border law enforcement cooperation; and
- The likely impacts of these possible EU measures.

The assessment of the impacts of the policy options

Regarding **information exchange via SIENA and other communication channels**, interviewees from one EU body did not expect immediate positive direct impacts if English was established as the default language for the use of SIENA. The stakeholders instead saw positive impacts if bilateral communication takes place in (common) national languages, as this would allow for a quicker management of information requests. Instead of establishing English as the default language for the use of SIENA, the representatives considered the introduction of a translation tool as more suitable for information exchange concerning cross-border cases. One interviewee from another EU body also highlighted that obstacles stemming from language barriers hamper efficient information exchange and stressed the need to address language barriers in the near future. In yet another interview, a critical opinion towards the establishment of SIENA as the preferred/default channel for information exchange concerning intra-EU cross-border cases was voiced. Since it was cumbersome for one interviewee to get access to SIENA in his/her operational work due to security restrictions of his/her organisation, s/he could not agree on positive impacts stemming from this potential EU measure.

Concerning the **definitions of requirements for data**, one interviewee highlighted the importance of data accuracy in relation to data, which is subject to exchange. Errors in databases, which appear to be common, undermine the added value of databases and can have a negative impact on fundamental rights, for instance if an innocent individual becomes subject to proceedings.

As concerns **training activities**, interviewees from one EU body did not see immediate positive impacts if shorter intervals between the EU-STNA were introduced (e.g. a reduction from four to two years) since a longer cycle allows for better strategic planning. Similarly, this stakeholder advised against the introduction of mandatory training on EU law enforcement cooperation for officers in specific roles relevant to cross-border law enforcement and at specific levels, as this stakeholder did not have positive experiences with the implementation of mandatory training a year ago. Free and voluntary learning methods were considered as the more feasible option in this regard.

Interviewees from other EU bodies highlighted the importance of awareness raising campaigns within the EU law enforcement community. Positive impacts from awareness raising campaigns were expected, as many officials were stated to not be aware of the existing measures and policies in place to facilitate information exchange.

EMPACT actors

Objectives and overview of the interviews with EMPACT drivers and support managers

Interviews with EMPACT stakeholders were conducted as part of the study, including:

- Ten individual interviews with EMPACT drivers; and
- Two Group interviews with EMPACT support managers (4 and 7 interviewees respectively).

A total of 21 stakeholders were interviewed in the individual and group interviews.

Key results from the interviews

Interviewees were asked about a series of aspects concerning cross-border cooperation, their efficiency and challenges encountered.

Structures for cooperation

Interviewees in the individual and group interviews were asked about the **use of multiple structures in place in cross-border cooperation**. The following structures were provided as prompts to the interviewees: Single Point of Contact (SPOCs); Police and Custom Cooperation Centres (PCCCs), National SIRENE Bureaux; Europol Liaison Officials; Swedish Framework Decision (SFD); Manual on cross border cooperation National Factsheets (13920/20).

There was **no overall consensus** on which tool is the preferred tool. Different structures seem to be used in different crime areas and countries. For example, the PCCCs between two countries were stated to work well, but this cannot always be replicated in other countries due to resource constraints. The Swedish Framework Decision was highlighted as particularly useful for financial crimes. Each structure in place was created with a specific purpose within cross border communication. As most of these structures were created decades ago, interviewees voiced concerns over these structures not reflecting the current needs of investigation teams, in particular with regard to cybercrime, where quicker and more direct cooperation with experts in the field is needed.

The **potential of centralisation** of these structures into one structure was discussed. Interviewees agreed that the existing structures should be revised instead of creating a new one. Centralisation into one system was raised as potentially problematic due to the number of requests which would be going through the system per day.

Interviewees acknowledged that **cross-border cooperation has increased** over the past decades. Cooperation has improved significantly already, however, the changing crime landscape is posing new challenges. Cross-border cooperation needs effective tools to address new types of crimes, such as cybercrimes, and new types of criminal networks, online and dispersed over several countries. There is a need to reflect this in national legislation and the agreements guiding cross-border cooperation. Currently the required paperwork and often the national legislation is slowing investigations down.

Information exchange platforms

Interviewees in the individual and group interviews were asked about the **use of information exchange platforms** in place in cross-border cooperation. The following structures were provided as prompts to the interviewees: SIENA; the Schengen Information System (SIS); the Europol Information System (EIS); Interpol exchange channels; and the Visa Information System (VIS).

Interviewees found that there are currently too many different platforms and databases for exchanging information. As with the cooperation structures, interviewees highlighted that these platforms/ databases were each created with a specific purpose in mind. However, different countries have different preferences concerning which platform to use. Because of the amount of platforms countries can choose from, information is often scattered and it is unclear what information is available. Interviewees suggested reviewing and reforming existing platforms and potentially link them, rather than creating a completely new tool.

Trust between the countries involved in cooperation was mentioned as the most important aspect for the efficient sharing of information. Interviewees explained that most countries are reluctant to upload sensitive information to share with everyone else and with Europol.

Multilateral Agreements

Interviewees in the individual and group interviews were asked about their **awareness of bi-/tri-/multilateral agreements** and how they are being used in practice. Few interviewees had experience working under bi-/tri-/multilateral agreements. It was nevertheless highlighted that for those colleagues working in the border regions, these agreements are useful to ensure smooth cooperation. It was highlighted that sometimes the bureaucracy and national legislation related to the agreements can slow down cooperation in border areas and make it more complicated for the officials working with them.

Future Needs

Interviewees in the individual and group interviews were asked about the **future needs** in cross-border cooperation. Most interviewees acknowledged the progress that has been made in cross-border law enforcement cooperation between different countries. However, interviewees requested reforms to reflect the changing crime landscape. Especially in the area of digital crimes legal reforms are required to account for the fast pace of the crimes.

The harmonisation and revision of structures, tools and legislation was also mentioned as a point for EU wide action.

Good practices

Interviewees also provided valuable information on 'good practices' in different areas of cross-border law enforcement cooperation. Suggestions included:

- **SPOCs:** For countries where the single points of contacts are well established, the SPOCs were seen as an added value to establish a course of action for the cooperation.

- **Trust / Personal Networks:** Interviewees mentioned trust as the key element for cross-border cooperation. It was explained that informal networks with officials from other countries with whom cooperation has existed for years are often the first point of contact when it is necessary to establish cooperation with another country. The network of the Europol liaison officials was also mentioned as a good practice for cooperation, where trust is built and which facilitates direct cooperation between the countries.

- **Trust / Crime-area specific network:** The Joint Cybercrime Action Taskforce (JCAT) was mentioned as a good practice. This taskforce connects cybercrime experts from across the EU to facilitate cooperation. Through continuous cooperation trust can be built, which results in better cooperation. One interviewee highlighted that shared knowledge of the language and terminology in this crime area has resulted in smoother cooperation. 'SMOKE' was also mentioned as an effective network of cooperation between police, customs and the tobacco industry in combatting counterfeit cigarette production.

- **Accessibility of communication tools:** In some countries the accessibility to, for example, SIENA computers, was highlighted as well developed. Two countries were mentioned as good examples, since SIENA computers are accessible across these countries and available to the officials who may need it.

- **Bilateral agreements:**

    - **Cooperation in border regions:** Bilateral agreements are seen as the most effective way of cooperation in the border regions and day to day cooperation.

Challenges

Interviewees were generally in favour of international cooperation and the structures and investigative tools which can be used. However, the interviewees highlighted a set of challenges they face when employing the available structures and investigative tools in practice.

- **Lack of harmonisation** and persistent **structural differences** between countries were considered the biggest challenges for law enforcement cooperation.

    - **Legislative perspective:** Several interviewees spoke about the challenges of using tools in cross-border cooperation due to the different legislation in the Member States. The rights of officials in countries across the EU and the Schengen area differ significantly and it is not always clear to foreign officials what rights they have. In addition, the authorisation of requests and tools is often regulated by national laws, creating substantial difficulties in cross-border cooperation.

    - **Operational perspective**: Across different countries the LEAs responsible for investigations may vary distinctively. These differences may relate to the structure of the police and customs bodies within the countries or to the rights each law enforcement agencies has within their own country. This can hinder cooperation, if it

is difficult for foreign officials to assess who the cooperation should be with. This challenge was highlighted in relation to structures, tools and information exchange.

- **Challenges related to the exchange of information**:
    - **Existing information**: It is often unclear what kind of information exists in other countries on persons or goods relevant to an investigation. Interviewees highlighted that using a two-step approach, i.e. making a request first to see if information is available and then to request the information itself often prolongs the investigation process. Member States often seem hesitant to share information in joint databases, often leading to a lack of data in those databases.
    - **Access to communication tools**: The access to communication tools differs significantly across Members. For example, in some countries SIENA computers are only available to officials in their capital city.
    - **Usage of information sharing tools**: While recognising that existing structures for information exchange serve different purposes, the large number of different tools in use can pose challenges. There is variation with regard to which tool is used for what purpose across the Member States. Sometimes this is due to the accessibility or procedures within the Member States. This lack of harmonisation leads to information for one case being partially shared through one tool and partially through another, sometimes with different recipients on these tools. This results in officials not having all necessary information. It was also mentioned that occasionally requests are submitted through different channels resulting in duplication of request.
- **Lack of human resources for cooperation:** The lack of personnel allocated to handle requests for cross-border cooperation was highlighted as a challenge for cooperation. Interviewees highlighted that those handling the requests are often overwhelmed with the number of requests received, which can delay responses to requests. It was also highlighted that often those persons that are responsible for handling the request may not be familiar with the specific crime area of the request, which can lead to issues in addressing it.
- **Lack of awareness of structures, tools and platforms:** Several interviewees mentioned that a lack of knowledge about the different cooperation tools available to officials on the national level can hinder cooperation on the EU level.

In summary

Overall, the interviews provided a wide range of views regarding cross-border law enforcement cooperation in terms of what is working well and what is not working so well, seen through the eyes of these stakeholders. The interviews shed light on the cross-border law enforcement cooperation and the practical realities the stakeholders are faced with every day. While some structures seem to be working well and facilitate cooperation, officials are often using informal structures to ensure smooth cooperation, as trust in officials from other countries is mentioned as the base of cooperation and the amount of channels and structures available are often confusing to use and need to be revised. There was a consensus that the overall cooperation tools were introduced for a good reason, but a revision needs to be done, especially within the changing crime landscape the EU and the Schengen Area are facing.

Member State representatives (case studies)

In agreement with the EU Commission, Austria, France, Slovenia, Sweden, and Switzerland were selected as case study countries. The five case study countries provide a mix in terms of the following criteria:

- **Population size:** The selected case studies encompass countries with rather small (Slovenia) and large population sizes (France). In total, 23% of the population in the countries analysed in the study are covered.[138]
- **GDP per capita:** The selection of case studies includes countries with rather low (Slovenia) and high (Austria, Sweden, Switzerland) GDP per capita.
- **Number of reported challenges in the countries:** The selected case studies encompass four countries (France, Slovenia, Sweden, Switzerland) that have high numbers of issues in existing sources that refer to all three core problems identified.
- **Number of bi/tri/multilateral agreements identified in the study:** The selected countries are either countries with medium number of agreements (France, Slovenia, Sweden) and high number of agreements (Austria, Switzerland).
- **Scope of the bi/tri/multilateral agreements analysed in the study:** The case study selection includes countries with agreements that cover most categories, i.e. SOC and public safety, information sharing as well as investigative tools and joint operations (Austria, France, Slovenia), and countries that e.g. cover mostly SOC and not all investigative tools and joint operations (Switzerland, Sweden).
- **Coverage of investigative tools:** Among the selected case studies, all but one country (Switzerland) cover all types of investigative tools.
- **Categories of competent authorities for the SFD:** The selection of case studies covers countries with rather low numbers (Slovenia) and rather high numbers of categories (Sweden) of competent authorities for the SFD.

[138] Eurostat (2021) Population on 1 January. Available at: link.

Criteria for the selection of case study countries

Country	Population Size in 2020	GDP per capita in 2020	Number of Reported Challenges in key sources	Number of Agreements Identified	Scope of the Bi-/Tri-/Multilateral Agreements Analysed			Investigative Tools Coverage	Number of Categories of Competent Authorities for the SFD
					SOC / Public Order and Safety	**Information Sharing**	**Investigative Tools and Joint Operations**		
Austria	8,900,000	42,110 €	5	11-15	Both	Yes	Yes	All	3
France	67,300,000	33,690 €	9	6-10	Both	Yes in all but one agreement	Yes in all but one agreement	All	3
Slovenia	2,100,000	22,010 €	10	6-10	Both in all but one agreement	Yes	Yes	All	2
Sweden	10,300,000	45,610 €	8	6-10	Only SOC	No	No	All	4
Switzerland	8,600,000	75,890 €	9	11-15	Only SOC in six agreements	Yes	Yes in all but two agreements	All but use of informants	3

Source: EY/RAND Europe Study's elaboration , based e.g. on Eurostat and desk research

A total of 26 national representatives were interviewed in the five case study countries in 12 individual case study interviews. Additionally, two follow-up interviews were conducted with representatives from Belgium.

Number of participants per case study country

Case study country	Number of interviews	Number of participants
Austria	1	1
France	4	12
Slovenia	4	6
Sweden	1	1
Switzerland	2	6

Source: EY/RAND Europe Study's elaboration , based on case study interviews

The case study interviews were conducted to gather additional detailed information concerning:

- Possible EU measures to address current problems affecting cross-border law enforcement cooperation; and
- The likely impacts of these possible EU measures.

The interviews were structured around the topic of access to and exchange of information.

Access to and exchange of information

The interviewees from the case study countries were either indifferent or favourable towards the potential EU policy measures that had been developed to address current challenges in relation to access to and exchange of information.

With regard to the **set-up and competencies of the SPOCs and PCCCs**, interviewees from two case study countries specified that they assume positive impacts from the policy options for those Member States that have not already set up their SPOCs and PCCC in line with the presented policy options. However, they expected little impact for their own countries as they are mainly already complying with the presented measures. For instance, the interviewees highlighted that they already have SPOCs operating 24/7 and that if there is an information request, requests can be handled in real-time with no delays, particularly in urgent cases. Other representatives, nevertheless, also estimated that if the SPOC were to have full access to relevant national case management systems, the time saved would be at least several days, as for non-urgent cases signatures by competent authorities are always required.

As concerns the SPOC/PCCC **Case Management Systems (CMS)** in the Member States, one representative explained that they are already in the planning phase for a CMS in their country, which would comply with the presented policy options such as the usage of Universal Message Format or that the degrees of urgency should be linked with deadlines. Hence, no major impacts were expected from the introduction of these potential EU measures. Interviewees from another case study country, however, expected positive impacts from the provision of a list of common requirements for functionalities, since the existing CMS are typically based on inhouse solutions and, consequently, not necessarily tailored to the needs of cross-border law enforcement cooperation.

Interviewees voiced different expectations about the impacts in relation to information exchange via SIENA and other communication channels. On the one hand, representatives from two case study

countries only saw limited added value if **English were to be established as the default language** for the use of SIENA and found SIENA user-friendly already. Stakeholders from another country did, however, expect to see positive impacts in terms of a reduction in working time currently spent on translation if English was established as default language for the use of SIENA. These stakeholders were of the view that SIENA could be made more user-friendly if a translation tool was integrated in SIENA, which would allow SPOCS to allocate human resources currently dedicated to help out on translation issues to other urgent tasks.

The stakeholders from the first two countries were more favourable towards **new, simpler, and more user-friendly forms**, which could result in a limited positive impact. Similarly, representatives from the third case study country indicated that they would expect clear positive impacts if more user-friendly forms were established.

As concerns the establishment of SIENA as the **preferred or default channel for information exchange**, representatives from one case study country indicated that, although they use SIENA already very frequently as their most important information exchange channel, their LEAs would greatly benefit from even more Member States and SAC using SIENA as the preferred channel.

One representative stressed that they in particular expected positive impacts from EU measures addressing the use of secure communication means. They currently rely on WhatsApp for fast cross-border communication and for sharing initiative information without personal data, but would prefer a police communication mobile app or platform linked to SIENA with encrypted messaging. Hence, the development of **common standards for secure communication means** and the development of a "central LEA app" would help to solve the security problems with respect to WhatsApp and reduce delays when waiting for replies and reactions from officials from the other side of the border.

Interviewees expressed different expected impacts concerning **training activities**. If English were defined as an appropriate criterion for specific roles within certain LEAs working on primarily on international cases, one interviewee saw little added value as those officials working in cross-border cases in his/her country who need to speak English have a sufficient command of English. On the other hand, representatives from another case study expected positive impacts. They illustrated their opinion with the example of the usage of SIENA: If an official needs support to fill in a form in SIENA, then the SPOCs helps with the translation. If appropriate English skills were defined as an entry criterion, then the SPOCs could spend less human resources (or less working time) to assist with translations. Concerning the introduction of mandatory training on EU law enforcement cooperation for officials in specific roles relevant for cross-border law enforcement, one interviewee stressed the positive impacts that could stem from a reduction in specific initial training, which are set up in advance before each joint operations. If training was more standardised, administrative costs for the performance of trainings and working hours spent by officials on trainings could be reduced.

The problem definition

Developments in the Public Order and SOC landscape

Overall, the interviewees agreed that **major issues are related to collaboration to fight SOC**. In particular, the experts reported the presence of three main types of organised crime groups:

- *Mafia-like groups*: A group that has a significant size and structure, which could be active in the economic sphere in infiltrations and in the illegal economy.
- *Local groups*: Small groups linked to the territory where many different groups operate, performing different activities and having a flexible organisational structure.

- *Emerging groups*: A mix of ethnic and local groups that has resulted from the migratory process that has affected Europe.

With reference to these groups, the consulted experts reported that in Europe expect that while there will be fewer mafia-like groups, emerging ethnic groups will be increasingly important in the future.

Law enforcement cooperation

The academic experts reported that, overall, the actual practice of law enforcement cooperation has not significantly changed in the last ten years and is still strongly based on **direct contacts and trust** between law enforcement officials, rather than on formal cooperation schemes.

Information sharing

Academics reported that one of the main emerging issues is the **high volume of data** (Big Data) to be analysed, since the analyses is challenging in cases of vast amounts of information, including the amount of additional human resources that are currently required.

With reference to the exchange of information, experts were critical towards the current **availability of external analyses concerning information exchange**. For instance, key EU bodies were stated to give no access to independent researchers, which hampers transparency and objective analysis.

Policy objectives

Academic experts highlighted that when designing policies, it is important to take into account different and sometimes conflicting types of rationales. The main types which are usually considered are: Economic rationality; political rationality; legal rationality and practical rationality. Therefore, it is fundamental to achieve a proper balance between the different rationalities and consider the relevance of all of them. However, according to the academics consulted, EU policies usually stem from political rationality and this in many cases contrasts with practical and professional rationality.

Over the last ten years, there have been some important developments, but the steps forward have not translated into operational practices that are easy to implement. Indeed, there are regulatory asymmetries between Member States that need to be reduced. Such asymmetries between Member States are exploited by criminals.

Focus groups

Objectives and overview of the focus groups

Four focus groups were carried out to inform the Study to support the preparation of an impact assessment on the EU policy initiatives facilitating cross-border law enforcement cooperation.

To inform the study and to make recommendations for possible additional measures in the area of intra-EU law enforcement cooperation and to propose, assess and compare policy options for possible future action, the Study Team conducted interviews, analysed existing bi-, tri-, and multilateral agreements on law enforcement cooperation between EU Member States and carried out three hours long focus groups on four agreements.

This synopsis report provides an overview of the focus groups conducted, which included:

- The bilateral agreement between Switzerland and France;
- The bilateral agreement between Germany and the Czech Republic;

- The trilateral agreement between Belgium, Luxembourg and the Netherlands (*BENELUX agreement*); and
- The multilateral agreement between Norway, Sweden, Denmark, Finland, and Iceland (*Nordic agreement*).

These four agreements were selected in consultation with DG HOME. They were chosen due to the strong history on law enforcement cooperation between the countries involved, which was expected to yield examples of good practices and remaining challenges in the area of law enforcement cooperation. The focus groups were conducted in the second half of March 2021.

In total 48 stakeholders participated in the focus groups. The stakeholders were selected for their experience working under the respective bi-/tri-/multilateral agreement. This included stakeholders with either strategic or operational level experience and stakeholders from either police, customs, or, other specialist departments.

Number of participants per focus group

Agreements	Number of participants
Benelux Agreement (BE, NL, LU)	9
DE – CZ agreement	12
CH – FR agreement	10
Nordic countries agreement (DK, FI, IS, NO, SE)	17

Source: EY/RAND Europe Study's elaboration , based on interviews of focus groups

Results of the focus groups

Benelux Agreement

The focus group on the *Treaty between the Kingdom of the Netherlands, Kingdom of Belgium and the Grand Duchy of Luxembourg on police cooperation* was conducted on 19 March 2021.[139] A total of nine stakeholders participated: five representatives from the Netherlands, two from Luxemburg and two from Belgium.

The purpose of the Treaty is to intensify political cooperation in the territories of the Contracting Parties in terms of prevention, investigation, and detection of criminal offenses as well as the maintenance of public order and safety. As the Treaty is currently in the process of being ratified by the three Member States, the focus group also looked at differences between the currently applicable version of the Benelux Treaty adopted on 8 June 2004, and the new one of 23 July 2018. Discussions and responses from stakeholders during the focus group indicate that overall, the treaty aligns with the wider EU framework for cooperation and exchange, and it is effective in supporting daily police cooperation. It enables law enforcement activities to be conducted without being hindered by borders. Examples include having central contact points and providing joint training for specialised interventions to police units. Moreover, two improvements under the new Benelux treaty include the fact that across border observation can start in the other country territory and that in the case of hot pursuit, authorities will have complete and unlimited access to proceed in other countries of the agreement.

[139] Treaty between the Kingdom of the Netherlands, Kingdom of Belgium and the Grand Duchy of Luxembourg on police cooperation (2018).

CZ – DE Agreement

The focus group on *the Treaty between the Czech Republic and the Federal Republic of Germany on Police Cooperation* was held on 17 March 2021.[140] A total of 12 stakeholders took part: three representatives from the Czech Republic and nine from Germany.

The agreement aims to generally strengthen the cooperation between the two countries and to prevent and investigate criminal activities. This includes cases that are classed as a crime by one party and as an administrative offence by the other party.

During the discussion, the participants highlighted the need, importance, and effectiveness of this bilateral agreement. They explained that cooperation between the two countries is important because of crimes occurring regularly in the border region. Overall, the participants considered the cooperation between the two countries to be speedy, efficient, and overall uncomplicated. For instance, the agreement allows to exchange information directly with customs investigation officials and mobile units. This is useful especially during drug investigation cases or in the fight against smuggling. Moreover, customs and police from both countries have the possibility to join common training, which are often both theorical and practical.

The discussion also indicated that a more centralised system and an increased involvement of the judicial authorities would be useful to further improve the cooperation and avoid possible duplications in the exchange of information.

CH – FR Agreement

The focus group on the A*greement between the Swiss Federal Council and the government of the Republic of France on Cross-border Cooperation in judicial, police and custom matters* was conducted on 15 March 2021.[141] A total of ten stakeholders joined the discussion: five from Switzerland and five from France.

The objective of the agreement is to prevent and investigate crimes and offences, as well as to ensure public order and safety. It came into force at a time in which Switzerland was yet part of the Schengen agreement, which means that the country actively pursued bilateral treaties with neighbouring countries. The idea of the agreement was to be *en pair* with the EU standards and to further address the needs of the police on the field. They rely on efficient communication and a common language to ensure effective cooperation. For instance, they make use of liaison officials, of various platforms that connect different agencies, and of more informal communication activities. Moreover, due to the area hosting many international organisations, the agreement also allows a smooth cooperation during demonstrations (e.g. demonstrations: against the Turkish government; for Armenian rights; for taxi drivers; for women rights), and the possibility to share information concerning risks and threats to the public order.

However, some existing processes make it difficult for officials to obtain information and intelligence quickly. Also, the lack of a common legal procedural code is limiting. Large differences in the two countries' legal structure can sometimes hinder effective cooperation.

[140] Treaty between the Czech Republic and the Federal Republic of Germany on Police Cooperation and on amendments to the Treaty between the Czech Republic and the Federal Republic of Germany on amendments to the European Convention on Mutual Assistance in Criminal Matters from 20 April 1959 and the facilitation of its application from 2 February 2000.

[141] Agreement between the Swiss Federal Council and the government of the Republic of France on Cross-border Cooperation in judicial, police and custom matters (2007).

Nordic countries Agreement

The focus group on the *Nordic Administrative Agreement on Cooperation between Police Authorities in the Nordic countries (NO-SE-DK-IS-FI)* was conducted on 22 March 2021.[142] A total of 17 stakeholders participated: two representatives from Norway, six from Sweden, three from Denmark, three from Finland and three from Iceland. The participants decided to start the focus group by delivering a brief presentation about the agreement. As part of this presentation, the stakeholders mentioned the strategic objectives for the Nordic police cooperation (2019-2022) which include effective law enforcement, progressive and future-proof policing, a strong regional voice on the international Arena and good conditions for police work, in the Nordic region.

The agreement, which is currently being evaluated, aims to prevent, detect, and investigate criminal offences in order to ensure public order and internal security. The discussion with the stakeholders indicated that this agreement constitutes a *memorandum of understanding,* setting out the parameters of the cooperation between the Nordic countries. Stakeholders believe that the cooperation is effective because it is mainly informal and based on trust. Cooperation takes place on a daily basis and is continuous between the Nordic countries. They have liaisons officials now covering 32 countries, which facilitates communication and the fight against crime. All countries that are party to the Nordic agreement have access to the different liaison officials (e.g. Norway has access to Danish liaison officials). They also have constant operative operations, e.g. on the bridge between Sweden and Denmark.

Good practices

The focus group activity also informed the identification of good practices and remaining challenges. Several focus group participants expressed that bi-/tri-/multilateral agreements are useful, as they can provide additional provisions that may be not covered in other existing frameworks, such as the Schengen Agreement[143] and the Prüm Convention.[144]

The discussions of the participants during the focus groups highlighted the following as good practices:

- **Common training**: Considered very useful to learn and practice new skills, establish trusting relationships and further foster the willingness to engage in cooperation. This also includes information sessions provided to local police forces with the aim to explain the links between the operational level and the bilateral agreement by showing the judicial viewpoint of the agreement as well as the practical implementation.
- **Regular meetings**: considered good opportunities to share experiences, discuss particular issues across countries, exchange information and explore strategies to prevent serious organised crime as well as an opportunity to further foster cooperation. During the COVID-19 pandemic these have been replaced by video conferences, and have also been used to discuss the latest infection rates and how each country was coping with the situation.

[142] Nordic Administrative Agreement on Cooperation between Police Authorities in the Nordic countries (2016).
[143] The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (1990). Available at: link.
[144] Prüm Treaty (on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration). Available at: link

- **Direct communication**: The participants explained that quick communication is an essential facilitator of successful collaboration. Police forces need to communicate efficiently to be one step ahead of criminals.

- **Liaison officials**: These are considered essential for an effective cooperation. However, the number of liaison officials differ between the countries. For instance, the Nordic countries have liaison officials (both customs and police forces) in about 32 countries, giving all countries that are a party to the Nordic agreement access to this kind of network, but it is not the case everywhere.

- **Willingness to cooperate:** By all the participants this was considered a fundamental ingredient of effective cross-border cooperation.

Challenges

Although the focus group participants mentioned many advantages of the bi-/tri-/multilateral agreements in question, and shared various good practices, they also touched upon some remaining challenges. During the discussions they identified a few shortcomings of - and gaps in - the EU framework for intra-EU law enforcement cooperation and shed light on internal cooperation issues. The key points highlighted below:

- **Lack of harmonisation** and persistent **structural differences** between countries were considered the biggest challenges for law enforcement cooperation.

- **Operational perspective**: Another key deficiency identified is the limited effectiveness of SPOCs, often due to the limited resources allocated to them at the national level, both in terms of number and type of police forces available.

- **Challenges related to the exchange of information**: Difficulties to easily find out what type of information is available in other countries, and logistic, budget and personnel limitations hinder the ability to exchange information and follow up quickly.

In summary

Overall, the focus group activity provided a wide range of views regarding cross-border law enforcement cooperation in terms of what is working well and what is working less well. The focus groups shed light on the cross-border law enforcement cooperation related measures and practices existing at the EU and national level, within the countries of the agreements selected.

Technical workshops

First technical workshop

The first technical workshop, which was held on 24 March 2021 and to which close to 200 participants registered, involved a presentation by the Study Team of preliminary findings concerning notably the problem assessment and interactive parallel workshops.

The main findings from the discussions in the break-out sessions in the workshop were as follows:

What are the issues at stake?

Access to and exchange of information

- Key issues include limited awareness of and access to relevant EU and national databases as well as limited interoperability of national systems;

- Some issues specifically relate to the implementation of the SFD, notably the forms included as an annex to the SFD are too cumbersome and the definition of urgency/timeframe is not clear;

- Police-to-police requests instead of other equally effective mechanisms (such as EUCARIS, ECRIS, VIS etc).

How are the current problems expected to develop in case no further EU action is taken?

Access to and exchange of information

- Current problems will become more relevant in case no further EU action is taken;

- The worsening of current problems is mainly attributed to new and evolving technological developments likely to affect the access to and exchange of information.

Is there a need for EU intervention to address current problems?

Access to and exchange of information

- Current problems need to be addressed at the EU level.

What types of policy measures could be considered to address the current problems?

Access to and exchange of information

- In order to improve access to and information exchange, EU intervention should ensure full interconnection and streamlining of available systems for the exchange of information, the overall consistency of the EU legal framework, and the full awareness and capacity of national law enforcement authorities. It should also ensure the integration of modern requirements into fundamental rights and data protection rules.

Second technical workshop, 25 May 2021

The second technical workshop aimed at collecting national stakeholder's points of view on possible EU measures to address current problems affecting cross-border law enforcement cooperation in relation to the access to and exchange of information, operational cooperation for public order and safety and operational cooperation for SOC and terrorism, as well as the discussion of likely impacts of these potential EU measures. Similarly to the first technical workshop, close to 200 persons signed up for the workshop. The workshop took place on 25 May 2021.

The main findings from each of the three breakout sessions are as follows:

Breakout session 1 - Access to and exchange of necessary information

- Set-up and competences of the SPOC and PCCCs
    - Strengths: Time savings, more clarity of competences, responsibilities and rules, increased monitoring of possibilities for the SPOCs concerning the cases, the access to national and international databases and platforms, possibility to ask for judicial authority support at any moment, and common standards of CMS;

- Weaknesses: The feasibility of some of the measures depending on the national-set up was questioned, and the structural differences of SPOCs, PCCCs and judicial authorities between Member States, and the actual availability of data highlighted as challenges.

- SPOC/PCCC Case Management Systems in the Member States
  - Strengths: An intelligent tool would facilitate the workflow, presence of minimum essential requirements for CMS for all Member States, time savings, better data quality, avoidance of duplications, establishment of similar workflows in different Member States;
  - Weaknesses: Costs for Member States in developing the CMS, feasibility linked to national specificities (the integration of specific solution within the national systems might be challenging, depending on the current individual solution used in the Member State).
- Information exchange via SIENA and other communication channels
  - Strengths: Time savings, increased clarity on which communication channel should be used when, increased level of security;
  - Weaknesses: Complexity of access rights.
- Use of secure communication means
  - Strengths: The idea of a "LEA app" was considered as interesting by some participants.
- Training activities
  - Strengths: Additional material provided by CEPOL would be welcomed, and harmonisation of the procedures would simplify the training;
  - Weaknesses: Training should not be too general but targeted, both in terms of the form and the content (e.g. efficient use of SIENA). The limited availability of time for the officials on the ground should be considered.

Results from the public consultation

1. INTRODUCTION

In the context of the *Study to support the preparation of an impact assessment on the European Union (EU) policy initiatives facilitating cross-border law enforcement cooperation*, carried out by EY and RAND Europe, a Public Consultation (PC) in all EU official languages concerning current problems and the future of cross-border law enforcement cooperation was carried out via the Commission's tool EUSurvey. The PC ran between 19 April and 14 June 2021. Overall, 20 responses were received from stakeholders in 12 countries, including 10 Member States (AT, BE, CZ, DE, EL, ES, HU, IT, LU and PT), one Schengen Associate Country (CH) and one third country (US).

2. BACKGROUND INFORMATION

Regarding the **profile of the respondents**, nine answered the survey as individuals (eight EU citizens and one non-EU citizen), while the remaining 11 respondents answered on behalf of an organisation (two public authorities, one business association, one trade union, two NGOs, one academic/research institution, and four "other"). The size of the concerned organisations was the following: five large (250 or more employees), three medium (50 to 249 employees), two small (10

to 49 employees) and one micro (1 to 9 employees) organisation. Of these organisations, five are included in the Transparency Register.[145]

3. PART I - QUESTIONS CONCERNING CURRENT PROBLEMS

The threat landscape

Considering the evolution of the **crime situation** in Europe, the majority of respondents agreed that the number of crimes increased in the last 5-10 years in all the main crime areas,[146] with the highest rates for cybercrime, drugs and trafficking in human beings. Similarly, the number is expected to further increase in the next 5-10 years (apart from trade of illicit tobacco).[147] Moreover, all these crime areas are considered to have a cross-border dimension and require EU-wide cooperation of law enforcement authorities to be properly addressed,[148] especially cybercrime, drugs, terrorism, financial crimes and trafficking in human beings.

From the point of view of **public order and safety**, respondents to the public consultation stated that the situation in the past-5-10 years did not deteriorate.[149] Nevertheless, similar to the responses for the crime areas above, most respondents agreed that all the key areas under investigation require EU-wide law enforcement cooperation.[150]

Cross-border law enforcement cooperation to fight transnational crimes

Around half of the respondents to the consultation considered themselves to have an extensive or even in-depth knowledge of the EU framework for cross-border law enforcement cooperation (56%, n=9). The position of the respondents on the effectiveness of the current **cross-border law enforcement cooperation mechanisms between EU Member States** to fight transnational crimes overall is fairly positive, as 43% (n=6), consider it high, 43% (n=6) moderate and 14% (n=2) small. Similarly, taking into consideration the situation in the individual crime areas, cooperation mechanisms are considered effective in most areas to a moderate extent,[151] with the exception of cybercrime, for which respondents are divided (36%, n=5 small extent, 21%, n=3 moderate, 29%, n=4 high, and 14%, n=2 very high) and drugs (50%, n=7 responding high or very high extent).

---

[145] The transparency register has been set up to answer core questions, such as what interests are being pursued, by whom and with what budgets. The system is operated jointly by the European Parliament and the European Commission. Available at: link.

[146] Percentage of respondents stating that the number of crimes has slightly or significantly increased: cybercrime 93% (n=13), drugs 93% (n=13), trafficking in human beings 85% (n=11), organised property crime 75% (n=9), environmental crimes 62% (n=8), trafficking of firearms 62% (n=8), illicit tobacco trade 58% (n=7), financial crimes 54% (n=7) and terrorism 54% (n=7).

[147] Percentage of respondents stating that the number of crimes will slightly or significantly increase: cybercrime 93% (n=14), financial crimes 71% (n=10), trafficking of firearms 71% (n=10), drugs 67% (n=10), terrorism 67% (n=10), organised property crime 65% (n=9), trafficking in human beings 64% (n=9), environmental crimes 57% (n=8) and illicit tobacco trade 43% (n=6).

[148] Percentage of respondents stating that the following crime areas have a cross-border dimension to a high or very high extent: cybercrime 100% (n=15), drugs 100% (n=15), terrorism 100% (n=15), financial crimes 93% (n=14), trafficking in human beings 93% (n=14), trafficking of firearms 79% (n=11) organised property crime 77% (n=10), illicit tobacco trade 67% (n=10) and environmental crimes 53% (n=8).

[149] Percentage of respondents stating that the security situation in the following areas did not deteriorate or did it to a small or to a moderate extent: cross-border commuting 85% (n=11), international sport/music/cultural events 69% (n=9), and tourism 57% (n=8).

[150] Percentage of respondents stating that the following areas require cross-border law enforcement cooperation to a high or very high extent: pandemics 87% (n=13), natural disasters 80% (n=12), cross-border commuting 67% (n=10), tourism 67% (n=10), safeguard of national public order and safety 53% (n=8) and international sport/music/cultural events 47% (n=7).

[151] Percentage of respondents stating that cooperation mechanisms are effective to a moderate extent: financial crimes 64% (n=9), trafficking of firearms 57% (n=8), organised property crime 50% (n=7), environmental crimes 46% (n=6), illicit tobacco trade 46% (n=6), terrorism 46% (n=6) and trafficking in human beings 42% (n=6).

Cross-border law enforcement cooperation to ensure public order

Regarding **public order**, half of the respondents deems cooperation mechanisms overall effective to a high or very high extent in protecting the mobility of EU citizens and safeguarding public order (50%, n=7). More specifically, a high level of effectiveness was noted in particular for international sport/music/cultural events, with 57% (n=8) of the respondents indicating that it is effective to a high or very high extent. An overall relatively high proportion of the respondents were also of the view that cooperation is rather effective in relation to cross-border commuting, with 50% (n=7) stating that this is a achieved to a moderate extent and 43% (n=6) to a high extent. The opinion is more mixed for natural disasters, pandemics and tourism.[152]

Barriers to cross-border law enforcement cooperation

According to the respondents, the **main issues affecting cross-border law enforcement cooperation** include that the relevant EU legal framework is not consolidated (i.e. it is spread across several legislative instruments), and that it is not consistently implemented across the Member States (i.e. the Member States implement it differently), with 67% (n=10) and 64% (n=9) of respondents respectively stating that these issues are problematic to a high or very high extent. Considering the safeguards to protect fundamental rights of persons subject to measures of cross-border cooperation, half of the respondents deems them sufficient to a high of very high extent (50%, n=8), while the other 50% (n=8) stated that they are sufficient only to a small or to a moderate extent.

Investigative tools to tackle cross-border crimes

Available **investigative tools** are considered to be effective in tackling and combating cross-border crimes,[153] in particular Joint Police Offices and the interception of communication, although more trust between the Member States was stated to be needed to a high or very high extent by 67% (n=10) of the respondents and higher technical and financial resources at the national level to a high or very high extent by 64% (n=9), and are thus are perceived to have the potential to enhance their use and overall effectiveness.

Investigative tools to tackle serious and organised crime at the national level

At **the national level, investigative tools** are considered to be less effective or even not effective at all,[154] with the exception of the interception of communication. Thus, the large majority of respondents sees the need for new tools to investigate organised crime groups in light of recent technological advancements/new technologies and the ability of criminals to exploit them (82%, n=9).

PART II - NEED FOR EU ACTION AND POSSIBLE POLICY OPTIONS

According to the majority of respondents, there is a **need for EU intervention** to improve cross-border law enforcement cooperation through the adoption of legislative and/or non-legislative measures in the fight against serious and organised crime (86%; n=12), terrorism (79%, n=10) and

[152] Natural disasters: 8% (n=1) not at all, 31% (n=4) small extent, 31% (n=4) moderate extent and 31% (n=4) high extent; pandemics: 8% (n=1) not at all, 27% (n=4) small extent, 38% (n=5) moderate extent and 23% (n=3) high extent; tourism: 29% (n=4) small extent, 29% (n=4) moderate extent and 43% (n=6) high extent.

[153] Percentage of respondents stating the tools are effective to a high or very high extent: Joint Police Offices 71% (n=10), interception of communication 69% (n=9), Special Investigation Units 64% (n=9), covert investigations 62% (n=8), Joint Patrols 57% (n=8), controlled deliveries 54% (n=7), informants 54% (n=7), hot pursuit 50% (n=7), witness protection 50% (n=7) and cross-border surveillance 46% (n=6).

[154] Percentage of respondents stating the tools are not effective at all or to a small or moderate extent: informants 71% (n=10), controlled deliveries 69% (n=9), hot pursuit 69% (n=9), witness protection 64% (n=9), covert investigations 54% (n=7), surveillance 50% (n=7) and interception of communication 42% (n=6).

other transnational crimes (71%, n=11), while such need is not perceived to be as strong for ensuring public order against less serious offences (31%, n=4).

Among those considering EU intervention to be necessary, the focus of such intervention should be the revision and update of existing legislative measures according to 16 respondents, and also on non-legislative measures (e.g. guidelines, recommendations, good practices), as noted by 11 respondents.

The answers to the more specific questions concerning **possible measures likely to enhance intra-EU law enforcement cooperation** show a similar picture. Those measures which are considered to have the potential to contribute to improving cross-border cooperation to a larger (high or very high) extent are the modernisation of the EU legal framework for law enforcement cooperation to cope with new challenges posed by criminals (67%, n=10), the setting up of new operational initiatives for law enforcement cooperation (64%, n=7) and the simplification and streamlining of the EU legal framework for law enforcement cooperation (53%, n=8). Comparatively less relevant would be the creation of a single set of rules for all law enforcement authorities (police, customs, etc.) (47%, n=7), the definition of EU common rules for the use of investigative tools to combat serious and organised crime/terrorism (43%, n=6) or the design of non-binding documents (new recommendations, guidelines and good practices) for law enforcement cooperation (33%, n=5). The position of the respondents on the extent to which the adoption of measures granting additional powers to law enforcement authorities would require additional safeguards to protect individuals' fundamental rights is mixed.[155]

List of the stakeholders consulted

Interviews

EU Bodies

Overview of the number of stakeholders consulted from EU bodies

EU Body/Institutions	N° of Interviewees
CEPOL	1
EDPS	1
EJN	1
EJTN	2
EMCDDA	1
EPPO	1
EUCPN	1
Eurojust	1
Europol	1
FRA	1

Source: EY/RAND Europe Study's elaboration

Academia and Think Tanks

Overview of the number of stakeholders consulted from academia and think tanks

Institution	N° of Interviewees

[155] 13% (n=2) respondents stating to a very high extent, 20% (n=3) to a high extent, 20% (n=3) to a moderate extent, 33% (n=5) to a small extent, and 13% (n=2) not at all.

Leiden University	1
Queen Mary University of London	1
Tilburg University	1
Transcrime (Università Cattolica of Milan)	1

Source: EY/RAND Europe Study's elaboration

EMPACT Drivers

Overview of the number of stakeholders consulted from EMPACT Drivers

Member State	Priority	N° of Interviewees
Belgium	**Cybercrime**	1
France	**Horizonal Expert Group on Document fraud**	1
France	**Organised Property Crime (OPC)**	1
Greece	**Facilitating Illegal immigration**	1
Italy	**MTIC fraud**	1
Lithuania	**Excise Fraud**	1
Spain	**Firearms**	1
Spain	**Drugs**	1

Source: EY/RAND Europe Study's elaboration

EMPACT Support Managers

Overview of the number of stakeholders consulted from EMPACT Support Managers

Priority	N° of Interviewees
Money laundering	1
Cybercrime - CSA/CSE	2
Excise and MTIC fraud	3
Environmental crime	1
OPC	1
Cybercrime – Cyber attacks on information system	1
Cybercrime – Non-cash payment Fraud	1
Criminal Finances, Money Laundering and Asset Recovery	1

Source: EY/RAND Europe Study's elaboration

Online survey

LEAs

Overview of the stakeholders consulted from LEAs

Country	Institution (n° of respondents)
Austria	Bundesministerium für Inneres
	Criminal intelligence service
	Ministry of Finance - Tax and Customs Administration
Belgium	Belgian federal police
	General Administration of Customs and Excises
Bulgaria	National Customs Agency of the Republic of Bulgaria
	Ministry of Interior
Croatia	Customs
	General Police Directorate, Criminal Police Directorate, General Crime Service (OPC and envir. Crime)
Cyprus	Cyprus police - c.i.d. (ops)
	Department of Customs and Excise
	Intelligence management analysis subdirectorate
	N.f.i.p. cyprus police

Country	Institution (n° of respondents)
Czech Republic	Customs
	The Police Presidium of the Czech Republic; Division for International Police Cooperation
	Police of the Czech Republic, National Organised Crime Agency
	Ministry of Interior
Denmark	Special investigation west / east jutland police
	Danish national police
	Copenhagen police - border crime centre oeresund
	Pccc padborg
	National Centre of Investigation
	Sydsjællands og Lolland Falsters politi
Estonia	Estonian Police and Border Guard Board
Finland	National Bureau of Investigation / Finnish Police
	National police board
	Finnish border guard
	Nbi finland /spoc
	Finnish Police / National Bureau of Investigation
	Finnish customs
France	Antinarcotics agency (ofast)
	Border police central directorate
	DCI - Direction de la cooperation internationale
	Dgddi
	French national border directorate
	Gendarmerie nationale
	National football information point
	National Gendarmerie / Central Service for Criminal Intelligence
	OCLDI - Central Office fighting against mobile organised crime
	Oclti
	Sirasco
Germany	Bmi
	Bundeskriminalamt/federal criminal police office
	Central customs authority
Greece	Hellenic police
Hungary	International law enforcement cooperation centre
	National Bureau of Investigation
	DG Law Enforcement Public Safety Protection and Guard
	Dg law enforcement duty department
	National Tax and Customs Administration
Ireland	An garda siochana - irish police
Latvia	State Revenue Service, Tax and Customs Police Department
Liechtenstein	Pccc schaanwald
	National police
Lithuania	Police Department under moi Public Police Board Response and Readiness Unit NFIP Lithuania
	Customs criminal service
Luxembourg	Grand ducal police
Malta	Customs
Netherlands	Customs
	Ministry of Justice and Security
Norway	National police directorate
Poland	Ministry of Finance / National Revenue Administration
Portugal	Polícia de Segurança Pública
	Policia judiciária
	Internal security system

Country	Institution (n° of respondents)
	Guardia nacional republicana
	Tax and Customs Authority
	Polícia judiciária - ct national unit (unct)
Romania	General Directorate for Operational Management - Ministry of Internal Affairs - Romania
	National Football Information Point - General Inspectorate of the Romanian Gendarmerie
Slovakia	Ministry of Interior of the Slovak Republic
	National crime agency (naka)
	Presidium of Police Force, Criminal Police Bureau, Spectator Violence Unit, National Football Information Point
	Presidium of the Police Corps, Criminal Police Office, Department of Criminal Investigation
Slovenia	General police directorate
Spain	Policia nacional
	Nfip - policia nacional
	State Secretary for Security
	Comisaría General de Policia Judicial- Unidad Central de Delincuencia Especializada y Violenta- Brigada de Patrimonio Histórico
	Customs
Sweden	Customs
	The swedish police authority
Switzerland	Swiss Federal Office of Police fedpol

Source: EY/RAND Europe Study's elaboration

National Judicial Authorities

Overview of the stakeholders consulted from National Judicial Authorities

Country	Institution (n° of respondents)
Cyprus	Eurojust National Member
Estonia	Eurojust National Member
Germany	Eurojust National Member
Latvia	Eurojust National Member
Netherlands	Eurojust National Member
Norway	Eurojust National Member
Portugal	Eurojust National Member
Romania	Eurojust National Member
Slovakia	Eurojust National Member
Sweden	Eurojust National Member
Switzerland	Eurojust National Member

Source: EY/RAND Europe Study's elaboration

National Data Protection Authorities

Overview of the stakeholders consulted from National Data Protection Authorities

Country	Institution (n° of respondents)
Belgium	National Data Protection Authority
Bulgaria	National Data Protection Authority
Croatia	National Data Protection Authority
Cyprus	National Data Protection Authority
Estonia	National Data Protection Authority
Hungary	National Data Protection Authority

Lithuania	National Data Protection Authority
Poland	National Data Protection Authority
Romania	National Data Protection Authority
Slovenia	National Data Protection Authority

Source: EY/RAND Europe Study's elaboration

Focus groups

Benelux Agreement

Overview of the stakeholders consulted with respect to the Benelux Agreement

Country	Institution (n° of participants)
Belgium	Federal Police (2)
Luxembourg	Police Grand-Ducale (2)
Netherlands	Netherlands Defence Academy
Netherlands	Ministry of Justice and Security (2)
Netherlands	National Police (2)

Source: EY/RAND Europe Study's elaboration

Czechia-Germany Agreement

Overview of the stakeholders consulted with respect to the Czechia-Germany Agreement

Country	Institution (n° of participants)
Czechia	International police cooperation directorate (3)
Czechia	Cezch republic liaison officer
Germany	Police Academy Hamburg
Germany	Customs
Germany	Bavarian State Police
Germany	PCCC
Germany	Ministry of Finance (2)

Source: EY/RAND Europe Study's elaboration

France-Switzerland Agreement

Overview of the stakeholders consulted with respect to the France-Switzerland Agreement

Country	Institution (n° of participants)
France	Secrétariat général des affaires européennes
France	Direction de la Coopération Internationale (DCI) (2)
France	Service de la Justice et des affaires intérieures (2)
France	Police Nationale
France	Gendarmerie
Switzerland	Federal Police
Switzerland	Département de la sécurité, de l'emploi et de la santé (3)

Source: EY/RAND Europe Study's elaboration

Nordic Agreement

Overview of the stakeholders consulted with respect to the Nordic Agreement

Country	Institution (n° of participants)
Denmark	National Police (3)
Finland	National Police (3)
Iceland	National Police (3)

Country	Institution (n° of participants)
Denmark	National Police (3)
Finland	National Police (3)
Iceland	National Police (3)
Norway	National Police (2)
Sweden	Swedish Police Authority (4)
Sweden	Customs

Source: EY/RAND Europe Study's elaboration

Case study interviews

Overview of the stakeholders consulted as case studies

Country	Institution (n° of case study interviews)
Austria	*planned*
France	Ministry of the Interior, National Police, Gendarmerie (4)
Hungary	*planned*
Slovenia	Ministry of the Interior, Criminal Police Directorate (4)
Sweden	*planned*
Switzerland	Federal Police (2)

Source: EY/RAND Europe Study's elaboration

ANNEX 3: WHO IS AFFECTED AND HOW?

Main stakeholders impacted by the preferred policy option

EU citizens

The preferred policy option aim to support law enforcement officers in the exercise of their tasks against criminal offences, thereby contribute to enhancing the security and well-being of EU citizens.

Law enforcement authorities

In particular the law enforcement authorities of Member States that are responsible for the exchange of international information, and the law enforcement officers on the ground, essentially in intra-EU border areas, having access to information. Europol and its secure communication channel SIENA and CEPOL, would also be impacted.

Costs and benefits of the preferred policy option

Costs of the preferred policy option

The preferred policy option requires IT investments at national level, and an increased need for training of impacted law enforcement officials. Specifically, for those that have not already done so, national SPOCs and PCCCs will have to establish a CMS, and to roll-out Europol's SIENA to these structures, and to criminal investigators.

For a CMS, a one-size fits all cost estimation is impossible, as national costs are largely depending on system complexity, number of users, functionalities, licenses, infrastructure, etc. For Europol, the respective costs could be of EUR 150.000, without infrastructure and hardware costs.

Establishing a common minimum set of data that has to be made available for exchange, as well as establishing SIENA as the privileged channel of communication and defining common requirements for functionalities of the CMS is expected to have a very positive impact on the

overall efficiency of the access to and exchange of information. It can be expected that the exchange of information will become swifter, less time consuming, and overall less burdensome in view of the information that can reasonably be expected from counterparts in other countries. This has also been confirmed in various interviews with national stakeholders[156].

The possible costs associated with SIENA

Europol estimated that the implementation of the SIENA functions foreseen in the baseline scenario could costs individual Member States around EUR 50,000 on an annual basis over the next five to seven years for the implementation of SIENA web services.

The calculation is based on several assumptions: There is already an existing case management system technologically able to integrate with SIENA web services and the network infrastructure does not require additional investments. The average EUR 50,000 take into account EUR 30,000 to 40,000 for technical development and 10,000 to 15,000 EUR staff training and technical visits to/by EUROPOL.

Europol estimated that, on the side of the Member States, the most expensive cost item relating to SIENA would be its integration with national Case Management Systems.

For users of the SIENA web application the costs are mainly limited to maintaining the national connection point, whereas the maintenance of rack, server, encryption etc. would be under Europol's responsibility.

As the new functionalities would be made available incrementally, the learning curve would – as much as possible be levelled. This means that associated costs to 'learn' how to apply SIENA are expected to be marginal.

With the launch of SIENA BPL, Member States would be able to take advantage of their secure infrastructure which allows further extensions of SIENA without incurring costs related to technical upgrades and accreditation to EU-RES.

Based on previous experience in supporting Member States with implementation of the web services, Europol estimated their necessary budgetary to be around 1 Mio. Euro. This amount is expected to facilitate the integration of SIENA web services in Member States that do not yet use it, e.g. through technical guidance on SIENA.

However, the majority of participants of breakout session 1 indicated at the 2nd technical workshop that working time could be reduced to a moderate extent only. It was explained, though, that this reduction of working time related to the access to and exchange of information overall. The working time spent on tasks of rather administrative nature, however, can be expected to decrease to a large extent. As a consequence, law enforcement officials are expected to be able to spend an even larger share of their working time on actually contributing to 'solving' cases rather than managing them.

Overall, the positive impacts of the measures on the efficiency of law enforcement cooperation are expected to be balanced from an efficiency perspective – at least to some extent – by the investments and operational costs the measures foreseen under this policy option may necessitate. More specifically, this refers to the following types of costs:

- Investments in IT-infrastructure (both hard- and software), as well as its continuous maintenance (see textbox above);
- Staff costs relating to an overall increased workload due more effective law enforcement cooperation (i.e. judicial authorities being available within SPOCs 24/7, more cases being handled, albeit in a more efficient manner); and
- Time spent to train officials in relation to new legislative requirements, processes, IT tools, as well as language training.

[156] Interviews conducted on 27. and 28.05.2021, as well as 04., 07., and 08.06.2021

Moreover, additional infrastructure costs are expected to be incurred stemming e.g. from the increased use of electricity, the use of office space (e.g. rent, heating, depreciation of physical assets). Comprehensive quantitative evidence of the level of these costs is, however, not available.

With specific regard to necessary investments in IT-infrastructure and maintenance in the area of cross-border law enforcement cooperation, no evidence is available. However, the European Commission published a report in 2018 in relation to the re-use of public sector information which references estimates for necessary technical and administrative investment costs for a national IT-development and roll-out project relating to the re-use of data[157]. The data stems from Poland and is provided in the following table.

Illustrative example of IT-project costs

Cost item	Budget (EURm)
IT equipment, programs and licenses, computers and servers	1.17
Preparation of project, feasibility study	0.20
IT services, audits and tests, APIs	2.10
Legal services, translations, consulting	0.15
Salaries (experts for open standards, trainers, portal design, partners)	2.19
Other salary related costs	0.05
Training	0.27
Training material	0.03
Information and promotion	0.15
Total	**6.28**

Source: European Commission (2018)

The illustrative example provided in the table above should be treated very carefully: It does not relate to IT developments in the area of cross-border law enforcement, but merely gives an idea of the level of costs for an IT project. For comparative purposes: The 2020 German federal budget contained an item called "Police IT Fund" in relation to which EUR 4.38 million were allocated.[158] In addition, there is IT-related budget allocated in each of the 16 federal states. In Bavaria, for instance, around EUR 2.15 million were devoted to the procurement and rental of hard- and software in 2020[159]. A very rough estimate of the overall IT-budget allocated to the German police forces (both federal and state levels) could, therefore, be between EUR 28 and 39 million[160]. It could be assumed that around 20% of that budget is spent on IT that is also used in some shape or form in relation to cross-border law enforcement cooperation. This equals an amount of EUR 5,6 to 7.8 million – which is roughly in line with the estimate above from Poland.

Member States are expected to incur costs related to the common minimum set of data that has to be made available by all Member States for exchange. These costs relate to both the implementation of

[157] European Commission (2018): Study to support the review of Directive 2003/98/EC on the re-use of public sector information. See: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-support-study-revision-public-sector-information-directive

[158] Bundesregierung (2020): Bundeshaushaltsplan. Einzelplan 06. Bundesministerium des Innern, für Bau und Heimat p. 39. See: https://www.bundeshaushalt.de/fileadmin/de.bundeshaushalt/content_de/dokumente/2020/soll/epl06.pdf

[159] Freistaat Bayern: Haushaltsplan 2019 /2020. Einzelpna 03 für den Geschäftsbereich des Bayerischen Staatsministeriums des Innern, für Sport und Integration. p. 219. See: https://www.stmfh.bayern.de/haushalt/staatshaushalt_2019/haushaltsplan/Epl03.pdf

[160] The budget of the state levels could e.g. range between EUR 1.5 and 2.15 million.

the necessary IT systems, as well as the collection of statistics. The magnitude of costs per Member State depends on the extent to which the current systems are already aligned with the requirements foreseen under this policy option. The costs are, however, expected to be covered within the IT-related costs identified above.

In particular **streamlining awareness and knowledge across law enforcement officials** may be a time-consuming, and thus budget-heavy exercise. It has repeatedly been pointed out by stakeholders at both the EU and national levels throughout this study that the knowledge and operational skills among officials in relation to cross-border law enforcement cooperation in the EU is insufficient to fulfil the tasks at hand in the most effective and efficient manner.

Although CEPOL has been providing training over the past couple of years to an increasingly large number of officials (close to 40,000 in 2020), including in the area of law enforcement cooperation and information exchange, the share of officials that has already been (or much rather continuously is) trained in this regard is considered to be comparatively low given the large amount of officials potentially involved in cross-border law enforcement operations. It is expected that only between 1% and 3% of all officials have been trained with regard to cross-border matters so far.

As part of an interview, CEPOL indicated that additional budget has been requested for the coming programming period in relation to the delivery of relevant further volume of cybercrime related services, as well as further services on Artificial Intelligence (AI) and big data analysis.

- With regard to the former, CEPOL for 2022 expects an increase in the number of annual onsite of 270 plus 1,500 additional participants online compared to 2021. This would require – on top of the planned 2021 resources - an additional budget of 900,000 EUR and an additional 5 Fulltime Equivalents (FTEs) – more specifically 2 FTEs training officials, 1 Analyst, 1 eLearning official, and 1 ICT official).

- As concerns the latter, CEPOL estimated that this would require, as of 2023, additional budget around 750,000 EUR plus 4 FTEs – more specifically 2 FTEs training officials, 1 Analyst, 1 eLearning official, and 1 ICT official).

In addition to the efforts of CEPOL, Member States themselves are already taking initiative with regard to training – both in relation to information exchange and operational cooperation. For instance, it was reported during the 2nd technical workshop in May 2021 that Belgium and France have an agreement in place about the mutual training of 7,000 officials to improve law enforcement cooperation with particular regard to road and train transport, as well as large events. In addition to the costs related to this training, it was explained that budget is used to provide content via a platform, as well as software for phones and tablets. The French representative mentioned that their budget for a training app is around EUR 100,000.

While these examples only serve illustrative purposes and cannot be aggregated to the EU level since the impacts on the Member States are likely to vary vastly due to existing structures and systems, this gives an idea of the level of investments needed.

There are various additional non-legislative measures at EU level foreseen under this policy option that necessitate costs. In relation to these, the table below provides potential high-level estimates. These estimates need to be treated very carefully. They are based on expert judgment and the experience of the study team. Nevertheless, the estimates represent the best data available.

Estimates for addition costs at EU-level related to information exchange

Measure	Cost estimate in Euro
Provision of a matrix concerning which information channel should be used in what cases and provision of information concerning what data are available in the Member States (beyond the minimum required set).	50,000 – 75,000

Measure	Cost estimate in Euro
Internal Security Fund (ISF) support would be foreseen for the SIENA roll-out.	5.0 - 7.5 million
Feasibility study on how to improve the secure digital and radio communication between the Member States.	300,000 – 500,000
Financial support to the work of the EU innovation hub and of the RECG (Radio-communication Expert Group – Sub-group of the LEWP).	750,000 – 1.0 million
Establishment of an awareness raising and training campaign within the EU law enforcement community.	1.5 – 2.0 million
CEPOL to provide training material to law enforcement agencies, e.g. on how to use EU databases efficiently.	750,000 – 1 million
CEPOL to provide voluntary induction training on cross-border law enforcement.	200,000 – 400,000 annually
Expansion of the existing CEPOL practice to provide online courses on an ad-hoc basis on new EU level developments.	650,000 – 900,000
Performance of a regular review of the training content provided by CEPOL and updating of material	50,000 – 100,000 annually

Source: EY/RAND Europe Study's elaboration

Benefits of the preferred policy option

While the costs of the preferred policy option can be roughly estimated, a quantification of their benefits is more difficult to achieve. For instance, the benefit of gaining two weeks' time in obtaining an information from another Member State that will help solve a crime is difficult to quantify in monetary terms.

Establishing a common minimum set of data that has to be made available for exchange, as well as establishing SIENA as the privileged channel of communication and defining common requirements for functionalities of the CMS is expected to have a very positive impact on the overall efficiency of the access to and exchange of information. It can be expected that the exchange of information will become swifter, less time consuming, and overall less burdensome in view of the information that can reasonably be expected from counterparts in other countries. This has also been confirmed in various interviews with national stakeholders[161].

Indicative overview of possible costs – Preferred option						
	Citizens/Consumers		Member State Administrations		Union Agencies	
	One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Direct costs						
Case Management Systems in SPOCs	0	0	EUR 1.5m[162]	unknown	0	0
Case Management Systems in PCCCs and equivalent bodies	0	0	EUR 6.75m[163]	unknown	0	0

[161] Interviews conducted as part of the support Study on 27 and 28.05.2021, as well as 04., 07., and 08.06.2021.
[162] Only 10 MS are expected to invest in a CMS at SPOC (hence a possible indicative cost of EUR 150.000 per Member State.
[163] The set-up of CMSs in a maximum of 45 PCCCs would cost EUR 6,750 million (45x EUR 150.000).

SIENA integration in SPOCs CMSs	0	0	EUR 1m[164]	unknown	Unknown	Unknown
SIENA integration in PCCCs CMSs	0	0	EUR 2.25m[165]	unknown	Unknown	Unknown
Europol (including both policy options 3.2 & 3.3)	0	0	0	0	Unknown	EUR 1.7m as part of Agency' budget
Total	***0***	***0***	***€11.5m***	***unknown***	***unknown***	***unknown***
Indirect costs						
Training	0	0	0	As part of MS training budget + ISF support (via national programmes) *[Wide differences between MS needs]*	unknown	As part of Agency' budget

This EUR 11.5 million would be considered as a maximum **one-off** cost given that a number of PCCCs are already connected to the SPOC CMS. Hence the SIENA integration in the SPOC CMS would de facto cover the SIENA integration in the connected PCCCs.

ANNEX 4: SUPPORTING INFORMATION ON THE HIGH-LEVEL PROBLEMS AND THEIR IMPACTS ON THE CORE PROBLEMS

Security and cross-border crime are, by definition, an international issue. Most European countries agree that organised crime is a problem in their country.[166]

As made clear in the 2021-2025 EU Strategy to Tackle organised Crime[167] and the 2020 EU Security Union Strategy[168] organised crime is, and will remain, a significant threat – causing harms to citizens, businesses, society and the economy. While organised crime is not a new threat, it is a persistent and serious threat, and ever evolving to exploit opportunities for profit and evade detection and disruption.

Globalisation, as well as increasing economic and social integration have accelerated the interconnection between domestic illegal markets and increased mobility of criminals across national borders. Some of the initiatives that aimed to promote legal economic exchange, such as deregulation of transportation and trade liberalisation, also benefitted illegal economic

[164] Only 20 MS are expected to invest in this integration (hence EUR 50.000 per Member State).
[165] Out of the 59 identified PCCCs, 14 are already connected to SIENA. The SIENA connection to a maximum of 45 PCCCs would cost EUR 2,250 million (45x EUR 50.000).
[166] Paoli, L. and Fijnaut C. (2004) General introduction. In: organised *Crime in Europe: Concepts, Patterns and Control Policies in the European Union and Beyond* C. Fijnaut and L. Paoli (eds.) Dordrecht: Springer.
[167] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle organised Crime 2021-2025 (SWD(2021) 74 final).
[168] Communication from The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions on the EU Security Union Strategy COM(2020) 605 final

exchanges.[169] The steady increase in cross-border passenger and freight traffic means that only selective border controls are possible.[170] Within the Schengen area, internal border controls have been dismantled, meaning that travel and communication within the EU has become easier.[171] Technological advancements have created opportunities for new types of cross-border crime, as well as for modernising traditional forms of crime.[172] For example, the illicit drugs market has become increasingly global and uses digital technologies, such as selling drugs online.[173] The advancements and increased use of digital technologies also mean there is no longer a need for a perpetrator to be in the same location as a victim.[174]

Additionally, the increased mobility of persons across Europe means that there is a significant movement of EU citizens for the purposes of tourism, and that sports, social and cultural events are attended by persons from across the EU 27 and the Schengen Associated Countries (SAC), meaning that effective preventive and responsive actions need to involve cross-border cooperation. The growing intra-EU mobility of people – restrictions due to the COVID-19 pandemic set aside – creates additional challenges for the prevention and fight against all forms of criminal and safety threats. All this has a significant negative impact on the area of freedom, justice and security and calls for a stronger and streamlined cooperation among EU Member States and between their competent law enforcement authorities.

The rapidly evolving criminal landscape and the mobility of people suggests that cross-border cooperation between Law enforcement authorities in the EU and the Schengen area will be crucial to tackle criminal offences, ensure public order and safety and allow EU citizens to safely enjoy their rights of free movement in the future.

1. The international mobility of criminal networks, the evolution of cross-border serious and organised crime (SOC), and the increasing associated harms

Mobility of crime

The 2021 European Union Serious and organised Crime Threat Assessment (EU SOCTA) makes it clear that international mobility is defining characteristic of criminal networks and provides a detailed overview of the situation[175].

Some criminal operations have global reach beyond borders.

For instance, organised property crimes carried out in the EU continue to be perpetrated primarily by mobile organised crime groups (MOCGs). Mobility remains the key characteristic of these MOCGs and is used to avoid detection and minimise the risk of apprehension. MOCGs travel long distances and are typically active in several countries. They are highly flexible in the selection of

[169] Paoli, L. and C. Fijnaut (2004) General introduction. In: organised *Crime in Europe: Concepts, Patterns and Control Policies in the European Union and Beyond* C. Fijnaut and L. Paoli (eds.), pp. 1-18. Dordrecht: Springer.
[170] Wagner J. (2021) Transnational organised Crime (TOC). In: Border Management in Transformation. Advanced Sciences and Technologies for Security Applications. Springer, Cham. Available at: link.
[171] Sallavaci, O. (2018) Strengthening cross-border law enforcement cooperation in the EU: the Prüm network of data exchange. Eur J Crim Policy Res 24, 219–235. link.
[172] Grabosky, P. (2013) Organised Crime and the Internet, The RUSI Journal, 158:5, 18-25, DOI: 10.1080/03071847.2013.847707.
[173] Spapens, T. (2015) Transnational organised crime. *International Encyclopedia of the Social & Behavioral Sciences (Second Edition),* pp. 596-601. Available at: link.
[174] Peter Grabosky (2013) organised Crime and the Internet, The RUSI Journal, 158:5, 18-25, DOI: 10.1080/03071847.2013.847707
[175] Europol (2021) Serious and organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union, p. 34 & 35.

their targets and will often change their country of activity to evade law enforcement or to respond to changes in the criminal landscape[176].

Some locations feature characteristics that benefit serious and organised crime in the EU and beyond. These locations are used to facilitate a single or multiple criminal activities, sometimes simultaneously. Key locations attract criminals due to their geographic position, proximity to or connections with source countries and consumer markets. They may offer efficient transport infrastructures, business and investment opportunities or other advantages to criminals.

Criminal activities in border regions take advantage of the natural delineations of individual law enforcement jurisdictions, which create options to evade law enforcement and provide proximity to multiple markets. Within the Schengen Area, border travel is unimpeded, allowing free movement of persons across borders. Geopolitical developments determine the relevance of specific regions for the flow of goods and people. Humanitarian emergencies, bilateral agreements and risk-reward considerations determine the attractiveness of a specific border region or section for criminals.

Urban areas are characterised by a concentration of people and often present a multitude of criminal opportunities. Burglaries are concentrated in urban areas. Pickpockets target victims in crowded places such as concerts, markets, on public transport or at railway stations. Organised robberies typically take place in urban areas and border regions. Victims of trafficking in human beings are typically exploited in urban areas where there is a larger potential client base. Capitals and major cities act as hubs along the main migrant smuggling routes. Here, migrants are temporarily accommodated in safehouses, receive fraudulent documents, plan and initiate secondary movements.

Remote areas provide more anonymity conducive to other criminal activities. Illicit tobacco production lines are usually set up in large warehouses in remote industrial areas, close to transportation hubs like motorways, border crossing points or ports. Remote areas in the countryside are ideal locations for the dumping of chemical waste from synthetic drug production, toxic waste from fuel laundering and other waste products. Thefts of construction and agricultural machinery are more likely to occur in rural areas. Archaeological sites and places of religious worship situated in remote areas are targeted for theft and looting. Trafficking of human beings for labour exploitation often takes place in rural areas home to agricultural production.

Airports are key transit points for goods and people, both licit and otherwise. Criminals make frequent use of the EU's main airports as well as smaller regional airports operating low-cost airlines. In addition, small airfields offer convenient access to the EU and specific regions. Trafficking activities by air have been disrupted during the COVID-19 pandemic. However, expansion plans for many major airports signal a further growth in passenger flows after the end of the pandemic.

A dense network of well-maintained motorways facilitates the free movement of goods and services within the EU. It is also a major crime enabler allowing criminals to travel and move goods quickly and anonymously. Travel by road is the most accessible way of travelling within the EU. Transport means on the road include lorries, vans, buses, cars, caravans, or taxis. Some vehicles are equipped with sophisticated concealment methods to hide drugs and other contraband or persons. Motorway infrastructure is used for smuggling raw material to production facilities and for distributing illicit goods produced in the EU or arriving at entry points.

A dense network of well-maintained motorways facilitates the free movement of goods and services within the EU. It is also a major crime enabler allowing criminals to travel and move goods quickly and anonymously. Travel by road is the most accessible way of travelling within the EU. Transport

[176] Europol (2021) Serious and organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union, p. 86.

means on the road include lorries, vans, buses, cars, caravans, or taxis. Some vehicles are equipped with sophisticated concealment methods to hide drugs and other contraband or persons. Motorway infrastructure is used for smuggling raw material to production facilities and for distributing illicit goods produced in the EU or arriving at entry points.

Other illegal goods such as illicit waste, synthetic drugs produced in the EU, and stolen vehicles or parts are shipped throughout the world departing from EU ports.

Accelerated by the COVID-19 pandemic, the shipping of orders placed online fulfilled by post and parcel services continues to expand in volume every year. Postal and parcel services are abused for the distribution of illicit goods such as drugs (cannabis, cocaine, synthetic drugs including new psychoactive substances), counterfeit currency, stolen and fraudulent documents and many other illegal commodities.

Clandestine locations such as private or rented apartments are used as pop-up brothels where victims are sexually exploited, including children. Apartments serve as safe houses used to conceal irregular migrants in between different legs of their journeys.

Reception centres for asylum applicants are targeted by human traffickers and migrant smugglers to recruit irregular migrants and potential trafficking victims. Upon their entry into the EU, facilitated irregular migrants and victims of THB are often accommodated in reception centres where they apply for international protection.

Increasing and evolving serious and organised crime

The 2021 EU SOCTA also outlines a number of areas where SOC appears to be increasing. For example, the use of violence by criminals involved in SOC is assessed to be intensifying, unprecedented quantities of cocaine are trafficked into the EU from Latin America and criminal groups are increasing their capacities to produce and distribute synthetic drugs.[177] Information compiled by Europol in the 2021 EU SOCTA also indicates that there is a growing threat from cyber-dependent crime – both in terms of the number and sophistication of attacks.

In relation to the future need for law enforcement cooperation, the 2021 EU SOCTA outlines ways in which SOC is evolving. Many aspects of this evolution are linked to technology and the digitisation of society, which creates new opportunities for criminals. The recruitment of trafficked human beings, for example, often takes place online, and organised crime groups (OCGs) are making use of cryptocurrencies. Other aspects of the evolution are driven by avoidance of anti-organised crime measures. For instance, to avoid EU anti-money laundering measures, money laundering attempts are "likely to be displaced towards sectors with nascent controls or limited oversight".[178]

The way in which the COVID-19 pandemic has been exploited by OCGs demonstrates the inherently adaptive and flexible nature of SOC. As the EU SOCTA points out – and as highlighted in the 2021 Council Conclusions[179] – OCGs were quick to adapt to the COVID-19 crisis. They changed their *modi operandi* to exploit opportunities in the dynamic and uncertain environment, targeting individual citizens, businesses and the public sector by, for example, distributing

[177] Europol (2021) Serious and organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.
[178] Europol (2021) Serious and Organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union, p. 28.
[179] Council of the European Union. (2021). The impact of the COVID-19 pandemic on internal security: threats, trends, resilience and lessons learned for Law Enforcement Agencies: outcomes of previous discussion and draft Council Conclusions. Brussels: Council of the European Union.

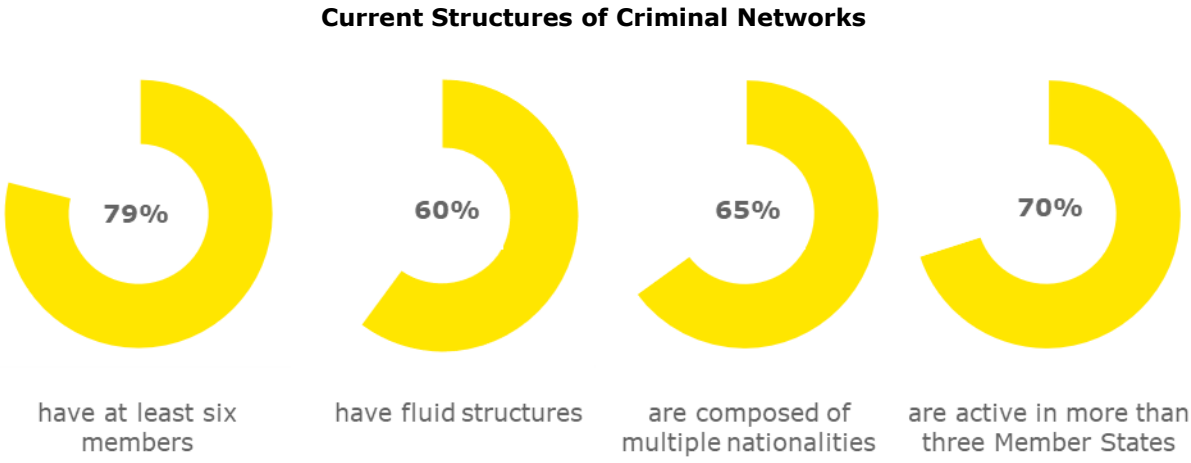
counterfeit and substandard personal protective equipment or performing phishing campaigns and ransomware attacks on healthcare organisations.[180]

The evolving nature of criminal networks

There is also evolution in the nature and size of criminal networks. Europol estimates that around one fifth of criminal networks are composed of no more than five members and are highly flexible. Most criminal networks do not follow strict hierarchical structures, but are rather loose and organic networks (see Figure 1 below),[181] which makes them difficult to disrupt and dismantle, and which means that these groups are more able to flex and adapt to exploit new opportunitites. For this reason, the 2021 EU SOCTA[182] lists high-risk criminal networks (including for corruption, money laundering and the use of firearms) as the most important crime threat facing the EU.

Criminal networks in the EU operate across national borders, exploit legal business structures and are highly flexible and adaptive. The 2021 EU SOCTA estimates that around 80% of the criminal networks engage in drug trafficking, organised property crime, excise fraud, human trafficking, online and other fraud and migrant smuggling.[183] Around 7 out of 10 operate in more than three countries and 65% involve individuals of several nationalities.

OCGs are opportunistic, for example, in exploiting innovations in transportation to develop new modes to traffic illicit goods.[184] As described above, this characteristic has also clearly shown during the COVID-19 pandemic. In general, OCGs tend to be flexible so as to mitigate risks, reduce operational costs and increase profit margins.



Source: EY/RAND Europe Study's elaboration based on Europol SOCTA 2021

The harms and security threat caused by organised crime

SOC causes economic harms. A 2013 study conducted for the European Parliament concluded that, at a minimum, the annual direct cost of organised crime activities in the EU was EUR 126.3 billion, with over EUR 35 billion in additional related costs.[185] Annual revenues from nine main criminal

[180] Europol (2020) How COVID-19-related crime infected Europe during 2020. The Hague: Europol; Europol (2020) Serious and organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.
[181] Europol (2021) Serious and organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.
[182] Europol (2021) Serious and organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.
[183] Europol (2021) Serious and organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.
[184] Europol (2015) *Exploring Tomorrow's organised Crime*. The Hague: Europol.
[185] Levi, M., M. Innes, P. Reuter & Gundur R. (2013) The Economic, Financial & Social Impacts of organised Crime in the EU. As of 8 December 2020: link.

markets[186] in the EU were estimated at between EUR 92 billion and EUR 188 billion in 2019[187] – between 0.66%-1.35% of the EU27 Gross Domestic Product (GDP).[188]

The analysis shows that the largest markets in terms of revenues were missing trader intra-community fraud (MTIC) fraud[189], illicit drugs, illicit tobacco (specifically cigarettes) and illicit waste. However, given the lack of figures on illicit markets, this quantification is likely an underestimation. The following table summarises low, mid, and high criminal revenue estimates for different criminal markets and years for the year 2019.

Headline criminal revenue estimates

Criminal markets and areas	Revenues, adjusted for inflation, 2019 (EUR million)		
	Mid	Low	High
Illicit drugs	30,688.41	26,708.13	35,514.56
Trafficking in Human Beings (THB) for sexual exploitation	7,185.93	401.94	13,969.91
Smuggling of migrants	289.37	215.60	363.15
MTIC fraud	77,425.00	50,858.00*	103,991.67
Illicit waste*	9,506.62	3,723.49	15,289.74
Illicit wildlife (European eels only)	18.05	4.71	31.39
Illicit firearms	408.09	273.69	753.96
Illicit cigarettes	8,309.15	8,012.62	10,087.48
Card payment fraud	1,816.43	-	-
Cargo theft*	3,347.86	144.39	6,551.32
ATM physical attacks*	22.00	-	-
Total	**139,016.91**	**92,181.00^**	**188,391.61^**

Notes: Estimates have been adjusted for inflation using price index data from Eurostat (2020). The low and high estimates have been generated using different methodologies, with each described in the annexes that support the market analyses. A common example is the use of a range of price data. In most cases, the mid estimate represents the mid-point (median) between the low and high value. These mid-point estimates should be interpreted with a high degree of caution because the distributions are not necessarily normally distributed, but have nevertheless been provided here for illustrative purposes.
* Denotes that the estimate does not include all 27 EU Member States: MTIC fraud lower bound estimate excludes HR and CY. Illicit waste estimates exclude BE, CY, LU, MT, SI. Lower bound cargo theft estimates exclude AT, BG, HR, CY, EE, FI, EL, LT, LU, ML, PL. Upper bound estimates exclude MT. ATM theft estimates exclude BE, BG, HR, EE, HU, LV, LT, MT, PL, SI. ^ Lower and upper boundary aggregate estimates presume card payment fraud and ATM attacks are equivalent to mid-level estimate.

Source: RAND Europe & EY for the EC (2021) Mapping the risk of SOC infiltrating legitimate businesses

These revenue estimates present only a limited picture of the complex consequences of how organised crime undermines the business environment and rule of law. The revenues generated by SOC are reinvested in further illicit activities or enter the legitimate economy, which undermines

[186] Illicit drugs, THB, Smuggling of migrants, Fraud, Environmental crime, Illicit firearms, Illicit tobacco, Cybercrime, organised property crime.
[187] RAND Europe & EY for the EC (2021) Mapping the risk of serious and organised crime infiltrating legitimate businesses.
[188] The EU GDP was EUR 13,900 billion in 2019. Eurostat (2020) *Which EU Countries had the highest GDP in 2019?* link.
[189] MTIC fraud is a form of VAT crime based on cross-border transactions. It requires Multilateral Tax Cooperation among Member States e.g. Council Regulation (EU) No 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added tax, MTIC is included within the EU priorities for the fight against serious and organized crime through EMPACT 2018-2021 & 2022-2025.

the business environment and leads to corruption as well as a lack of trust in institutions, while also negatively impacting the growth potential of the economy.[190] organised crime also undermines personal and state security, and threatens safety, stability and development - at the individual, local, national and transnational levels.[191]

Organised crime also results in direct costs to citizens' health and security.[192] For example, in relation to Trafficking in Human Beings (THB), victims (including children) are recruited into sexual exploitation and forced labour.[193] To control victims, traffickers use psychological and physical abuse. There is evidence that persons with developmental and physical disabilities are targeted, and some evidence that age of identified victims is decreasing, with children constituting nearly a quarter (23%) of the identified victims.[194].

Impact on free flow of persons across internal borders within the Schengen area

Organised crime has an indirect impact on the free movement of people within the EU. As concerns the reasons why Member States have introduced temporary controls at internal borders under Articles 25 and 28 of the Schengen Border Code[195], out of 300 notifications between October 2006 and the end of April 2021, on 24 occasions (8%) the reason given cited terrorist threats, on 6 occasions (2%) the reason was given as related to organised crime and 44 (15%) were for dealing with demonstrations/sports/summits etc. (this latter reason is relevant to the second high level problem, identified in the problem tree above). To put this in context, in nearly 170 cases (57%) the reason given was the COVID-19 virus – which was thus by far the most common reason given.

The Commission has, on several occasions[196], stressed that improved law enforcement cooperation and the use of police checks is a preferred compensatory measure to internal border control.

2. The growing intra-EU mobility of citizens and the interconnection of EU markets

The growing intra-EU mobility of people creates additional challenges for the prevention and fight against all forms of criminal and safety threats (e.g. in border regions, in relation to international mass events, in touristic areas and in case of mass disasters). The main factors behind and effects of this high-level problem are presented below.

EU mobility for work and leisure is increasing

[190] Europol (2021) Serious and organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.
[191] UNODC and UNICRI (2005) Trends in Crime and Justice: The evolving challenge of transnational organised crime, 25–54.
[192] RAND Europe & EY for the EC (2021) Mapping the risk of serious and organised crime infiltrating legitimate businesses.
[193] RAND Europe & EY for the EC (2021) Mapping the risk of serious and organised crime infiltrating legitimate businesses.
[194] European Commission. (2018). 'Second report on the progress made in the fight against trafficking in human beings (2018) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims'. Available at: link. European Commission. (2020). 'Report from the Commission to the European Parliament. Third report on the progress made in the fight against trafficking in human beings (2020) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims {SWD (2020) 226 final}'. Available at link.
[195] Member States' notifications of the temporary reintroduction of border control at internal borders pursuant to Article 25 and 28 et seq. of the Schengen Borders Code: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/borders-and-visas/schengen/reintroduction-border-control/docs/ms_notifications_-_reintroduction_of_border_control.pdf
[196] COMMISSION RECOMMENDATION of 12.5.2017 on proportionate police checks and police cooperation in the Schengen area C(2017) 3349 final

First, the intra-EU mobility continued to grow until the outbreak of COVID-19.[197] The number of people residing in an EU-27 Member State other than the one of their citizenship have been notably increasing over the years. The total amount of these people in the EU-27 amounted to 14,4 million persons in 2020 and increased by 22% since 2014.[198] It can be expected that a significant part of EU citizens is regularly crossing borders to travel back and forth between their Member State of residence and the Member Sate of citizenship and will continue to do so after the pandemic.

In 2017, the EU internal border regions covered approximately 40% of the EU's territory and were home to 30% of the population, i.e. 150 million people.[199] In 2018, the residents of the EU made in total 1.1 billion trips, either for business or privately – an increase of 11% since 2014.[200] In 2018, 240 million persons in the EU (64 % of the population) went at least on one private trip (as opposed to business trips), an increase by 4 % since 2012.[201] There has also been an increase in the number of EU citizens travelling for educational or training purposes.[202] Lastly, there has been an increase in intra-EU migration of EU citizens. In 2019, 3.3% of the EU citizens of working age (20-64) had a nationality of an EU Member State other than the EU Member State of residence, compared to 2.4 % in 2009.[203] Similarly, at SACs/EU air borders, Frontex estimated that there is an increase in passenger flows of about 5% per year across Europe.[204]

As regards cross-border tourism, the number of nights spent at tourist accommodation establishments in foreign Member States has been slightly increasing over the past decade, amounting to almost three billion in 2019.[205] As regards cross-border labour mobility, two million out of 190 million employed persons lived and worked outside their home Member State[206], and this number has also been increasing in the past decade. After the COVID-19 crisis, the cross-border mobility of citizens is expected to continue to increase in the EU. It can be expected that criminals are as well increasingly mobile across-borders. The fact that there are no border controls in the Schengen area enables criminals to cross-borders as they like without being subject of controls, which makes it more complicated for LEAs to monitor criminal activities. Moreover, criminals use the mobility of citizens and cross-border traffic to smuggle illegal goods or irregular migrants across-borders. As a reference, the Swindon Railway station, in the UK, is known to be a gateway for children smuggling drugs into London.[207]

Despite the fact that the COVID-19 pandemic has drastically reduced pan-European (and worldwide) mobility in 2020 and 2021, the flows of persons will likely continue to increase in importance again in the near future.

The movement of persons creates a need for law enforcement cooperation at the borders and beyond

[197] For intra-EU labour mobility, please see Eurostat (2021) People on the move. Available at link. Four cross-border tourism, please see Eurostat (2021) EU tourism halved in 2020. Available at link.
[198] Eurostat (2021) People on the move. Available at link.
[199] European Commission (2017) Boosting Growth and cohesion in EU border regions. Brussels: European Commission. Available at link .
[200] Eurostat (2020). *People on the move – statistics on mobility in Europe.* As of 8 April 2021: Available at link, p. 26.
[201] Eurostat (2020). *People on the move – statistics on mobility in Europe.* As of 8 April 2021. Available at: link, p. 28.
[202] European Commission. 2020. *Erasmus+ Annual Report 2019*. Luxembourg: Publications Office of the European Union. As of 8 April 2021: link, p. 32.
[203] Eurostat (2020) *EU citizens living in another Member State - statistical overview.* As of 8 April 2021: link.
[204] Frontex (2020) *Risk analysis for 2020*. Luxembourg: Publications Office of the European Union, p. 36.
[205] Eurostat (2021) Nights spent at tourist accommodation establishments by residents/non-residents. Available at link.
[206] Eurostat (2021) People on the move. Available at link.
[207] BBC News (2021) Swindon railway station as gateway for drug trafficking. Available at link.

Specifically at border regions, cooperation is needed, for example, to undertake transport control,[208] detain or pursue suspects crossing borders (travelling by car[209] or on public transport such as trains,[210] for example) and search for missing persons.[211] There is a daily need for law enforcement officials to be able to conduct "normal" and policing activities around and across borders regions.[212]

In addition to border regions, cooperation is needed in relation to demonstrations attended by international participants, state visits and summits, the protection of VIPs,[213] and sports and music events with international audiences.[214] Indeed, mass gatherings and public places remain a key target for terrorist attacks[215] - highlighting the threat to public safety and the need for continued cooperation.

In the case of international events with spectators, it is of vital importance to have close operational cooperation between the involved authorities "in order to ensure an overall situation picture and threat assessment".[216] The need for cooperation is thus an important part of the security policy at mass events.[217] An example of a recognised good practice where this does happen frequently is at football matches, where there is a history of law enforcement cooperation.[218]

The need to manage the pandemic is another issue, which has created an increased need for cooperation at the border over the last year,[219] and which highlights the interconnectedness of Member States and SACs – with the impacts on health and security cascading between countries. The movement of persons for tourism similarly creates a demand for law enforcement cooperation.

Cross-border mobility, in particular for touristic purposes after the COVID-19 pandemic, is expected to increase. A crucial enabler for this development is the effective and efficient management of public order and safety. Therefore, it can be expected that the measures foreseen under this policy option will have a positive economic impact, e.g. in terms of increased GDP in tourism-related industries.

Increasing interconnection of EU markets

The increasing mobility of EU citizens has been accompanied by an increasing interconnection of EU markets both within the EU and with the rest of the world. In times of global trade, international value chains and trade flows, trade between the EU market and other world's economies has become more and more interlinked. EU businesses have increasingly organised their production globally by breaking up their value chains into smaller parts to be supplied from worldwide providers. In the last five years, extra-EU imports have significantly increased by 16% to EUR 1 935 billion in 2019.[220] A relevant example of how world's economies are increasingly

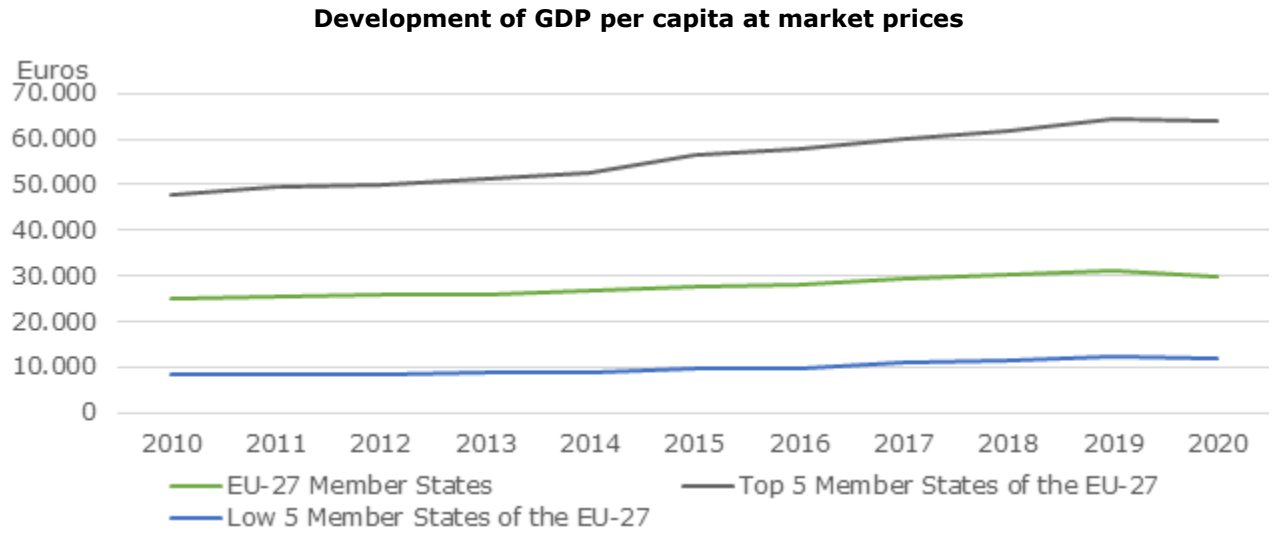
[208] Focus Group on FR-CH bilateral agreement.
[209] Focus Group on DE-CZ bilateral agreement.
[210] Focus Group on Benelux trilateral agreement.
[211] Survey: Q 92, 1 representative from a PCCC.
[212] Focus Group on Benelux trilateral agreement.
[213] Focus Group on Nordic multilateral agreement; Survey: Q 13A, 1 National EMPACT Coordinators (NEC), 2 representatives from public order departments/ National Football Info Points (NFIP) and 1 representative from a PCCC.
[214] Survey: Q 13A, 2 representatives from public order departments/NFIP and 1 representative from a SPOC.
[215] Europol. 2020. EU Terrorism Situation and Trend Report.
[216] Survey: Q 92, 1 representative from a public order department/NFIP.
[217] Council Document 13887/20 - Manual on cross-border operations. Available at: link.
[218] Council of the European Union (2016) Council Resolution concerning an updated handbook with recommendations for international police cooperation and measures to prevent and control violence and disturbances in connection with football matches with an international dimension, in which at least one Member State is involved ('EU Football Handbook'). *Official Journal of the European Union*, 444(01). link.
[219] Survey: Q 13A, 1 representative from a PCCC and one representative from a specialised investigative Unit; Q 92, 1 representative from a SPOC.
[220] Eurostat (2021) Extra-EU imports of main CPA groups, 2015-2019. Available at link.

interconnected is the major interruption of trade flows caused by one container ship blocking the Suez Canal in March 2021.[221]

As markets will likely continue to increasingly act globally and be interconnected, SOC is expected to globalise as well. As a reference, the cocaine drug market, the second largest illicit drug market in the EU after the cannabis market, is rapidly more acting at a global level and becoming more globally connected. On the one hand, serious and OCGs from different nationalities are increasingly entering the cocaine market in the EU. Whereas Colombian and Italian serious and OCGs played a central role in the cocaine market in the past, serious and OCGs are increasingly of e.g. Albanian, British, Dutch, French, Moroccan, Spanish and Turkish origin. On the other hand, European serious and OCGs are increasingly establishing presence in Latin American countries in order to better manage production facilities. As concerns the smuggling of cocaine, it is not only North Africa that is increasingly emerging as a significant transit point but also the EU, which is increasingly serving as a transit point for the cocaine markets in e.g. Australia, Russia and Turkey.[222] In the near future, it is expected that serious and OCGs will continue to rapidly exploit opportunities that are arising from the existence of global commercial markets and the related global logistical developments.

The increasing interconnection of the EU markets has not translated into higher levels of social equality across the EU; on the contrary, social and economic disparities between Member States continue to persist in the long term. In terms of GDP and economic growth, the disparity between Member States – particularly between the East-Central Member States and the former Member States – remains large. A clear example is the difference in terms of GDP per capita between Germany and Romania. According to Eurostat data, the GDP per capita in Germany had slightly increased in the last ten years and amounted to 40 070 Euros in 2020. In Romania, on the other hand, the GDP per capita, despite slight increases in the last ten years, amounted only to 11 270 Euros in 2020.[223] How large the economic disparities are is also visible when comparing the average GDP per capita of those five Member States with the highest GDP per capita with the average for the five Member States with the lowest GDP per capita. Whereas the GDP per capita of the top five is not just far higher in absolute terms, it has also increased more in the past decade than the average GDP per capita for the five Member States with the lowest GDP (see).[224] Economic disparities are an opportunity for criminals since it is increasingly attractive for them to travel to wealthier European regions and commit criminal activities there. For instance, during the tourist season, organised groups of young children from Romania are sent to Paris, Berlin, London etc. for pickpocketing among tourists.[225] It is expected that the economic disparities will likely not only persist but increase in the short term since a deep and severe recession at a global scale has been forecasted because of the COVID-19 pandemic.[226]

[221] BBC (2021) Suez Canal reopens after giant stranded ship is freed. Available at link.
[222] Europol/European Monitoring Centre for Drugs and Drug Addiction (2019) EU Drug Markets Report 2019. Available at link.
[223] Eurostat (2021) Gross domestic product at market prices. Available at link.
[224] Eurostat (2021) Gross domestic product at market prices. Available at link.
[225] Der Tagesspiegel (2016) So funktioniert das Netz der Taschendiebe. Available at link.
[226] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.



Source: EY/RAND Europe Study's elaboration based on Eurostat (2021)

A shift to the online world

Another relevant social development is the incessant digitalisation of lives and production. The shift to the online world is not a recent process; however, it underwent a without precedents acceleration after the outbreak of the COVID-19 pandemic. Before COVID-19, being online has already been a matter of course for many EU citizens with 85% of people using the internet at least once a week in 2020. Since 2014, these numbers have been moderately increasing by 10% until the pandemic has seen a large increase in internet use.[227] After having reached a peak during the health crisis, it is expected that the life of many EU citizens continues to take place online to a significant extent. Especially the prevalence of social media and online platforms is expected to increase. It is anticipated that leading private technology firms continue to dominate the digital market and to continue to retain their monopoly positions. The monopoly on personal data held by these private companies will continue to pose significant risks of criminal use of personal data.[228] As regards the work force, close to 40% of those currently working in the EU began to telework fulltime as a result of the pandemic in 2020.[229] It is likely that a significant part of these home-based workers will continue working remotely also after the end of the COVID-pandemic.

3. Evolution of the situation

Serious and organised crime, as well as situations critical for public order and safety are complex and multi-facetted phenomena whose evolution is affected by surrounding social and technological developments. Technological developments have a direct impact on the prevalence and severity of SOC and situations critical for public order and safety. Technology is used to facilitate terrorism attacks, to create more innovative criminal business models, and to enhance communication among criminals. Social developments expected to affect criminal threats in the next years are directly linked to the increasing interconnection of persons across the EU, which reduces, or even overrides, territorial distances, thus creating new opportunities for criminals to exploit.

It should be noted that technological and social developments affect both criminal networks and law enforcement agencies (LEAs). Criminals are, indeed, dynamic and quick to exploit the latest

[227] EU Commission (2020) Use of Internet and Online Activities. Available at link.
[228] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[229] Eurofund (2020) Living, working and COVID-19, COVID-19 series, Publication Office of the European Union. Available at link.

technological developments. As they manage to quickly adopt and integrate new emerging technologies into their *modus operandi*, criminals are able to ensure business continuity and can further expand their criminal activities.[230] Thus, LEAs face the challenge to keep pace with criminal groups. However, at the same time, LEAs can take advantage of and use new technologies to cope with evolving criminal patterns.

The criminal use of technological developments varies depending on the specific crime area. For instance, technology has been used to facilitate and improve terrorism attacks, to create more innovative criminal business models, to enhance communication among criminals, or to reduce chances of being caught. Specific examples of how new technologies may be exploited by criminal are:

- AI: AI can be applied to traditional criminal activities such as password guessing and social engineering in order to maximise profits in a shorter time.[231] LEAs, on the other hand, can use AI to forecast the likelihood and nature of criminal activities. For instance, a prefecture police in Japan has developed a tool to detect, analyse and predict the location and time for crimes and accidents based on data such as weather, past crimes in the area, urban mobility etc.[232]

- 3D Printing: as 3D Printing is becoming increasingly widely available, it can offer criminals new opportunities for firearm production and trafficking or for the trade in counterfeit goods.[233]

- Robotics: drones, which can be considered as advanced equipment in the field of robotics, are increasingly sold for private use and hence easily accessible for criminals. Criminals may use them for several activities, including corporate espionage. On their side, LEAs can use drones as patrol drones for prisons and borders.[234]

- New payment methods: blockchain and the emergence of different cryptocurrencies ensures anonymous online money transfers for criminals. Cryptocurrencies facilitate payments for transactions across all areas of cybercrime since reliability, irreversibility of transactions and anonymity have made cryptocurrencies as the default payment method for payments from victims to criminals (e.g. in the case of ransomware) or criminals to criminals (e.g. in the Dark web).[235]

In the following, illustrative examples in three crime areas[236] are presented, which show how criminals use the latest technological developments in different SOC areas and how the impact of such developments is likely to develop in the next years:

- **Cybercrime:** Nearly all criminal activities include some sort of cyber dimension. Especially during the COVID-19 pandemic, criminals have pushed innovation in the area of cybercrime by devising new *modi operandi* and by adapting existing ones to exploit the situation. For instance, with the increasing number of workers working remotely due to

[230] Europol (2017) Serious and organised crime threat assessment. Available at link.
[231] Europol (2020) Internet Organised Crime Threat Assessment. Available at link.
[232] Interpol/Unicri (2020) Towards responsible AI innovation. Available at link.
[233] Europol (2015) Exploring tomorrow's organised crime. Available at link.
[234] Interpol/Unicri (2019) Artificial intelligence and robotics for law enforcement. Available at link.
[235] Europol (2020) Internet Organised Crime Threat Assessment. Available at link.
[236] The two crime areas (cybercrime and financial crime) were selected based on responses from the online survey. These two crime areas are the areas with the highest shares of expected significant or slight increases in the next 5-10 years. Survey: Q 10, 87% (n=47) of LEA's respondents indicated that cybercrime will slightly or significantly increase, 75% (n=42) of LEA's respondents indicated that cybercrime will slightly or significantly increase.

COVID-19, criminals increasingly started compromising business emails and using Artificial Intelligence (AI) to mimic the voice of a CEO. Other examples of cybercrime attacks include ransomware or identity fraud. Despite the majority of cybercrimes being well known, criminals have often succeeded due to insufficient cybersecurity. It is expected that criminals will continue to invent and apply different forms of cybercrime in the near future, making cybercrime remaining as one of the most dynamic forms of crime.

- **Financial Crime:** It is expected that criminals will benefit from the latest technological developments and will increasingly commit financial crimes. The most prominent example of how criminals have used recent technological developments in the case of financial crime is non-cash payment fraud. In 2020, non-cash payment fraud increased as concerns the sophistication of social engineering and phishing. An example of financial crime during the COVID-19 pandemic is the abuse by criminals of the support and recovery funds, which some Member States established to stabilise their economies.[237] In Germany, for instance, around 25,000 suspected cases of coronavirus aid fraud were investigated in spring 2021.[238]

- **Drug trafficking:** Apart from small disruptions during the first lockdown, the drug trafficking has continued as usual.[239] Drug traffickers quickly adapted to travel restrictions and border closures by increasing their use of encrypted messaging services, social media apps, online sources and mail and home delivery services.[240] For instance, encrypted software based on Pretty Good Privacy and commercial encryption are commonly used among drug sellers and buyers.[241] In the near future, criminals are likely to further push innovation in drug production and trafficking methods, the establishment of new trafficking routes and the growth of online markets.

One important social development with respect to SOC is the persisting social and economic disparities between the Member States. In terms of GDP and economic growth, the disparity between Member States remains large.[242] At the same time, the national markets are increasingly interconnected both within the EU and with the rest of the world.[243] As the markets will likely continue to increasingly act globally and be interconnected, SOC is expected to further globalise as well. As noted in the previous section on the high-level problems, the cocaine drug market is becoming more globally connected as serious and OCGs from different nationalities are increasingly entering the cocaine market in the EU. Whereas Colombian and Italian serious and OCGs played a central role in the cocaine market in the past, serious and OCGs today are more often of e.g. Albanian, Moroccan, Spanish and Turkish origin.[244] It is expected that serious and OCGs will continue to rapidly exploit opportunities, which are arising from the existence of global commercial markets and the related global logistical developments. LEAs, on the other hand, will with some certainty at the same time increase their capabilities to fight the prevalence and severity of SOC, also in light of the increasing availability and possibilities of advanced technologies.

As concerns situations critical for public order and safety, one example of technological developments for political or sports mass gatherings is the use of new technologies, such as end-to-end encrypted communication apps, exploited by e.g. hooligans travelling across-borders to attend

[237] Europol (2021) Serious and organised Crime Threat Assessment: A corrupting influence, European Union.
[238] Deutsche Welle (2021) COVID aid: Germany uncovers over 25,000 cases of fraud. Available at link
[239] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[240] EMCDDA (2021) European Drug Report 2021. Trends and Developments. Available at link.
[241] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[242] Eurostat (2021) Gross domestic product at market prices. Available at link.
[243] Eurostat (2021) Extra-EU imports of main CPA groups, 2015-2019. Available at link.
[244] Europol/European Monitoring Centre for Drugs and Drug Addiction (2019) EU Drug Markets Report 2019. Available at link.

and riot at football matches.[245] In recent years, the nature of terrorist attacks at mass gatherings has shifted to attacks being carried out by single individuals with little preparation and easily available weaponry.[246] It is expected that this threat will increase, particularly as the latest technologies can be misused, e.g. in the case of malicious use of drones.[247] As LEAs are expected to increasingly cooperate to ensure public order and safety during political mass gatherings or to prepare for terrorist attacks, they will likely continue to face operational technological challenges for cross-border cooperation, which stem from limited interoperability of the databases and IT systems in place.[248]

Social developments with respect to situations critical for public order and safety mainly relate to the fact that intra-EU mobility continued to grow until the outbreak of COVID-19.[249] As regards cross-border labour mobility, two million out of 190 million employed persons lived and worked outside their home Member State in 2020[250], and this number has also been increasing in the past decade. As concerns cross-border tourism, it has continuously intensified in the last decade, but halved in 2020 compared to 2019 due to COVID-19.[251] After the COVID-19 crisis, the cross-border mobility of citizens is expected to continue to increase again in the EU. It can be expected that criminals are also increasingly mobile across-borders and are likely to use the mobility of citizens and cross-border traffic to smuggle illegal goods or irregular migrants across borders.[252] The fact that there are no border controls in the Schengen area enables criminals to cross borders as they like without being subject to controls, which makes it more complicated for LEAs to monitor criminal activities.

To conclude, technological and social developments are expected to continue to affect both serious and OCGs and LEAs. As criminals are likely to continue to be quick to exploit the latest technological and social developments, LEAs will likely face the challenge of keeping pace with criminal groups. In the near future, the problems are therefore expected to evolve in a steady manner.

Impacts of high-level problems on the core problems

The rapidly evolving criminal landscape suggests that cross-border cooperation between LEAs in the EU and the Schengen area will be crucial to tackle SOC, ensure public order and safety and allow EU citizens to safely enjoy their rights of free movement in the future. As detailed above, the cross-border element of threats posed by SOC in the EU is becoming increasingly important. This is mainly due to: (i) the evolution of the nature and *modi operandi* of intra-EU OC groups that are more and more characterised by a networked environment, where cooperation between criminals is fluid, systematic and of a cross-border nature; and to (ii) new and emerging crime opportunities, which are not limited to single Member States or SAC. Yet, the increasing intra-EU mobility calls for coordination among Member States in order to ensure effective policing activities towards the prevention of threats to public order and safety, for instance in case of international and mass-gathering events.

[245] BBC News (2016) Euro 2016: Who is to blame for the Marseille violence. Available at link.
[246] BBC News (2015) Paris attacks: What happened on the night. Available at link.
[247] EU Commission (2020) A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond. Available at link.
[248] Technical workshop held on 24 March 2021.
[249] For intra-EU labour mobility, please see Eurostat (2021) People on the move. Available at link. Four cross-border tourism, please see Eurostat (2021) EU tourism halved in 2020. Available at link.
[250] Eurostat (2021) People on the move. Available at link.
[251] Eurostat (2021) Nights spent at tourist accommodation establishments – monthly data. Available at link.
[252] BBC News (2021) Swindon railway station as gateway for drug trafficking. Available at link.

However, there is evidence that **the current intra-EU law enforcement cooperation suffers from uncertainties and inefficiencies that hinder the deployment of a coordinated response and leaves room for vulnerabilities**.

The following sections show how current cross-border law enforcement cooperation is not fully suitable to face emerging security threats and point out existing issues in relation to information exchange. The analysis covers the nature and scale of the problems identified, shows the shortcoming of the existing cooperation measures and practices and describes the challenges that remain to be addressed.

Overview of the drivers and issues behind core problem #1

Key drivers behind Core Problem 1 - The access to and exchange of necessary information among law enforcement authorities is subject to legal, technical and structural challenges	
Legal driver: Law enforcement authorities face difficulties in interpreting and implementing relevant EU provisions	• The scope of application of some EU measures is unclear, including between (i) the Swedish Framework Decision (SFD) vs. CISA (i.e. preventive and/or repressive operations) and (ii) the SFD vs. the Naples II Convention (whether only police or also customs authorities can use both these measures) • There is no requirement to ensure that a common minimum set of data is made available for exchange • Deadlines are usually not met when a judicial authorisation is required to deliver the requested information. There is no obligation to have a judicial authority available 24/7 within the Single Points of Contact, thereby slowing down the judicial authorisation process where needed. • The distinction between urgent and non-urgent cases provided for in the SFD and the SFD forms to be used (on a voluntary basis) for information exchange is unclear and (unnecessarily) complex • The Swedish Framework Decision is not aligned with the 2016 Law Enforcement Data Protection Directive
Technical driver: Law enforcement authorities have insufficient knowledge of existing mechanisms, skill gaps and outdated IT infrastructure	• SPOCs/Police Customs Cooperation Centres (PCCCs) are not always equipped with the necessary information management tools (e.g. a case management system with common dashboard and automatic/semi-automatic data upload and cross-check) • The use of rudimentary search tools hampers the adoption of transliteration and "fuzzy logic" search • Law enforcement officials on the ground do not always use secure communication means
Structural driver: National and regional information hubs set up by law enforcement authorities have different roles, means and capabilities which make their cooperation sub-optimal	• SPOCs/PCCCs do not always play their coordination role and lack resources to face the increasing number of requests • Information from (i) different units within the SPOCs and (ii) from the PCCCs (and equivalent structures at the border area) is not always integrated in the SPOC information management system • Direct and user-friendly access to all relevant EU and international databases and platforms is not the norm in the SPOCs and the PCCCs • The specific national stakeholders entitled to access and use EU and international databases and platforms vary between the Member States • National LEAs have limited awareness and knowledge of relevant databases • There is limited availability of training for law enforcement staff involved in cross-border information exchanges and cooperation • The choice of channel for information exchange lies with the Member States, leading to a duplication of requests in some cases

Key drivers behind Core Problem 1 - The access to and exchange of necessary information among law enforcement authorities is subject to legal, technical and structural challenges	
	• Language barriers hamper the efficient cross-border exchange of information

Source: EY/RAND Europe Study's elaboration

****

Examples of criminal activity in the EU and their evolution

The following three examples of criminal activity in the EU illustrate recent trends in criminal threats and give indications about likely future developments.

As long as travel restrictions are in place due to the pandemic, **criminals are producing and selling fake COVID-19 test certificates in the EU.** Europol warns that fraudsters are able to produce high-quality counterfeit or fake documents with high-quality printers and different software. Recent examples include:

- In France, a forgery ring was dismantled at the Charles de Gaulle Airport, which sold negative test results to passengers for EUR 300.
- In Spain, fraudsters were apprehended who sold fake test results for EUR 40.[253]

In France, almost thirty hospitals were targeted by cyberattacks in 2020, while these hospitals struggled with COVID-19 patients. During these cyberattacks, malware paralysed the IT systems in hospitals, which often did not have sufficient security systems in place, until hospitals pay high ransoms. During a recent malware attack in Villefranche-sur-Saône near Lyon, operations were slowed down. While the lab and machines could operate, the hospital staff could not process results through computers. This forced them to send notifications around in the hospital manually on paper and increased the burden on health workers already dealing with the high pressure of COVID-19. Since the beginning of 2021, French authorities have monitored no less than one cyberattack per week against French hospitals.[254]

A cross-border investigation of the Spanish Civil Guard, the Dutch Police, the United States Homeland Security and Europol **dismantled an OCGs trafficking cocaine from South America to Europe**. Latin American criminal networks are increasingly collaborating with international EU-based criminal networks for cocaine shipping. In this case, the international cocaine cartel extended over Amsterdam, Papendrecht, Rotterdam, Utrecht, Valencia and Malaga. During the operation, the LEAs seized six tonnes of cocaine, jewellery, cash and encrypted devices. It is assumed that the cocaine cartel communicated via self-developed encrypted mobile applications.[255]

Key relevant social and technological developments

Social and technological developments affect everyone, the citizens, the criminal groups and the law enforcement authorities.

How do criminals use the latest social and technological developments?

The criminal use of social and technological developments varies depending on the specific crime area; thus, the impact of such developments on different crime areas in the next years is likely to vary as well.

Expected impact of social and technological developments per crime area relating to criminals

[253] Europol (2021) Europol warning on the illicit sale of false negative COVID-19 test certificates. Available at link
[254] VOA (2021) Along with COVID, France's Hospitals Battle Cyberattacks. Available at link.
[255] Europol (2020) Cocaine Cartel shipping from South America busted in Spain and the Netherlands. Available at link.

Crime area	Criminal use of social and technological developments
Cybercrime	Nearly all criminal activities include some sort of cyber dimension.[256] Especially during the pandemic, criminals pushed innovation in the area of cybercrime by devising new modi operandi and by adapting existing ones to exploit the situation. For instance, with the increasing number of workers working remotely due to COVID-19, criminals increasingly started compromising business emails and using AI to mimic the voice of a CEO.[257] Other examples of cybercrime attacks include ransomware, where criminals increase pressure by threatening publication of data if the victim does not pay or identity fraud, where criminals misuse personal information to commit crimes.[258] Online frauds are further facilitated by the fact that criminals do not need to leave their place but either commit cybercrime anywhere in Europe or send other people across-borders in order to commit crime. Despite the majority of cybercrimes are well known, criminals have often succeeded due to insufficient cybersecurity.[259] It is expected that criminals will likely continue to invent and apply different forms of cybercrime in the near future, making cybercrime remaining as one of the most dynamic forms of crime. More specifically, the following types of future trends and dynamics can be identified: • Cybercriminals increasingly work together to maximise their profits, which could result in more offerings, more diverse products and services, increased specialisation, and more integrated packages of CaaS. • Cybercrime could become a more viable career for able hackers if criminal justice responses cannot keep up. • Cybercriminals could be driven deeper underground.
Financial crime	It is expected that criminals will likely benefit from the latest technological developments and will likely increasingly commit financial crimes. The most prominent example of how criminals have used the latest technological developments in the case of financial crime is non-cash payment fraud. In 2020, non-cash payment fraud increased in sophistication of social engineering and phishing. As was the case for cybercrimes, criminals have quickly adapted to the social development that life increasingly shifts to the online world. Especially attacks via mobile phones have gained importance among criminals and are expected to increase. For instance, smashing attacks increased during the pandemic, where criminals send fraudulent text messages, pretending to be from trusted senders, to financial institutions and their customers.[260] Another recent example of financial crime during the pandemic is the abuse of the support and recovery funds by criminals which some Member States have established to stabilise their economies.[261] In Germany, for instance, no less than 25 000 suspected cases of coronavirus aid fraud are currently investigated.[262] More specifically, the following types of future trends and dynamics can be identified • There is an emerging trend towards fraudulently trading intangible goods and services, such as cloud computing. • Due to Brexit, VAT fraud will likely be displaced to other countries.
Drug trafficking	As drugs can be increasingly purchased online in the Dark web and are delivered across Europe via parcel services, it becomes easier for consumers to access drugs.

[256] Europol (2020) Internet Organised Crime Threat Assessment. Available at link.
[257] Ibid.
[258] Ibid.
[259] Ibid.
[260] Europol (2020) Internet Organised Crime Threat Assessment. Available at link.
[261] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[262] Deutsche Welle (2021) COVID aid: Germany uncovers over 25,000 cases of fraud. Available at link

Crime area	Criminal use of social and technological developments
	The pandemic has barely impacted this development. Apart from small disruptions during the first lockdown, the drug trafficking has continued as usual.[263] Criminals are expected to remain quick to take advantage of new opportunities and to continue to make the drug market digitally enabled.[264] Also, the drug market is increasingly globalising. For instance, Mexican drug cartels have recently set up crystal meth production with Chinese chemicals in the Netherlands.[265] More specifically, the following types of future trends and dynamics can be identified: • Drug producers are maximising their production outputs by using new technologies, such as climate-control systems or solar-powered tube wells. • Herbal cannabis, synthetic drugs and precursors are increasingly produced illegally in the EU. These drugs markets are becoming more profitable, due to regulatory loopholes and global commercial trafficking routes. • Online trade is becoming more prevalent in drug markets in Europe.
Illicit tobacco trade	As markets will continue to increasingly act globally and continue to be increasingly interconnected, criminals are expected to commit smuggling operations at a global scale. For instance, a recent fraud scheme detected by Europol consisted of illegally diverting cigarettes from EU internal and external transit customs procedures to the black market without paying millions in taxes.[266] More specifically, the following types of future trends and dynamics can be identified: • Tobacco products are more often smuggled in smaller shipment sizes. • There is an increase in illicit domestic manufacturing. • Tobacco products other than cigarettes are expected to increase their market share.
THB	THB has witnessed a constant development in the EU in recent years. In 2018, no less than 14 000 victims were registered in the EU.[267] As long as COVID-19 prevails, the likelihood of THB is expected to decrease. In the long term, the social development that cross-border mobility is increasing and that borders in the Schengen area not subject to controls make it easier for criminals to smuggle human beings from one EU Member State to another. As soon as cross-border mobility reaches at least pre-crisis levels, THB in expected to go up again since there is persistent demand for low-wage workers employed in manual jobs.[268] As concerns technological developments, it is expected that the use of online platforms and services to identify and advertise victims continues to increase in the long term.[269] Furthermore, as identity fraud becomes increasingly sophisticated, traffickers are expected to increasingly use stolen personal data to provide trafficking victims with new identities, which are unlikely to fall within risk categories of LEAs.[270] More specifically, the following types of future trends and dynamics can be

[263] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[264] European Monitoring Centre for Drugs and Drug Addiction, Europol (2019) EU Drug Markets Report. Available at link.
[265] NDR Info (2021) Der grosse Sprung – Wie mexikanische Drogenkartelle nach Europa draengen. Available at link.
[266] Europol (2020) Customs thwart illegal cigarette trade in the EU and UK: 17 arrests and 67 million cigarettes seized. Available at link.
[267] European Commission (2020) Data collection on trafficking human beings in the EU. Available at link.
[268] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[269] Ibid.
[270] Europol (2015) Exploring tomorrow's organised crime. Available at link.

Crime area	Criminal use of social and technological developments
	identified: • Traffickers are increasingly making use of psychological and emotional violence and threats, rather than physical abuse, to control victims. • People with developmental and physical disabilities are increasingly being targeted. • The age of identified victims is decreasing. • Traffickers continue to rely on social media, VoIP and instant messaging. • Traffickers increasingly use legal businesses that can conceal exploitation, such as hotels and massage parlours.
Organised property crime	As long as COVID-19 prevails, the likelihood of organised property crime at private buildings is expected to decrease since people spend more time at their places. Commercial premises and medical facilities, on the other hand, are expected to be increasingly targeted.[271] In the long term, criminals are expected to increasingly use e.g. drones in order to survey residential areas and to look for suitable properties to target. More specifically, the following types of future trends and dynamics can be identified: • Domestic burglary, robberies and cargo theft are expected to rise slightly or stabilise. • Motor vehicle theft is expected to stabilise. • Profitable and incidences of cultural goods trafficking are expected to continue to grow. • Social media and GPS allow thieves across all organised property crimes to monitor targets and plan routes. • Online platforms are more and more used to sell loot anonymously.
Environmental crime	A short-term social development relates to COVID-19 waste crime. Since the outbreak of the COVID-19 pandemic, there has been an increase in growth in unlawful sanitary waste treatment and disposal.[272] In the long term, it is expected that this criminal activity will decrease and go down to pre-crisis levels. As concerns technological developments, the increasing reliance on technology in all areas of life and the built-in obsolescence for many devices generate unprecedented amounts of e-waste in the form of e.g. discarded devices, which is increasingly exploited by OCGs. Electronic devices containing precious metals such as gold or palladium are trafficked on a global scale just like drugs or firearms. In the long term, the illicit trade in e-waste is expected to grow both in terms of quantities traded and in the quality of the methods used by criminals.[273] More specifically, the following types of future trends and dynamics can be identified: • Illegal waste shipments are re-routed to emerging important countries, especially in South and South-East Asia, since the ban of solid waste important by China in 2018.

[271] European Parliament (2020) Organised Property Crime in the EU. Available at link.
[272] Europol (2020) COVID-19 Waste crime: Europe-wide operation to tackle unlawful sanitary waste disposal. Available at link.
[273] Europol (2015) Exploring tomorrow's organised crime. Available at link.

Crime area	Criminal use of social and technological developments
	• Waste Electrical and Electronic Equipment and end of life vehicles are emerging sub-markets in the illegal waste market.
Trafficking of firearms	The development of firearms trafficking has been rather constant in the EU in recent years.[274] The increasing trade globalisation, the absence of border controls inside the EU and the availability of new and anonymous payment methods will likely increase trafficking of firearms in the future. Moreover, the technological development of 3D printing enables criminals to exploit new opportunities for firearm trafficking.[275] More specifically, the following types of future trends and dynamics can be identified: • There is an increased availability of weapons. • The dark net is increasingly used to sell firearms. • Conflict areas were and still are a source of illicit firearms.
Illegal immigration	Illegal immigration has been continuously increasing in the recent past with a peak during the refugee crisis in 2015 and is expected to continue to increase.[276] The increasing exploitation of Big Data and personal data enables criminals to carry out complex identity frauds.[277] For instance, criminals can sell these stolen identities to irregular immigrants who wish to enter the EU. As long as COVID-19 prevails, the likelihood of illegal immigration is expected to slightly decrease. However, in the long term, technological developments in relation to identity frauds enable criminals to increase the severity of crime in the area of illegal immigration. More specifically, the following types of future trends and dynamics can be identified: • The routes taken and country of origin evolve over time. The Eastern Mediterranean route is expected to remain a focus of the smuggling of migrants. • Hubs where demand and supply of smuggling services meet are rather stable over time. • There can be an increase in the number of fraudulent documents as part of an increase in the abuse of legal channels to get into the EU.

Source: EY/RAND Europe Study's elaboration based on desk research

How do LEAs use technological developments and how are they affected by the latest social developments?

Social developments affect to all areas of SOC, requiring LEAs to increasingly cooperate across-borders. Especially in the long-term, social developments such as increased intra-EU mobility and increasingly globalised criminal markets will put LEAs in front of operational challenges. Notably, the increasing prevalence and severity of SOC will likely require LEAs to involve more offices and officials, to invest more time and to handle higher costs caused by more and more intense joint operations. Particularly the shift to the online world will put LEAs in front of operational challenges. The increasing digitalisation and use of social media go hand in hand with the increasing spread of misinformation, fake news and conspiracy theories. Europol anticipates that the

[274] EU Commission (2021) Trafficking in firearms. Available at link.
[275] Europol (2015) Exploring tomorrow's organised crime. Available at link.
[276] Statista (2021) Number of illegal entries between border-crossing points (BCPs) detected in the European Union (EU) from 2009 to 2019. Available at link.
[277] Europol (2015) Exploring tomorrow's organised crime. Available at link.

use of deep fakes will become a serious challenge for the digital environment.[278] However, LEAs have limited powers to counter this information manipulation which can in the end distort political discourse or manipulate elections.

As regards **technological developments**, in the short term, LEAs face operational challenges such as limited interoperability of national law enforcement databases and limited knowledge of available databases[279]. These challenges could reasonably remain prominent in the near future but are expected to decrease in the long term. As these operational technological challenges decrease, LEAs will with some certainty increase their capabilities to fight the prevalence and severity of SOC in the long term, also in light of the increasing availability of advanced technologies which can be used by them. Looking at robotics as a reference, LEAs are expected to increasingly use drones as patrol drones at borders. For instance, Frontex considers observing refugees in the central and eastern Mediterranean with drones developed by the military[280], whereas this form of surveillance is already common practice in the United States.

AI has emerged as the most promising technology to enhance law enforcement surveillance.[281] The application of AI technology will likely increase as LEAs aim to rely on a more data-driven approach to criminal investigations. The expected result of this is that LEAs will enhance detection rates and will more often succeed in detecting complex structures of criminal activity when combatting serious and OCGs. The following illustrative cases show how AI can be applied in different areas of SOC and how it continues to gain importance in the near future:

Overview of potential uses of AI by LEAs for different crime areas

Crime areas	Potential use of AI by LEAs
Cybercrime, financial crime, THB, illegal immigration	AI can be used to combat online child sexual abuse or terrorist use of social media.[282]
Organised property crime, environmental crime, illicit tobacco trade, illegal immigration, THB	AI and robotics can be used for robotic patrol and surveillance systems.[283] It should be noted that in the recently adopted proposal for an AI Regulation, the use of AI systems for real-time remote biometric identification of natural persons in public spaces – which is considered as particularly intrusive in relation to the rights of freedoms – is allowed in a few narrowly defined situations.[284]
Illicit tobacco trade, drug related crimes, THB, trafficking of firearms	AI can be used for autonomous research, analysis and reply to requests for international mutual legal assistance.[285]
All areas of SOC:	AI can be used to forecast where and what types of crimes are likely to occur in order to optimize law enforcement resources.[286]

[278] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[279] Technical workshop held on 24 March.
[280] Euractiv (2020) EU signs €100m drone contract with Airbus and Israeli arms firms. Available at link.
[281] On 21 April 2021, the EU Commission adopted a proposal for the Artificial Intelligence Act. This proposal highlights the important role of AI in the future and explicitly discusses the use of AI in the case of law enforcement. For further details, see EU Commission (2021) Artificial Intelligence Act. Available at link.
[282] Interpol (2020) Artificial intelligence and law enforcement: challenges and opportunities. Available at link.
[283] Interpol/UNICRI (2019) Artificial intelligence and robotics for law enforcement. Available at link.
[284] EU Commission (2021) Artificial Intelligence Act. Available at link.
[285] Interpol/UNICRI (2019) Artificial intelligence and robotics for law enforcement. Available at link.
[286] Ibid.

Source: EY/RAND Europe Study's elaboration based on desk research

How do citizens and businesses use technological developments and how are they affected by the latest social developments?

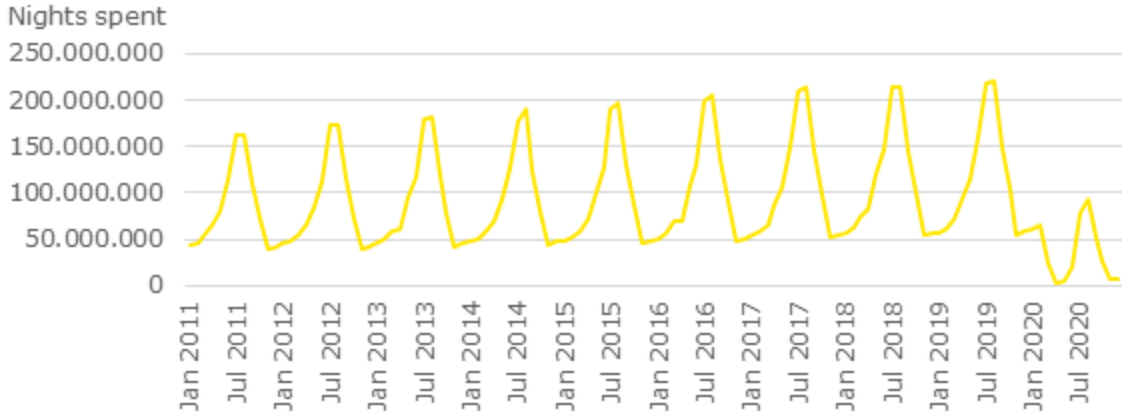
Most sport and mass gathering events have been cancelled since the outbreak of the pandemic and are cancelled or postponed in the upcoming months. It remains unclear to what extent a crowd will be allowed to attend the e.g. European Soccer Championship 2021 or Wimbledon 2021. Due to the pandemic, businesses are expected to increasingly rely on digital tools for visitor management, which can be exploited for criminal purposes, e.g. through cyber-attacks. In the long run, it is assumed that mass sports events will take place without COVID-restrictions in the EU.[287] For instance, the 2024 Summer Olympics and the 2023 *Fédération Internationale de Football Association* (FIFA) Women's World Cup are expected to take place under pre-crisis conditions. As concerns relevant social developments, likely challenges to public order and safety can be primarily linked to increasing cross-border mobility of sports fans travelling to other Member States and SACs in order to attend matches. At the same time, likely challenges to public order and safety could be linked to the use of new technologies such as end-to-end encrypted communication apps, exploited by e.g. hooligans travelling across-borders to attend and riot at football matches as was the case during the Union of European Football Associations (UEFA) Euro 2016 riots.[288]

A similar argument applies to mass cultural events and political mass gatherings. Likely challenges to public order and safety can be linked, on the one hand, to the use of technologies such as end-to-end encrypted communication apps by event attendees/organisers and, on the other hand, to ransomware attacks by criminals in order to commit identity fraud of ticket purchasers. An example for identity fraud is the online theft of personal details of 64000 visitors of the Tomorrowland festival in Belgium.[289] As concerns social developments, likely challenges to public order and safety can be primarily linked to increasing cross-border mobility. For instance, an example of a threat to public order and safety were political activists who travelled to Hamburg from across entire Europe during the G20 summit in 2017.[290]

As previously detailed in this section, cross-border mobility has noticeably increased in the past decade with e.g. increasing cross-border commuting and constantly increasing cross-border tourism. As concerns cross-border tourism, it has continuously increased in the last decade but halved in 2020 compared to 2019).[291] After the COVID-19 crisis, it is expected that tourism will be at least back to pre-crisis levels once borders are open again and quarantine rules are manageable for tourists.

[287] Technical workshop held on 24 March.
[288] BBC News (2016) Euro 2016: Who is to blame for the Marseille violence. Available at link.
[289] The Brussels Times (2018) Hackers steal personal details of 64,000 Tomorrowland visitors. Available at link.
[290] Deutsche Welle (2017) After G20: A look at left-wing radicalism in Europe. Available at link.
[291] Eurostat (2021) Nights spent at tourist accommodation establishments – monthly data. Available at link.

Development of the number of nights spent at tourist accommodation establishments by non-residents in the EU-27



Source: Eurostat (2021)

As concerns cross-border commuting, it is assumed that cross-border commuting will likely to go back to increasing pre-crisis levels in the long run since important parts of cross-border commuters work in the construction field.[292] Thus, one expected result related to the social developments is that businesses will increasingly struggle to cope with the increasing numbers of foreign visitors. For instance, businesses in Venice could reasonably increasingly struggle with waste management during tourist season[293] and with citizens increasingly overrunning cities like Dubrovnik with Games of Thrones tourism.[294]

How do LEAs use the latest technological developments and how are they affected by the latest social developments?

As stated in the previous section, it is assumed that mass sports events will take place without COVID-restrictions in the EU in the long term and hence require substantial preparation of joint operations and law enforcement cooperation of LEAs[295] in order to prevent e.g. football hooliganism and terrorism. In recent years, the nature of terrorist attacks at mass gatherings has shifted to attacks being carried out by single individuals with little preparation and easily available weaponry such as in the case of the attacks at the football match at the Stade de France in 2015.[296] It is expected that this threat increases, particularly as the latest technologies can be misused, e.g. in the case of malicious use of drones.[297] In difference to citizens and businesses, a result of this for LEAs is that LEAs have to cooperate across the entire EU to prepare for threats from single actor attacks as well as more sophisticated attacks. Similarly to the argument made in the section for SOC, it is expected that the social developments relating to e.g. the increasingly global value chains will with some certainty require LEAs to increasingly cooperate across-borders.

A similar argument applies to mass cultural events and political mass gatherings. In difference to the way citizens and businesses are affected, LEAs face operational technological challenges for cross-border cooperation which stem from limited interoperability of the databases and IT systems

[292] Eurostat (2021) People on the move. Available at link.
[293] The Guardian (2019) Sinking city: how Venice is managing Europe's worst tourism crisis. Available at link.
[294] Vox (2019) Game of Thrones tourism is wildly popular – and not just because the show is a hit. Available at link.
[295] Technical workshop held on 24 March.
[296] BBC News (2015) Paris attacks: What happened on the night. Available at link.
[297] EU Commission (2020) A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond. Available at link.

in place.[298] As is the case for mass sports events, LEAs are expected to increasingly cooperate to ensure public order and safety during mass cultural events and political mass gatherings and to prepare for terrorist attacks. In the long term, it is expected that the usage of technological developments by LEAs such as AI will reduce the severity of disruption of public order and safety.

As regards cross-border tourism and cross-border commuting, as long as the crisis prevails, the prevalence of tourism and cross-border commuting are expected to remain at lower levels in comparison to the pre-crisis increases in tourism and commuting. In difference to citizens and businesses, LEAs have to ensure that public order is not disrupted by e.g. terrorism in the public sphere and are expected to increasingly rely on the use of technological developments such as shared databases or cross-border radio-telecommunication solutions to ensure that public order and safety – and in the short run especially health safety – is guaranteed. In the long run, where it is expected that cross-border tourism and cross-border commuting to increase, LEAs will likely use technological developments such as AI (a) to reduce the severity of disruption of public order and safety and (b) to enhance cross-border cooperation.

****

[298] Technical workshop held on 24 March 2021.

ANNEX 5: SUPPORTING INFORMATION ON THE PROBLEMS 1, 2 & 3

1. HORIZONTAL SUPPORTING INFORMATION REGARDING THE PROBLEMS 1, 2 & 3

Overview

The EU framework for facilitating cross-border law enforcement cooperation is spread across a range of legislative texts and non-binding policy initiatives. The documentary review identified 22 relevant EU measures that cover to different extent the three main areas of analysis of the study. More specifically, 15 legislative measures (i.e. Regulations, Directives and Council Decisions) and 7 non-binding measures (i.e. manuals, handbooks, guidelines and factsheets) have been identified.

The EU legal framework for facilitating cross-border law enforcement cooperation between EU Member States and the Schengen area precedes the TFEU and includes **foundational legal agreements,** such as:

- The **Schengen *acquis* – the 1990 CISA**,[299] which sets out the terms to establish common standards for controls of the EU's external borders and removed border checks between the signature countries.[300]
- The **1998 Naples II Convention** on mutual assistance and cooperation between customs administrations,[301] which includes some provisions on criminal law enforcement cooperation. The Convention enables central coordinating units appointed within each national customs administration to exchange requests (in principle in writing) for information, surveillance, and enquiries.[302] Moreover, the Convention establishes that customs administrations must provide each other with the necessary staff and organisational support when cooperating on cross-border issues.[303]
- Part of the **Prüm Decisions** related to operational cooperation.[304] The Prüm Treaty was fully introduced at Union level by **Council Decision 2008/615/JHA** on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and by **Council Decision 2008/616/JHA** on the implementation of Decision 2008/615/JHA.
- **Council Framework Decision 2006/960/JHA** of 18 December 2006 (or so-called **Swedish Framework Decision** (**SFD**))[305] on simplifying the exchange of information

[299] The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (1990). Available at: link.

[300] EU countries applying the Schengen acquis include Belgium, France, Germany, Luxembourg, the Netherlands, Portugal, Spain, Austria, Italy, Greece, Denmark, Finland, Czechia, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia. Non-EU Member States applying the Schengen rules include Iceland, Norway, Switzerland and Liechtenstein.

[301] Close cooperation between EU customs administrations (Naples II Convention) (1998). Available at: link.

[302] Mutual assistance can be provided also spontaneously, without prior request, for covert surveillance and the provision of information. *Ibidem.*

[303] Special forms of cooperation listed in the Convention are: Mutual assistance Hot pursuit — cross-border pursuit of suspects; Cross-border surveillance; Covert investigations; Joint special investigation teams; Controlled deliveries. *Ibidem*.

[304] Only the Articles 16-23 of Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Article 17 of Council Decision 2008/616/JHA are covered (another legal initiative is to cover the remaining parts of Prüm). Council Decision 2008/615/JHA. Available at: link. Council Decision 2008/616/JHA. Available at: link.

[305] 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 (2006). Available at: link.

and intelligence between LEAs of the Member States of the European Union. Adopted in the wake of the 2004 Madrid attacks, it institutes a new legal system improving information exchange, for example, by establishing a time-frame for responding to requests. According to the SFD, the exchange of information between LEAs of different Member States should not be subject to stricter conditions than those that apply between LEAs within a State.

- **Council Decision 2007/412/JHA** of 12 June 2007 amending Decision 2002/348/JHA concerning security in connection with football matches with an international dimension. The Decision aims to prevent and combat football-related violence in order to ensure the safety of EU citizens, by outlining methods for internationally coordinated policing of football events.
- **Council Decision 2006/560/JHA** of 24 July 2006 amending Decision 2003/170/JHA on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States, which amends the provision of Decision 2003/170/JHA establishing a common framework for liaison officers seconded from the Member States with the aim of improving cooperation in preventing and combating all forms of international crime.[306]

While these conventions and decisions contribute to consolidating the EU legal framework in the area of Freedom, Security and Justice, **they do not apply to all EU Member States and SACs and leave considerable flexibility to the Member States in implementing them at the national level**. For example, some EU Member States, including Bulgaria, Croatia, Cyprus and Romania, have not fully integrated the Schengen area, and Ireland has opted out of the Schengen Agreement.

Additional EU legislation has been introduced since the TFEU to further harmonise EU LEAs' approach and cooperation to tackle cross-border crimes and ensure the safety and security of EU citizens. These legislative tools include, among others, **Regulations on the creation of EU decentralised agencies in the area of Freedom, Security and Justice** such as Europol, Frontex, Eurojust and eu-LISA. These agencies play a crucial role in facilitating information sharing and supporting operational cooperation between Member States and SACs. More specifically, they contribute to the assessment of common security threats, help define common priorities for operational action, and promote and facilitate cross-border cooperation and prosecution. However, Member States' and SACs' engagement and contribution to the work of these agencies varies and the EU decentralised agencies have limited decision-making power and competences on operational matters.

Besides the establishment of a legislative framework facilitating cross-border law enforcement cooperation within the EU and the Schengen Area, **the EU has also fostered greater cooperation between law enforcement bodies through the publication of recommendations and guidelines, as well as a series of strategic and operational initiatives**.

Recommendations and guidelines developed at the EU level are non-binding documents, which seek to record good practices for law enforcement cooperation within the EU and Schengen area and provide additional clarification. These non-binding measures provide, among the others, on instructions to implement the SFD and Naples II Convention, recommendations for the correct application of the Schengen Acquis, on Single Point of Contacts (SPOCs) and Police Customs Cooperation Centres (PCCCs) and measures to prevent and control violence and disturbances in connection with football matches with an international dimension. While these recommendations and guidelines lay out the grounds for adopting common approaches to tackling cross-border crimes, they are not legally binding for EU Member States or SACs. As such, they do not

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

participate in harmonising the legal framework for cross-border cooperation in the strict sense, but may still serve to align the approaches of the Member States and SACs based on an increased common understanding of and approach to the implementation and application of existing provisions.

The following sections provide a descriptive overview of the nature and content of the EU measures related to the three dimensions of analysis of the study, i.e. access to/exchange of information, operational cooperation for public order and safety, and operational cooperation to combat SOC and terrorism. Moreover, specific EU measures have been identified in relation to data protection during cross-border law enforcement operations. These are also described. Finally, the last section focuses on EU measures establishing EU decentralised agencies relevant to intra-EU law enforcement cooperation.

The table below provides an overview of all identified relevant EU measures along with the relevant dimension(s) of analysis covered by each measure. It shall be noted that some EU measures include provisions that are relevant for more than one dimension of analysis. Given the horizontal nature of exchange of information, most of the measures analysed under this dimension also include provisions that are relevant to SOC and public order.

EU measures by dimension of analysis

Measures
Binding measures
CISA 1990
Convention on mutual assistance and cooperation between customs administrations (Naples II Convention) - OJ C 24 1998
Council Decision 2002/348/JHA concerning security in connection with football matches with an international dimension
Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences
Council Decision 2006/560/JHA of 24 July 2006 amending Decision 2003/170/JHA on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States
Council Decision 2007/412/JHA concerning security in connection with football matches with an international dimension
Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime
Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime
Council Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences
Council Decision 2009/917/JHA on the use of information technology for customs purposes
Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence (SFD)
Regulation (EU) 2018/1860 on the use of the SIS for the return of illegally staying third-country nationals
Regulation (EU) 2018/1861 on the establishment, operation and use of the SIS in the field of border check
Regulation (EU) 2018/1862 on the establishment, operation and use of the SIS in the field of police cooperation
Regulation (EU) 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration

Measures
Non-binding measures
Council Document 10000/07 - Proposal for a Council Recommendation on a standard procedure in Member States for cross-border enquiries by police authorities in investigating supply channels for seized or recovered crime-related firearms
Council Document 9512/10 - Guidelines on the implementation of Council Framework Decision 2006/960/JHA
Council Document 9105/11 - PCCCs guidelines
Council Document 6721/3/14 - Draft SPOC Guidelines for international law enforcement information exchange
Council Document 10492/14 - Guidelines for a SPOC
Council Document 13034/14 - Guidelines on the implementation of SFD
Council Document 5825/20, 2 December 2020 (Manual on Law Enforcement Information Exchange)
Council Resolution concerning an updated handbook with recommendations for international police cooperation and measures to prevent and control violence and disturbances in connection with football matches with an international dimension (2006/C 322/01- Football Handbook)
Data Protection (binding)
Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector
Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data
Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
Regulation (EU) 2018/1725 on the processing of personal data by the Union institutions, bodies, offices and agencies
EU Agencies' legal basis (binding)
Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on CEPOL
Regulation (EC) No 1920/2006 on EMCDDA
Regulation (EU) 2016/794 on Europol
Regulation (EU) 2018/1726 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)
Regulation (EU) 2018/1727 on Eurojust
Regulation (EU) 2019/1896 on EBCGA

Source: EY/RAND Europe Study's elaboration based on desk research

Access to/exchange of information. Most efforts to harmonise national legislation focus on improving information sharing between LEAs across the EU and the Schengen area. There are several binding measures that establish provisions on the access to and exchange of information between Member States and SACs. Together, these legislative instruments were introduced as an attempt to reconcile Member States' and SACs' fragmented law enforcement approaches with the growing need to jointly tackle shared cross-border threats. As such, legislative efforts have sought to ensure that information available to LEAs in one Member State is also available to other Member States or SACs. These legal texts have thus introduced cooperation instruments to centralise intelligence used for law enforcement and facilitate the exchange of information.

To this end, a **"one stop shop" (OSS) strategy** has been promoted at the EU level to increase cross-border information exchange, simplify and centralise information sharing and access to

information.[307] Pursuant the OSS strategy, Member States' and SACs' Lead Supervisory Authorities[308] may request/provide mutual assistance and conduct joint operations for carrying out investigations or for monitoring the implementation of a measure concerning a data controller or processor established in another Member State. In doing so, "Member States shall ensure that conditions not stricter than those applicable at the national level for providing and requesting information and intelligence are applied for providing information and intelligence to competent LEAs of other Member States".[309]

EU legislative measures mainly focus on the types of information to be exchanged and the actors in charge of such an exchange. With regard to the types of information, different EU measures cover specific types of information, such as personal data, travel documents, information concerning and resulting from criminal investigations, terrorism offences, VISA data, road traffic data, firearm data, immigration data. These legislative instruments are accompanied by non-binding measures aimed at providing recommendations related to their implementation. For example, Council Document 10000/07[310] provides a Manual that shall be applied to a systematic tracking of firearms aiming at combating illicit manufacturing and illicit trafficking and using means and methods commonly agreed on and established by the EU Member States.

Also with regard to the actors in charge of exchanging information, different measures focus on different types of actors responsible for exchanging specific types of information. For instance, the SIS framework – built on Regulation (EU) 2018/1860, Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862 –on the establishment, operation and use of the SIS[311] focuses on the exchange of supplementary information, such as information connected to alerts in SIS, via a dedicated channel (SIRENE mail relay) and the SIRENE Bureaux. Regulation (EU) 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration[312] establishes a framework for interoperability across different systems,[313] allowing for better detection of security threats and identity fraud, and helps preventing and combating illegal immigration through the establishment of:

- A European search portal (ESP), allowing competent authorities to search multiple information systems simultaneously, using both biographical and biometric data;

[307] Council Document 6721/3/14 - Draft SPOC Guidelines for international law enforcement information exchange Available at: link.

[308] Pursuant Regulation (EU) 2016/679, "In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation".

[309] 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, Art. 3 (3). Available at: link.

[310] Council Document 10000/07 - Proposal for a Council Recommendation on a standard procedure in Member States for cross-border enquiries by police authorities in investigating supply channels for seized or recovered crime-related firearms. Available at: link.

[311] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU. Available at: link.

[312] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816. Available at: link.

[313] The Entry/Exit System (EES); The Visa Information System (VIS); The European Travel Information and Authorisation System (ETIAS); Eurodac; The Schengen Information System (SIS); The European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN); Europol data; Interpol database.

- A shared biometric matching service enabling the searching and comparing of biometric data (fingerprints and facial images) from several EU information systems;
- A common identity repository containing biographical and biometric data of non-EU nationals available in several EU information systems;
- A multiple identity detector enabling the detection of multiple identities across different EU information systems.

In order to cope with the increasing exchange of cross-border information, the Council Document 10492/14 established the **SPOCs** across countries,[314] in order to maximise the use of available resources, avoid overlaps and make cooperation with other Member States and SACs more efficient, fast and transparent. Besides the SPOCs, other key actors in the intra-EU law enforcement landscape are the **PCCCs** set up by Council Document 9105/11[315], which are operational centres responsible for handling crisis situations and events having an international dimension. Moreover, the **National Firearms Focal Points (NFFP)** were set up by COM (2015) 624 final[316] with the aim to develop expertise and improve analysis and strategic reporting on illicit trafficking in firearms notably through the combined use of both ballistic and criminal intelligence.

In relation to exchange of information and cooperation concerning terrorist offences, Council Decision 2005/671/JHA[317] states that Member Statas shall appoint **national competent authorities in charge** of sharing relevant information with other Member States and SACs as well as with Eurojust and Europol.

Moreover, pursuant to Council Decision 2003/170/JHA[318], **liaison officers posted abroad** were established for maintaining contacts with the authorities in the countries or organisations where they are based with a view to contributing to preventing or investigating criminal offences" (Article 1). Pursuant Article 8, as amended by Council Decision 2006/560/JHA,[319] Member States can request to use Europol liaison officers seconded to third countries or international organisations for exchanging information about serious threats of criminal offences and vice versa.

Some EU legislative measures introduced specific tools and information systems that can be used to exchange information between LEAs. Besides measures relating to horizontal platforms (e.g. SIS), there are also measures that cover tools for the exchange of specific types of information, such as drugs information (Reitox), identity documents (ESP),[320] and customs information.

It is worth mentioning that most EU measures relating to information systems refer to generic "electronic means of communication", thus leaving room to the Member States to choose the most appropriate tool to exchange information.

[314] Council Document 10492/14, Draft Guidelines for a Single Point of Contact (SPOC) for international law enforcement information exchange. Available at: link.
[315] Council Document 9105/11, European Best Practice Guidelines for Police and Customs Cooperation Centres (PCCCs). Available at: link.
[316] COM (2015) 624 final. Available at: link.
[317] Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences. Available at: link.
[318] Council Decision 2003/170/JHA of 27 February 2003 on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States. Available at: link.
[319] Council Decision 2006/560/JHA of 24 July 2006 amending Decision 2003/170/JHA on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States. Available at: link.
[320] The European search portal (ESP) allows competent authorities to search multiple information systems simultaneously, using both biographical and biometric data and it can be therefore used to search data related to persons or their travel documents.

Furthermore, Council Decision 2009/917/JHA on the use of information technology for customs purposes[321] established a joint automated information system named "Customs Information Systems" (CIS) with the aim to "assist in preventing, investigating and prosecuting serious contraventions of national laws by making information available more rapidly, thereby increasing the effectiveness of the cooperation and control procedures of the customs administrations of the Member States." (Article 1.2).

The information and data available in this system can be also personal data with the specification that they must be inserted in the system with some limitation (listed in the article 4.2). This information is accessible to Europol and Eurojust. It should be noted that "Only the supplying Member State shall have the right to amend, supplement, rectify or erase data which it has entered in the" CIS (article 13).

The CIS is a part of the Anti-Fraud Information System (AFIS) operated by the European Anti-Fraud Office (OLAF), which hosts a set of anti-fraud applications under a common technical infrastructure aiming at the timely and secure exchange of fraud-related information between the customs competent national and EU administrations.

The AFIS includes also the Customs Investigation Files Identification Database (FIDE), which stores data on persons and businesses who are or have been the subject of an administrative enquiry or a criminal investigation by a Member State customs authority. Council Decision 2009/917/JHA and Regulation 515/97[322] provide the legal basis for CIS and FIDE and define their policy of access. CIS and FIDE information stored under the Council 2009/917/JHA is accessible to all Member States customs authorities, Europol and Eurojust. CIS and FIDE information stored according to Regulation 515/97 is accessible to all Member States customs authorities and competent Commission departments.

The legislative measures that have introduced tools for the exchange of information are accompanied by non-binding measures that provide instructions and operational details on specific EU provisions and include guidance for collecting and sharing data and information. For example, Council Document No 5825/20[323] is a Manual on Law Enforcement Information Exchange, which provides details for exchanging information via different channels such as Interpol/Europol/SIRENE. Council Document No 9512/10[324] provides Guidelines on the implementation of the SFD, including practical information about proper channels of communication to be used.

The following table provides an overview of EU tools/databases and systems for the exchange of information, including:

- Secure Information Exchange Network Application (SIENA);
- SIS II;
- VIS;
- Europol Information System (EIS);
- Tools/information systems that are mainly used by a specific category of actors (CIS, EUROSUR, Prüm, National Football Info Points (NFIP), NFFPs networks);
- Prüm automated data exchange systems;
- Bilateral contacts.

[321] Council Decision 2009/917/JHA on the use of information technology for customs purposes. Available at: link.
[322] Regulation 515/97 is out of the scope of this study. Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters. Available at: link.
[323] Council Document 5825/20, 2 December 2020, Manual on Law Enforcement Information Exchange. Available at: link.
[324] Council Document 9512/10, 26 May 2010 - Guidelines on the implementation of Council Framework Decision 2006/960/JHA. Available at: link.

Overview of EU tools and information systems for the exchange of information

Tool/ information system	Legal basis	Actors entitled to use the tool	Type of information exchanged
SIENA	• Council Framework Decision 2006/960/JHA	• National competent law enforcement authority[325] • Europol or Eurojust	Provision of information and intelligence
	• Regulation (EU) 2016/794	• ENUs	Information preventing and combating organised crime, serious international crime and terrorism involving two or more Member States
	• CISA - Art. 39	• NCPs • SPOC	Cross-border and intra-European operational actions/ operations, public order/ security/preventing criminal offences/ mass gatherings/ disasters, serious accidents
	• Council Document 10492/14	• SPOC • Liaison officers • Bilateral channels based on cooperation agreements at national, regional and local level (PCCCs)	Information on criminal matters
SIS II	•	• National competent law enforcement authority • Europol or Eurojust	
	• Council Decision 2007/533/JHA, • Regulation (EU) 2018/1860 • Regulation (EU) 2018/1861 • Regulation (EU) 2018/1862	• National authorities responsible for border control[326] • Europol • Eurojust • Frontex	Conditions and procedures for entering and processing alerts in the SIS on persons and objects, and for exchanging supplementary information and data in police and judicial cooperation on criminal matters
	• Regulation (EU) 2016/794	• ENUs	Information preventing and combating organised crime, serious international crime and terrorism involving two or more Member States
	• COM (2015) 624 final	• NFFP • Europol	Information in the area of firearms trafficking
VIS	• Council Decision 2008/633/JHA	• LEAs • Europol	• Data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area
EIS	• Regulation (EU) 2016/794	• ENUs	• Information preventing and combating organised crime, serious international crime and terrorism involving two or

[325] To be understood as a national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities. The designation of national competent authority falls within each Member State's competence.

[326] Including: supplementary information requests at the national entry bureau (SIRENE Bureau); customs, judicial, migration and visa issuing authorities under Regulation 1987/2006; vehicle registration authorities; and under the new Regulation 2018/1862, firearm, boat, aircraft registration authorities, security authorities.

Tool/ information system	Legal basis	Actors entitled to use the tool	Type of information exchanged
			more Member States
	• COM (2015) 624 final	• NFFP • Europol	• Information in the area of firearms trafficking
CIS	• Council Decision 2009/917/JHA • Regulation 515/97	• National competent customs administration • Competent Commission departments • Europol • Eurojust	• Data on commodities, means of transport, businesses, persons, fraud trends, availability of expertise, items detained, seized or confiscated, cash detained, seized or confiscated
FIDE[327]	• Council Decision 2009/917/JHA • Regulation 515/97	• National competent customs administration • Competent Commission departments • Europol • Eurojust	• Data on persons or businesses subject to an administrative enquiry or a criminal investigation by a Member State customs authority.
EUROSUR	• Regulation (EU) 2019/1896	• National authorities responsible for border management (NCPs)	• Data on detecting, preventing and combating illegal immigration and cross-border crime
Prüm network for the supply of non-personal and personal data	• Council Decision 2008/615/JHA	• NCPs	• Supply of data in relation to major events; • Supply of information in order to prevent terrorist offences
NFIP	• Council Decision 2007/412/JHA • Council Resolution 2006/C 322/01	• NFIP • National competent authorities	• Information on high-risk supporters; • Strategic, operational and tactical information
NFFP	• COM (2015) 624 final	• NFFP • Europol	• Information in the area of firearms trafficking
Bilateral and regional liaison officers in PCCC	• CISA - Art. 39	• NCPs • SPOC	• Cross-border and intra-European operational actions/ operations, public order/ security/preventing criminal offences/ mass gatherings/ disasters, serious accidents
Bilateral contact points	• Council Framework Decision 2006/960/JHA	• National competent law enforcement authority • Europol or Eurojust	• Provision of information and intelligence
Liaison officers in liaison bureaux	• CISA - Art. 47 • Council Decision 2006/560/JHA	• Liaison Officers	• Information on criminal matters

Source: EY/RAND Europe Study's elaboration based on desk research

SIENA, SIS II, VIS and EIS are the tools/information systems that can be used by a wide array of actors ranging from Member States' competent authorities, European Agencies (Europol, Eurojust, Frontex), and national bodies (e.g. SPOCs, PCCCs and NFFPs).

Actors that more frequently are entitled to use the tools listed in the table below are:

[327] FIDE is out of the scope of this study.

- Europol (5 tools/information systems, namely SIENA, SIS II, VIS, EIS, and liaison officers in liaison bureaux);
- Member States' competent law enforcement authority (4 tools/information systems, namely SIENA, SIS II, VIS, and liaison officers in liaison bureaux);
- Eurojust (4 tools/information systems, namely SIENA, SIS II, CIS and bilateral contact points);
- Europol National Unit (ENUs) (3 tools/information systems, namely SIENA, SIS II and EIS).

Thus, **different tools can be used by the same actor**, although each tool is intended to be used for different objectives/type of information, hence there is no overlap or inconsistency.

Namely:

- Three different tools can be used by ENUs to prevent and combat organised crime, serious international crime and terrorism involving two or more Member States: SIENA, SIS II and EIS;
- Two different tools can be used by NFFPs to share information in the area of firearms trafficking: SIS II and EIS

Moreover, different actors can use the same tool (SIENA) to share the same type of information: both NCPs and SPOCs can share information related to cross-border and intra-European operational actions/ operations.

Some EU measures make a step further and provide indications in relation to the timing for the exchange of information and the language to be used. As for the timing, the SFD states that requests for information shall be answered within eight hours (urgent request), one week (non-urgent request) or 14 days (all other cases). Guidelines on the implementation of the SFD[328] provide details for the identification of "urgent cases", however, no definition of "not urgent" and "other cases" is provided.

A generic timeframe is also provided by Council Decision 2008/633, which requires to exchange information "immediately and, in any case, no later than 60 days".[329] Concerning the language to be used, two relevant measures have been identified. Council Decision 2002/348 concerning security in connection with football matches with an international dimension states that "National football information points shall communicate in their own language, with a translation in a working language common to both sides, save as otherwise arranged between the parties concerned"[330] and the Naples II Convention requires that "Requests shall be submitted in an official language of the Member State of the requested authority or in a language acceptable to such authority".[331] These measures are aimed to ensure that information is exchanged in a way that can be understood by the receiving Member State.

[328] Council Document 13034/14 - Guidelines on the implementation of SFD. Available at: link.
[329] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences. Available at: link
[330] Council Decision 2002/348/JHA: Council Decision of 25 April 2002 concerning security in connection with football matches with an international dimension. Available at: link.
[331] Close cooperation between EU customs administrations (Naples II Convention) (1998). Available at: link.

Overview of the extent to which the issues identified in the Impact Assessment are also reported in the Schengen Evaluation Reports (2015-2019)

The Schengen *acquis* includes a wide-ranging and fast-developing set of rules as well as compensatory measures to counterbalance the absence of internal border controls. The Schengen Evaluation and Monitoring Mechanism monitors the implementation of the Schengen acquis by the countries that apply the Schengen acquis in part or in full. It also assesses the capacity of those countries where internal border controls have not yet been lifted to implement the Schengen acquis in full.

The Schengen Evaluation and Monitoring Mechanism assesses in particular, the implementation of measures in the areas of external borders, return, visa policy, **police cooperation,** the Schengen Information System (SIS), data protection, and the absence of border control at internal borders.

The Commission carries out evaluations over a five-year cycle following multiannual and annual programmes, together with experts from Member States as well as EU agencies that participate as observers.

Each country is evaluated at least once every five years. Additional ad-hoc evaluations in the form of unannounced evaluations or revisits can be organised, as required. Thematic evaluations are an additional tool for assessing the implementation of specific parts of the Schengen acquis across several countries at the same time. The figure below illustrates the five-year evaluations process.

Evaluation reports are presented to the Schengen Committee (in which all Member States are represented) and, subject to its positive opinion, adopted by the Commission. Upon a Commission proposal, the Council adopts the recommendations to address any deficiencies identified in the evaluation reports, concluding the first phase of the evaluation. As a follow-up, the country concerned must submit an action plan listing the remedial actions to implement the Council recommendations. The Commission assesses the action plans in cooperation with the relevant evaluation experts. The evaluated country has an obligation to report on the progress made every three months. When all remedial actions have been taken, the Commission closes the evaluation concluding the second phase.

Core problem	Drivers	AT	BE	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IT	LT	LU	LV	MT	NL	PL	PT	SE	SI	SK	CH	IS	LI	Total	Share of countries
Law enforcement authorities do not effectively and efficiently exchange information with their partners in other Member States	**Difficulties in the implementation of relevant EU provisions**																												
	Some requirements set in the SFD are unclear and (unnecessarily) complex		■	■	■	■	■	■					■	■	■	■		■		■	■	■	■	■	■	■	■	**19**	**73%**
	Uncertainties in the use of the proper legal basis			■			■						■		■					■			■	■				**7**	**27%**
	Insufficient knowledge of existing mechanisms, skill gaps and outdated IT infrastructures																												
	National LEAs have limited awareness and knowledge of relevant databases			■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	**24**	**92%**
	Limited offer of training that is focused on cross-border law enforcement cooperation	■		■		■	■		■	■	■		■	■	■	■		■	■	■	■	■	■	■	■		■	**20**	**77%**
	Language barriers hamper the cross-border exchange of information	■		■				■	■	■		■	■	■	■					■				■		■		**12**	**46%**
	Use of rudimentary search tools hampers the adoption of transliteration and "fuzzy logic" search			■			■		■	■	■		■		■		■			■		■	■	■			■	**13**	**50%**
	Differences in national implementation choices																												
	SPOCs do not always play their coordination role and lack resources to face the increasing number of requests							■	■							■			■		■			■	■			**7**	**27%**
	Differences in access rights and use EU of and international databases and platforms between national law enforcement authorities	■		■		■	■	■	■		■	■	■	■	■	■	■	■		■	■	■	■	■		■	■	**21**	**81%**
	Total	**3**	**1**	**7**	**2**	**4**	**6**	**5**	**6**	**4**	**4**	**3**	**5**	**4**	**6**	**3**	**1**	**4**	**3**	**7**	**5**	**5**	**6**	**8**	**4**	**4**	**5**	**115**	

Source: Elaboration by the Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation

2. VERTICAL SUPPORTING INFORMATION REGARDING THE PROBLEM 1

Overview of binding EU measures with respect to the access to and exchange of information (Part 1)

	Council Decision 2006/560 on the common use of liaison officers posted abroad	Council Decision 2008/633 (VIS for terrorist offences and of other serious criminal offences)	Council Framework Decision 2006/960 (SFD)	Regulation 2018/1860 Regulation 2018/1861 Regulation 2018/1862	Regulation 2019/818 (Interoperability between EU information systems)
Objective	To ensure that Europol's liaison officers seconded to third countries and international organisations provide it with information relating to serious threats of criminal offences to Member States for those criminal offences for which Europol is competent under the Europol Convention	To provide access to Member States' designated authorities and the European Police Office (Europol) for consultation of the Visa Information System (VIS) for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences	To establish the rules under which Member States' law enforcement authorities may exchange information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations	• Regulation 2018/1860: to strengthen enforcement of the EU's return policy and reduces incentives for illegal immigration into the EU. • Regulation 2018/1861: to define the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement. • Regulation 2018/1862: to define the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters	To establish a European search portal (ESP) for the purposes of facilitating the fast, seamless, efficient, systematic and controlled access of Member State authorities and Union agencies to the EU information systems
Type of information to be exchanged	Serious threats of criminal offences	VIS data (personal data, travel data)	Information and intelligence referred to any type of information or data held by Law Enforcement Authorities (LEAs) or held by public authorities/private entities and which is available to LEAs without the use of coercive measures.	Personal data and supplementary information	Personal data and travel documents
Tools/ information systems used to exchange information		Substantiated request in written or electronic form	• Annex A includes a form to be used by the requested Member State in case of transmission/delay/ refusal of information • Annex B: request form for information and	SIS	ESP

	Council Decision 2006/560 on the common use of liaison officers posted abroad	Council Decision 2008/633 (VIS for terrorist offences and of other serious criminal offences)	Council Framework Decision 2006/960 (SFD)	Regulation 2018/1860 Regulation 2018/1861 Regulation 2018/1862	Regulation 2019/818 (Interoperability between EU information systems)
			intelligence to be used by the requesting member state		
Specific actors involved in the exchange of information	Europol liaison officers	Designated authorities of Member States	Competent law enforcement authority; Competent Prosecutor/Judicial authority	Sirene Bureau	Member State authorities and EU agencies having access to, at least, one of the EU information systems. Queries to the Common Identity Repository (CIR) shall be carried out by a police authority
Timing for exchanging information		Immediately and, in any case, no later than 60 days	Urgent request of information or intelligence held in a database directly accessible by a law enforcement authority: 8 hours (able to be postponed to maximum 3 days); Non urgent request of information or intelligence referred to the crimes above, held in a database directly accessible by a law enforcement authority: 1 week; Other cases: within 14 days		
Language to be used for the exchange of information			Language applicable for the channel used		
Requirements for exchanging information relating to specific areas		Two requirements are necessary: Access for consultation must be necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences; There are reasonable grounds to consider that consultation of VIS data will contribute to the prevention, detection or			

	Council Decision 2006/560 on the common use of liaison officers posted abroad	Council Decision 2008/633 (VIS for terrorist offences and of other serious criminal offences)	Council Framework Decision 2006/960 (SFD)	Regulation 2018/1860 Regulation 2018/1861 Regulation 2018/1862	Regulation 2019/818 (Interoperability between EU information systems)
		investigation of a criminal offence			
Mechanisms to ensure Data Protection when accessing/exchanging information		Each Member State shall adopt the necessary security measures with respect to data to be retrieved from the VIS pursuant to this Decision and to be subsequently stored	Usage of channels for international law enforcement cooperation without any further specification	Member States shall ensure that the independent supervisory authorities designated in each Member State monitor the lawfulness of the processing of personal data in SIS on their territory, its transmission from their territory and the exchange and further processing of supplementary information on their territory	Biometrical templates shall be stored in the shared BMS only for as long as the corresponding biometric data are stored in the CIR or SIS. Common identity data shall be deleted from the CIR in an automated manner in accordance with the data retention provisions of Regulation (EU) 2019/816
Requirement to develop cross-border threat assessment/risks analysis					

Source: Elaboration by the Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation

Overview of binding EU measures with respect to the access to and exchange of information (Part 2)

	Council Decision 2005/671 (exchange of information and cooperation concerning terrorist offences)	Council Decision 2008/615/JHA (Prüm Decision)	Council Decision 2002/348/JHA concerning security in connection with football matches with an international dimension	Council Decision 2007/412/JHA concerning security in connection with football matches with an international dimension	Council Decision 2009/917 (Information technology for customs purposes)	Naples II Convention
Objective	To share information with Europol, Eurojust and Member States	To improve cross-border cooperation and exchange of information between authorities responsible for the prevention and investigation of criminal offences	To prevent and combat football-related violence	The measure provides some amendments to the Decision 2002/348/JHA concerning security in connection with football matches with and international dimension	To establish Customs Information System; To establish customs files identification database	To provide information which may enable the requesting Member State to prevent, detect and prosecute infringements
Type of information to be exchanged	Personal data, relevant information concerning and resulting from criminal investigations	Personal data and information	Personal data	Strategic operational and tactical information	Personal data and all data useful to achieve the objective in the following categories:	

	Council Decision 2005/671 (exchange of information and cooperation concerning terrorist offences)	Council Decision 2008/615/JHA (Prüm Decision)	Council Decision 2002/348/JHA concerning security in connection with football matches with an international dimension	Council Decision 2007/412/JHA concerning security in connection with football matches with an international dimension	Council Decision 2009/917 (Information technology for customs purposes)	Naples II Convention
	conducted by LEAs with respect to terrorist offences which affect or may affect two or more Member States				Commodities; Means of transport; Businesses; Persons; Fraud trends; Availability of expertise; Items detained, seized or confiscated; Cash detained, seized or confiscated. No items of personal data shall be entered in any event within the category "fraud trends"	
Tools/ information systems used to exchange information				Information shall be exchanged using the appropriate forms contained in the appendix to the Football Handbook (2006/C 322/01)	Customs Information System (established for the purpose)	
Specific actors involved in the exchange of information		Specific National Contact Point (NCP)	National football information point (NFIP)	NFIP and competent authorities in Member States	Direct access to data entered into the Customs Information System shall be reserved to customs administrations, but may also include other authorities competent, according to the laws, regulations and procedures of the specific Member State	Customs authorities
Timing for exchanging information						
Language to be used for the exchange of information			National language. Translation in a working language common to both sides should be used	National language. Translation in a working language common to both sides should be used		Requests shall be submitted in an official language of the Member State of the requested

	Council Decision 2005/671 (exchange of information and cooperation concerning terrorist offences)	Council Decision 2008/615/JHA (Prüm Decision)	Council Decision 2002/348/JHA concerning security in connection with football matches with an international dimension	Council Decision 2007/412/JHA concerning security in connection with football matches with an international dimension	Council Decision 2009/917 (Information technology for customs purposes)	Naples II Convention
						authority or in a language acceptable to such authority
Requirements for exchanging information relating to specific areas			Public order purpose (preventing and combating football-related violence)		Personal data may be entered into the Customs Information System only if there are real indications, in particular on the basis of prior illegal activities, to suggest that the person concerned has committed, is in the act of committing or will commit serious contraventions of national laws	Request shall include: The applicant authority making the request; The measure requested; The object of, and the reason for, the request; the laws, rules and other legal provisions involved; Indications on the natural or legal persons being the target of the investigation; A summary of the relevant facts
Mechanisms to ensure Data Protection when accessing/exchanging information		The level protection of personal data at the national level should at least be equal to that resulting from the Council of Europe Convention for the Protection of Individuals and its Additional Protocol	Personal data shall be exchanged in accordance with the domestic and international rules applicable and using the appropriate forms contained in the appendix to the Football Handbook (2006/C 322/01)		Data entered into the Customs Information System shall be kept only for the time necessary to achieve the purpose for which they were entered. The need for their retention shall be reviewed at least annually by the supplying Member State	The customs authorities shall take into account in each specific case the requirements for the protection of personal data. They shall respect the relevant provisions of the Convention of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data
Requirement to develop cross-border threat assessment/risks analysis			NFIP should provide at the request of another NFIP a risk assessment of their own country's			

	Council Decision 2005/671 (exchange of information and cooperation concerning terrorist offences)	Council Decision 2008/615/JHA (Prüm Decision)	Council Decision 2002/348/JHA concerning security in connection with football matches with an international dimension	Council Decision 2007/412/JHA concerning security in connection with football matches with an international dimension	Council Decision 2009/917 (Information technology for customs purposes)	Naples II Convention
			clubs and national team			

Source: Elaboration by the Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation

Overview of non-binding EU measures with respect to the access to and exchange of information

	Council Document No 9512/10 (Guidelines on the implementation of SFD)	Council Document 10492/14 (Guidelines for SPOC)	Council Document 6721/3/14 (SPOC guidelines)	Council Document 13034/14 (Guidelines on the implementation of SFD)	Council Document No 5825/20 (Manual on Law Enforcement Information Exchange)	Council Document No 9105/11 (PCCCs guidelines)	Football Handbook (2006/C 322/01)
Objective	To enhance the effective and expeditious exchange of information and intelligence between law enforcement authorities	To provide guidelines for SPOC for which SPOC should access, directly or at request from competent authorities, to the broadest range of relevant national databases and in any case to all those databases available to the authorities represented in the SPOC	To provide guidelines for SPOC for which SPOC should access, directly or at request from competent authorities, to the broadest range of relevant national databases and in any case to all those databases available to the authorities represented in the SPOC			To provide guidelines for PCCCs for which PCCCs should act as a "facilitator" of information exchange between States.	To provide a Handbook helping NFIP coordinating the exchange of information on football matches. The NFIP should contribute to public order, peace and safety, thus aiming at an efficient use of the available resources. The NFIP should also aim to facilitate international police cooperation regarding the police approach to the football issues and to promote the exchange of information

	Council Document No 9512/10 (Guidelines on the implementation of SFD)	Council Document 10492/14 (Guidelines for SPOC)	Council Document 6721/3/14 (SPOC guidelines)	Council Document 13034/14 (Guidelines on the implementation of SFD)	Council Document No 5825/20 (Manual on Law Enforcement Information Exchange)	Council Document No 9105/11 (PCCCs guidelines)	Football Handbook (2006/C 322/01)
							between the police services of the different countries
Type of information to be exchanged	Any type of information or data which is held by law enforcement authorities, public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures	Any type of information contained in law enforcement databases, identity documents database, visa database, immigration office database, prisoners database, information exchange with the national liaison officers, border control database	Any type of information contained in law enforcement databases, identity documents database, visa database, immigration office database, prisoners database, information exchange with the national liaison officers, border control database			Information related to petty and moderately serious crime, illegal migration flows and public order problems	General and personal information
Tools/ information systems used to exchange information	Annex A :form to be used by the requested Member State in case of transmission/delay/refusal of information; Annex B: request form for information and intelligence to be used by the requesting Member State	SIS, CIS SIENA, Interpol (I-24/7 communication system), and sTESTA network	SIS, CIS and sTESTA network			Secure internal and external communications system, (e.g. systems similar to those employed by the national operational agencies - telephony, fax, e-mail, etc.). To increase efficiency and budgetary rationality, each PCCC party should be able to use a national	

	Council Document No 9512/10 (Guidelines on the implementation of SFD)	Council Document 10492/14 (Guidelines for SPOC)	Council Document 6721/3/14 (SPOC guidelines)	Council Document 13034/14 (Guidelines on the implementation of SFD)	Council Document No 5825/20 (Manual on Law Enforcement Information Exchange)	Council Document No 9105/11 (PCCCs guidelines)	Football Handbook (2006/C 322/01)
						line to communicate with its home country agencies and authorities. Dedicated software should be installed in order to facilitate the circulation of information within the PCCC in real time and to ensure daily recording and fast processing of questions referred to it and standardised recording of statistics	
Specific actors involved in the exchange of information	Police, customs and other authority authorised by national law to detect, prevent and investigate offences or criminal activities	SPOC Judicial authorities (when appropriate)	Europol, Interpol, SIRENE			PCCCs and Member States national agencies	Liaison officers, national football information point; for international tournaments, the formal request for support should come from the minister of the department responsible in the organising country, who will receive advice from the NFIP concerned
Timing for exchanging information		All databases are accessible to the unit on a 24/7					

	Council Document No 9512/10 (Guidelines on the implementation of SFD)	Council Document 10492/14 (Guidelines for SPOC)	Council Document 6721/3/14 (SPOC guidelines)	Council Document 13034/14 (Guidelines on the implementation of SFD)	Council Document No 5825/20 (Manual on Law Enforcement Information Exchange)	Council Document No 9105/11 (PCCCs guidelines)	Football Handbook (2006/C 322/01)
		basis, where necessary via on-call duty officers					
Language to be used for the exchange of information	Member State language						The national language can be used for the communication between the different NFIPs if a copy of it is provided in the working language common to the two parties (unless other arrangements have been made between the parties concerned)
Requirements for exchanging information relating to specific areas	Requests and answers exchanged shall always provide Europol in copy each time that the request falls under Europol's mandate		A request is sent through one channel only and if it is sent through different channels at the same time, this is clearly indicated. The channel is not be changed during an on-going operation or during any phase unless it is absolutely necessary and the partner's choice of channel when replying to the requests is respected. A change of				Public order purpose (preventing and combating football-related violence)

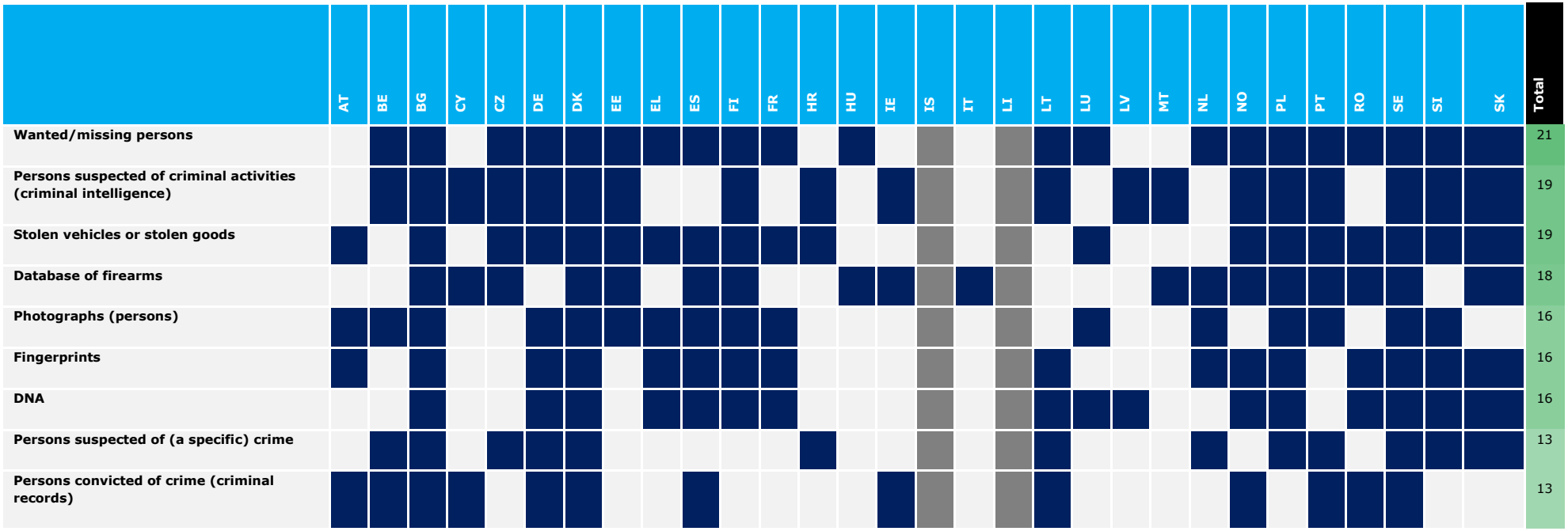
	Council Document No 9512/10 (Guidelines on the implementation of SFD)	Council Document 10492/14 (Guidelines for SPOC)	Council Document 6721/3/14 (SPOC guidelines)	Council Document 13034/14 (Guidelines on the implementation of SFD)	Council Document No 5825/20 (Manual on Law Enforcement Information Exchange)	Council Document No 9105/11 (PCCCs guidelines)	Football Handbook (2006/C 322/01)
			channel is communicated to all parties, including the reason for the change. The purposes of and restrictions on the processing of information defined by the provider of the information are respected. Whenever possible, the SPOC replies directly to the international request, where appropriate with copy to the concerned national authority. Where the SPOC cannot reply directly, it forwards the request to the appropriate competent national authority, even if the original request was wrongly addressed to another authority. When a request is refused, the grounds for				

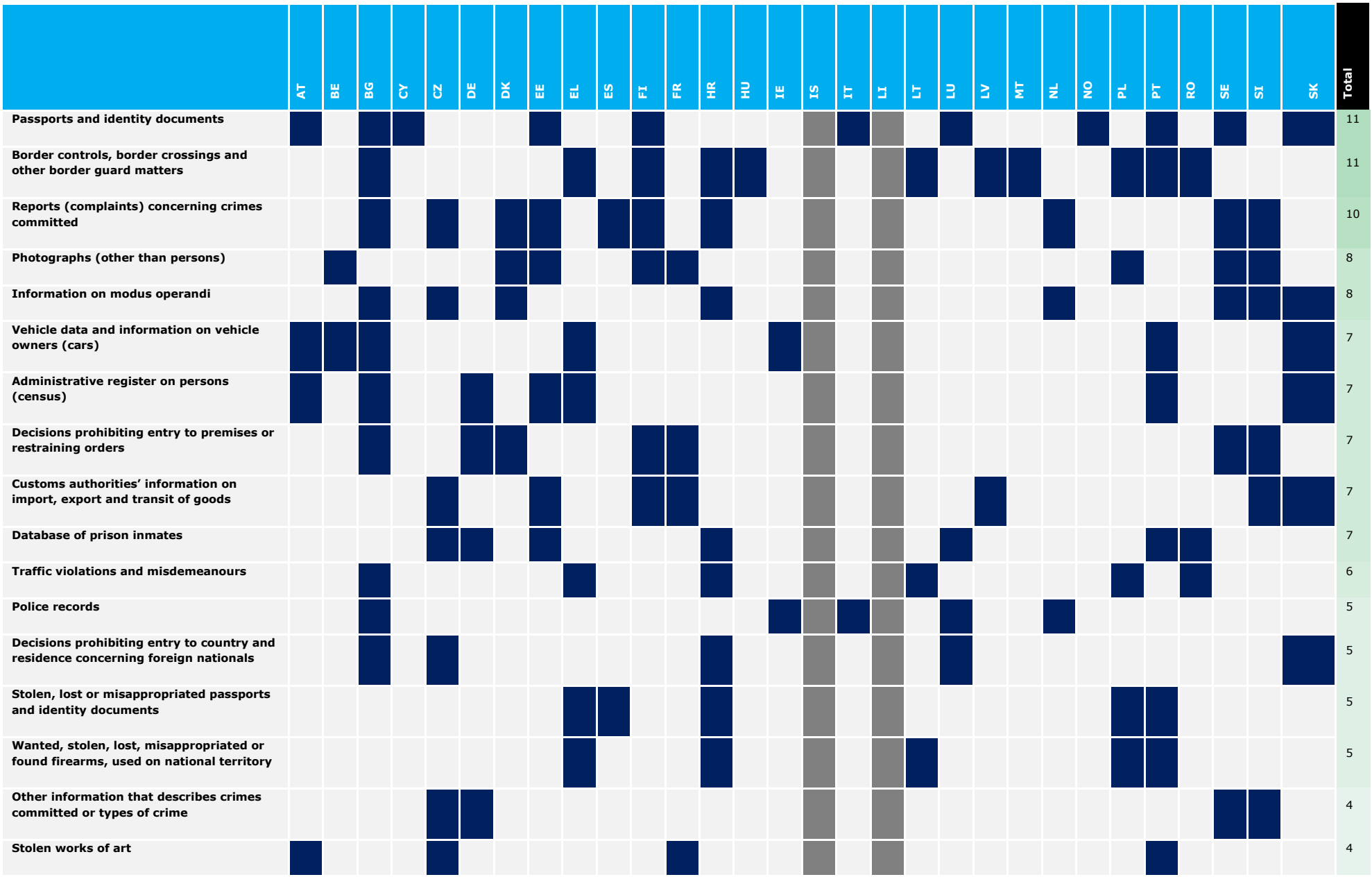
	Council Document No 9512/10 (Guidelines on the implementation of SFD)	Council Document 10492/14 (Guidelines for SPOC)	Council Document 6721/3/14 (SPOC guidelines)	Council Document 13034/14 (Guidelines on the implementation of SFD)	Council Document No 5825/20 (Manual on Law Enforcement Information Exchange)	Council Document No 9105/11 (PCCCs guidelines)	Football Handbook (2006/C 322/01)
			refusal have to be provided through the initial channel. When receiving a reply from the national authorities to an international request, the unit proactively verifies whether this information can be useful to another Member State, Europol or Eurojust and if this is the case, requests and encourages the owner of the information to transmit the information further				
Mechanisms to ensure Data Protection when accessing/exchanging information		The SPOC shall respect all applicable data protection rules	The SPOC shall respect all applicable data protection rules			The exchange of information must comply with current data protection and data dissemination provisions in the respect of the national legislation	In accordance with the applicable national and international legislation, the NFIP should be responsible for administering the personal data regarding risk supporters
Requirement to develop cross-border threat assessment/risks analysis							With regard to football matches with an international dimension, it is necessary that

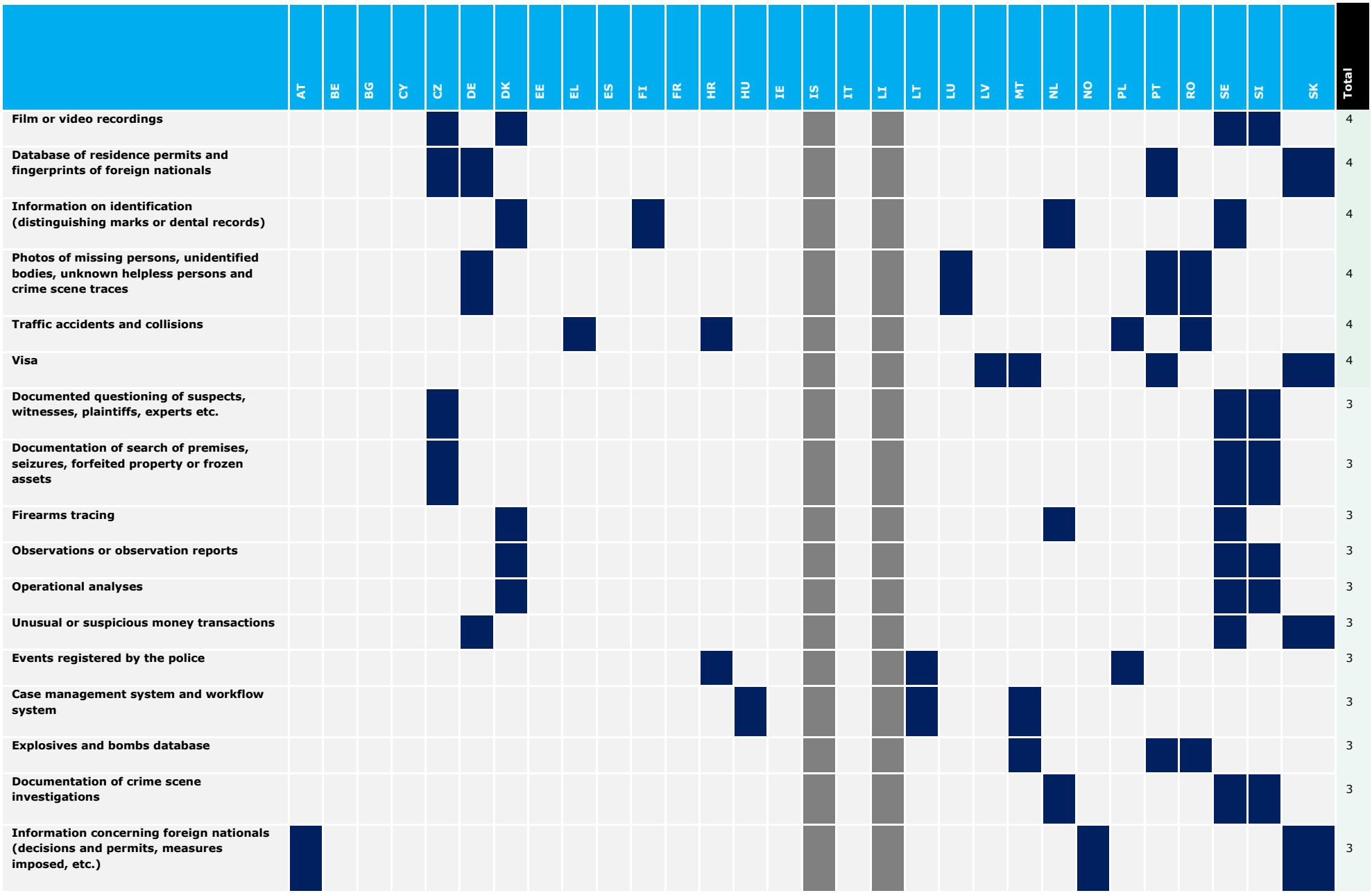
	Council Document No 9512/10 (Guidelines on the implementation of SFD)	Council Document 10492/14 (Guidelines for SPOC)	Council Document 6721/3/14 (SPOC guidelines)	Council Document 13034/14 (Guidelines on the implementation of SFD)	Council Document No 5825/20 (Manual on Law Enforcement Information Exchange)	Council Document No 9105/11 (PCCCs guidelines)	Football Handbook (2006/C 322/01)
							the NFIP has at its disposal, for the benefit of the NFIPs of the other countries, an updated risk-analysis related to its own clubs and its national team

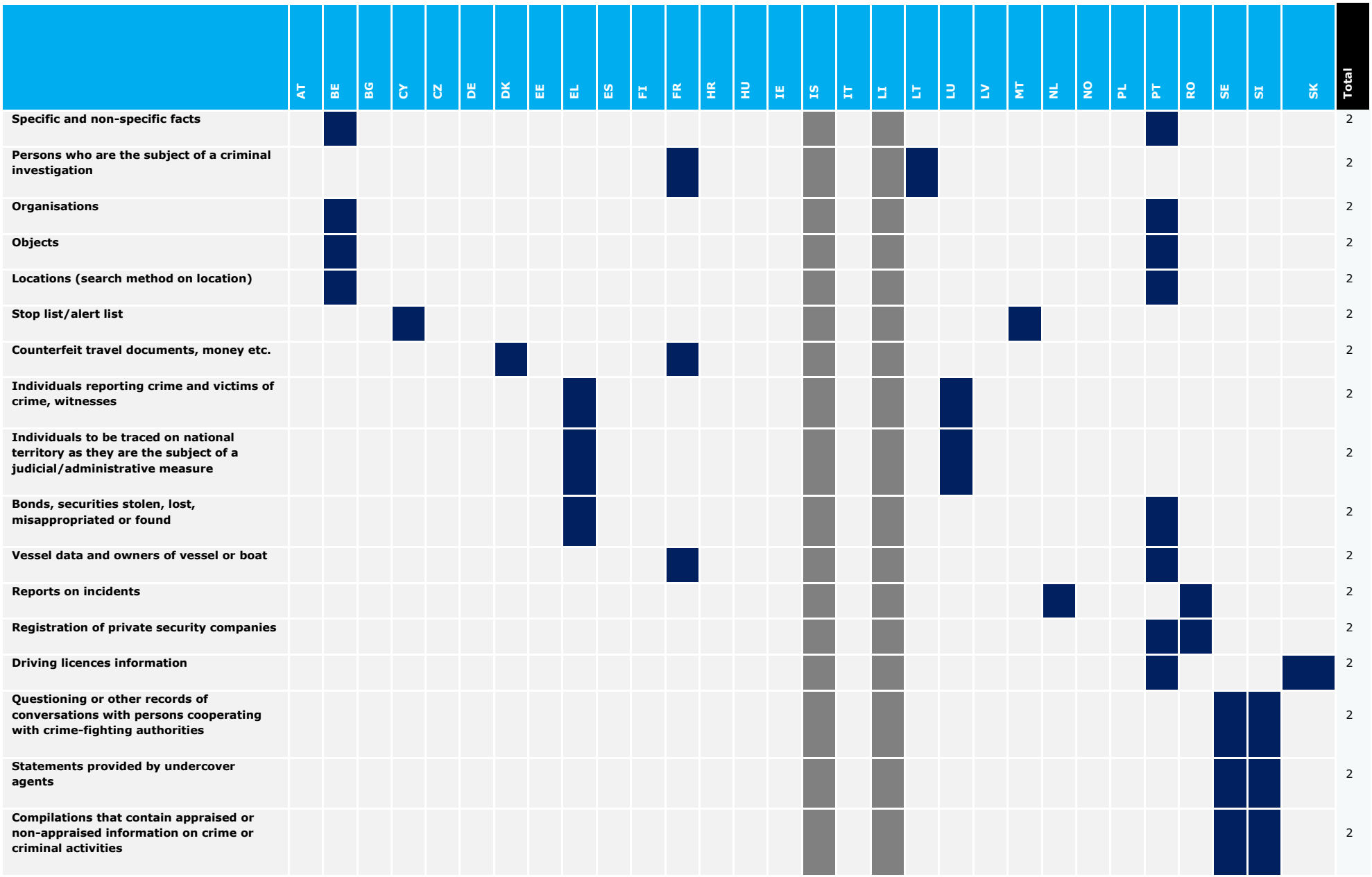
Source: Elaboration by the Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation

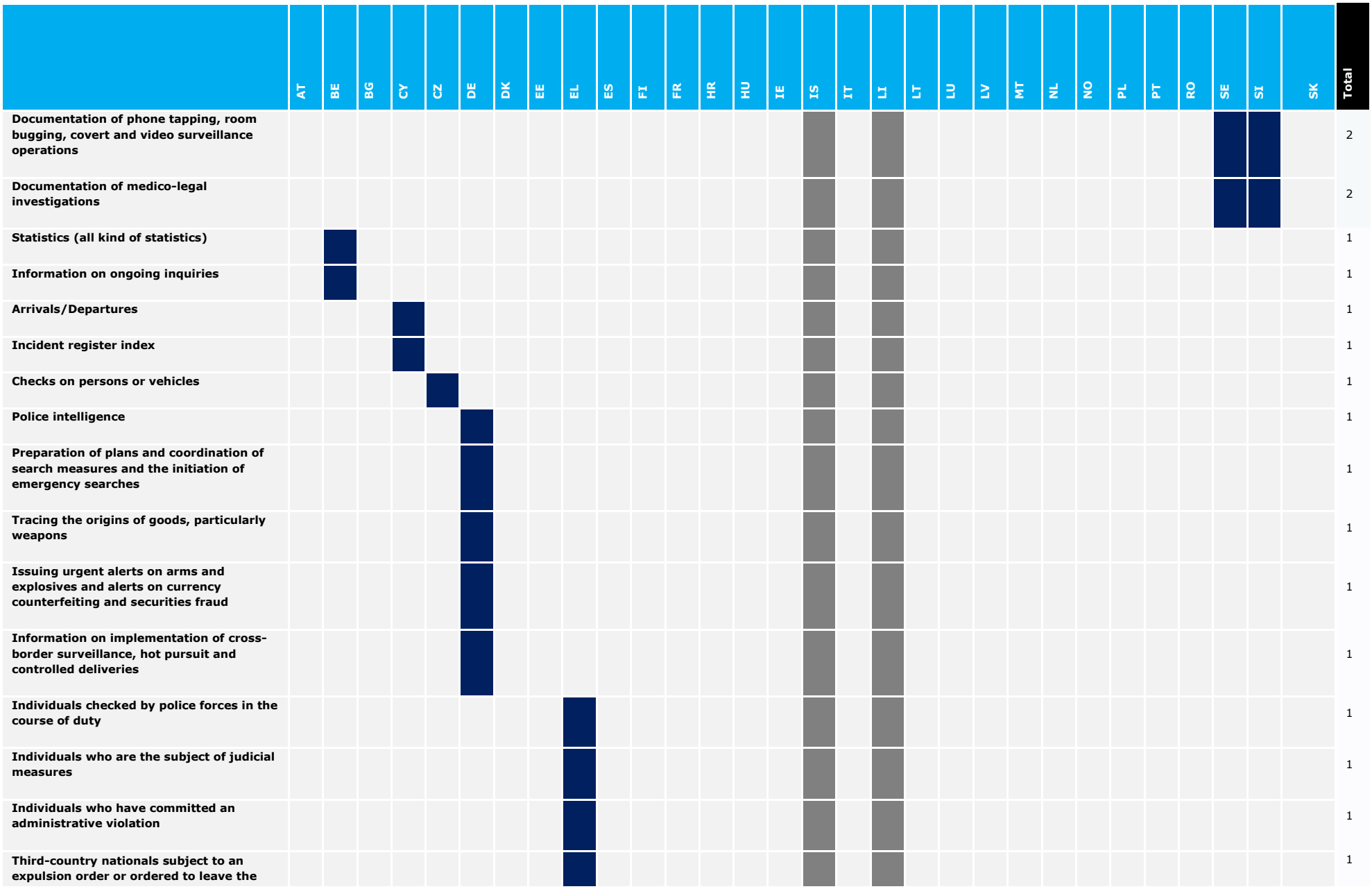
Types of data available to SPOCs from databases managed by the SPOC and directly accessible



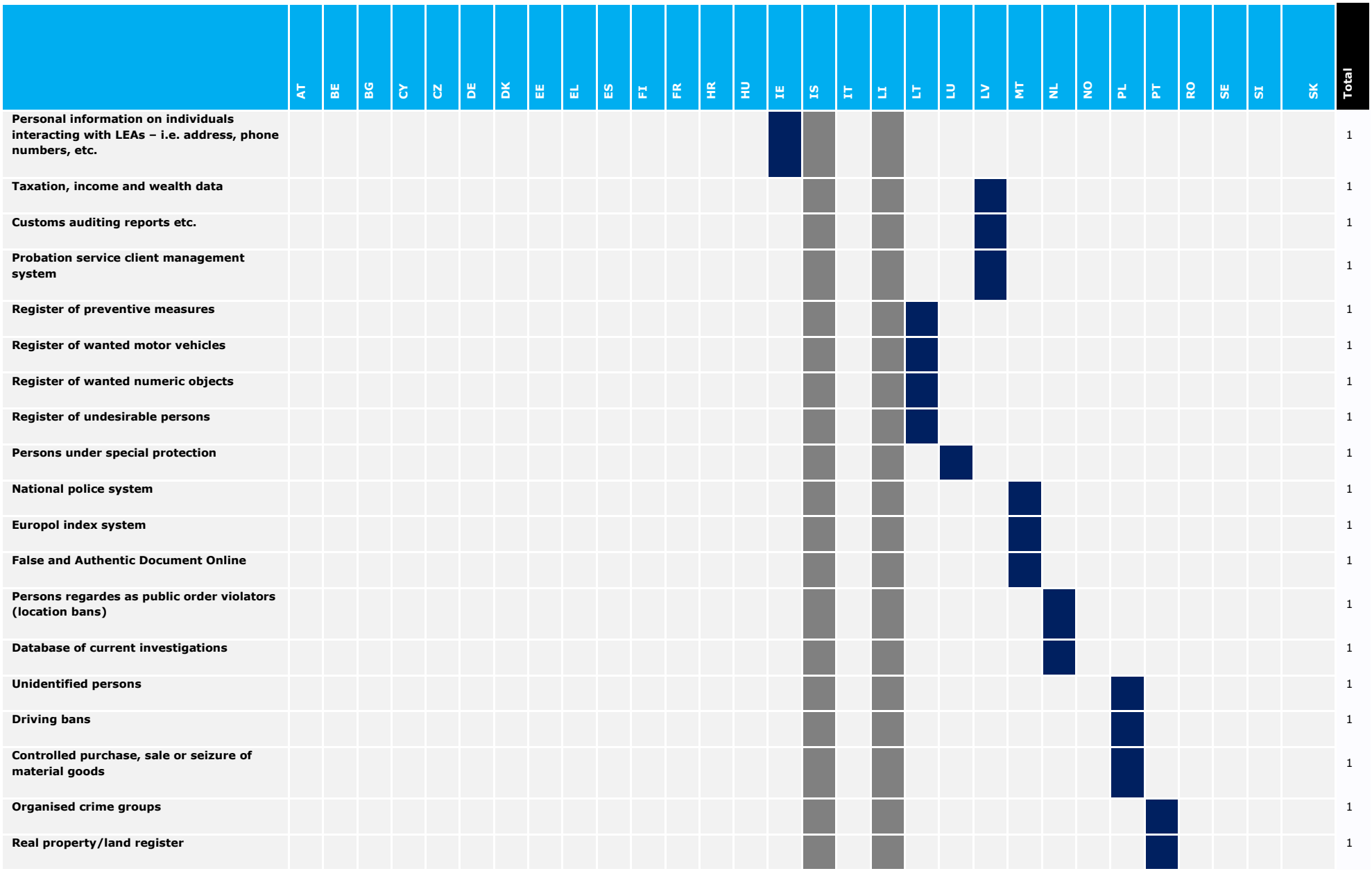

AT
BE
BG
CY
CZ
DE
DK
EE
EL
ES
FI
FR
HR
HU
IE
IS
IT
LI
LT
LU
LV
MT
NL
NO
PL
PT
RO
SE
SI
SK
Total
Passports and identity documents 11
Border controls, border crossings and other border guard matters 11
Reports (complaints) concerning crimes committed 10
Photographs (other than persons) 8
Information on modus operandi 8
Vehicle data and information on vehicle owners (cars) 7
Administrative register on persons (census) 7
Decisions prohibiting entry to premises or restraining orders 7
Customs authorities' information on import, export and transit of goods 7
Database of prison inmates 7
Traffic violations and misdemeanours 6
Police records 5
Decisions prohibiting entry to country and residence concerning foreign nationals 5
Stolen, lost or misappropriated passports and identity documents 5
Wanted, stolen, lost, misappropriated or found firearms, used on national territory 5
Other information that describes crimes committed or types of crime 4
Stolen works of art 4


AT BE BG CY CZ DE DK EE EL ES FI FR HR HU IE IS IT LI LT LU LV MT NL NO PL PT RO SE SI SK Total
Film or video recordings 4
Database of residence permits and fingerprints of foreign nationals 4
Information on identification (distinguishing marks or dental records) 4
Photos of missing persons, unidentified bodies, unknown helpless persons and crime scene traces 4
Traffic accidents and collisions 4
Visa 4
Documented questioning of suspects, witnesses, plaintiffs, experts etc. 3
Documentation of search of premises, seizures, forfeited property or frozen assets 3
Firearms tracing 3
Observations or observation reports 3
Operational analyses 3
Unusual or suspicious money transactions 3
Events registered by the police 3
Case management system and workflow system 3
Explosives and bombs database 3
Documentation of crime scene investigations 3
Information concerning foreign nationals (decisions and permits, measures imposed, etc.) 3


AT
BE
BG
CY
CZ
DE
DK
EE
EL
ES
FI
FR
HR
HU
IE
IS
IT
LI
LT
LU
LV
MT
NL
NO
PL
PT
RO
SE
SI
SK
Total
Specific and non-specific facts 2
Persons who are the subject of a criminal investigation 2
Organisations 2
Objects 2
Locations (search method on location) 2
Stop list/alert list 2
Counterfeit travel documents, money etc. 2
Individuals reporting crime and victims of crime, witnesses 2
Individuals to be traced on national territory as they are the subject of a judicial/administrative measure 2
Bonds, securities stolen, lost, misappropriated or found 2
Vessel data and owners of vessel or boat 2
Reports on incidents 2
Registration of private security companies 2
Driving licences information 2
Questioning or other records of conversations with persons cooperating with crime-fighting authorities 2
Statements provided by undercover agents 2
Compilations that contain appraised or non-appraised information on crime or criminal activities 2


AT
BE
BG
CY
CZ
DE
DK
EE
EL
ES
FI
FR
HR
HU
IE
IS
IT
LI
LT
LU
LV
MT
NL
NO
PL
PT
RO
SE
SI
SK
Total
Documentation of phone tapping, room bugging, covert and video surveillance operations 2
Documentation of medico-legal investigations 2
Statistics (all kind of statistics) 1
Information on ongoing inquiries 1
Arrivals/Departures 1
Incident register index 1
Checks on persons or vehicles 1
Police intelligence 1
Preparation of plans and coordination of search measures and the initiation of emergency searches 1
Tracing the origins of goods, particularly weapons 1
Issuing urgent alerts on arms and explosives and alerts on currency counterfeiting and securities fraud 1
Information on implementation of cross-border surveillance, hot pursuit and controlled deliveries 1
Individuals checked by police forces in the course of duty 1
Individuals who are the subject of judicial measures 1
Individuals who have committed an administrative violation 1
Third-country nationals subject to an expulsion order or ordered to leave the 1

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
national territory									■							■		■														
Owners of vehicles, documents involved in crime, lost or found									■							■		■														1
Individuals holding, buying, selling, storing or transporting weapons on or from national territory									■							■		■														1
European individuals holding a work permit									■							■		■														1
Individuals who are the subject of a foreign arrest warrant									■							■		■														1
Individuals banned from sporting events									■							■		■														1
Spouses of individuals involved in crimes									■							■		■														1
Persons found dead									■							■		■														1
Search due to administrative measures									■							■		■														1
Police station buildings management									■							■		■														1
Latent fingerprints and DNA databases									■							■		■														1
Third-country nationals who have applied for asylum									■							■		■														1
'Prisoners on leave' database									■							■		■														1
Previous histories of natural and legal persons who have committed customs offences												■				■		■														1
Data collected from submissions to the PHAROS platform for reporting unlawful conduct online												■				■		■														1
Database of minor offences												■				■		■														1
Previous enquiries – who has enquired on an entity															■	■		■														1

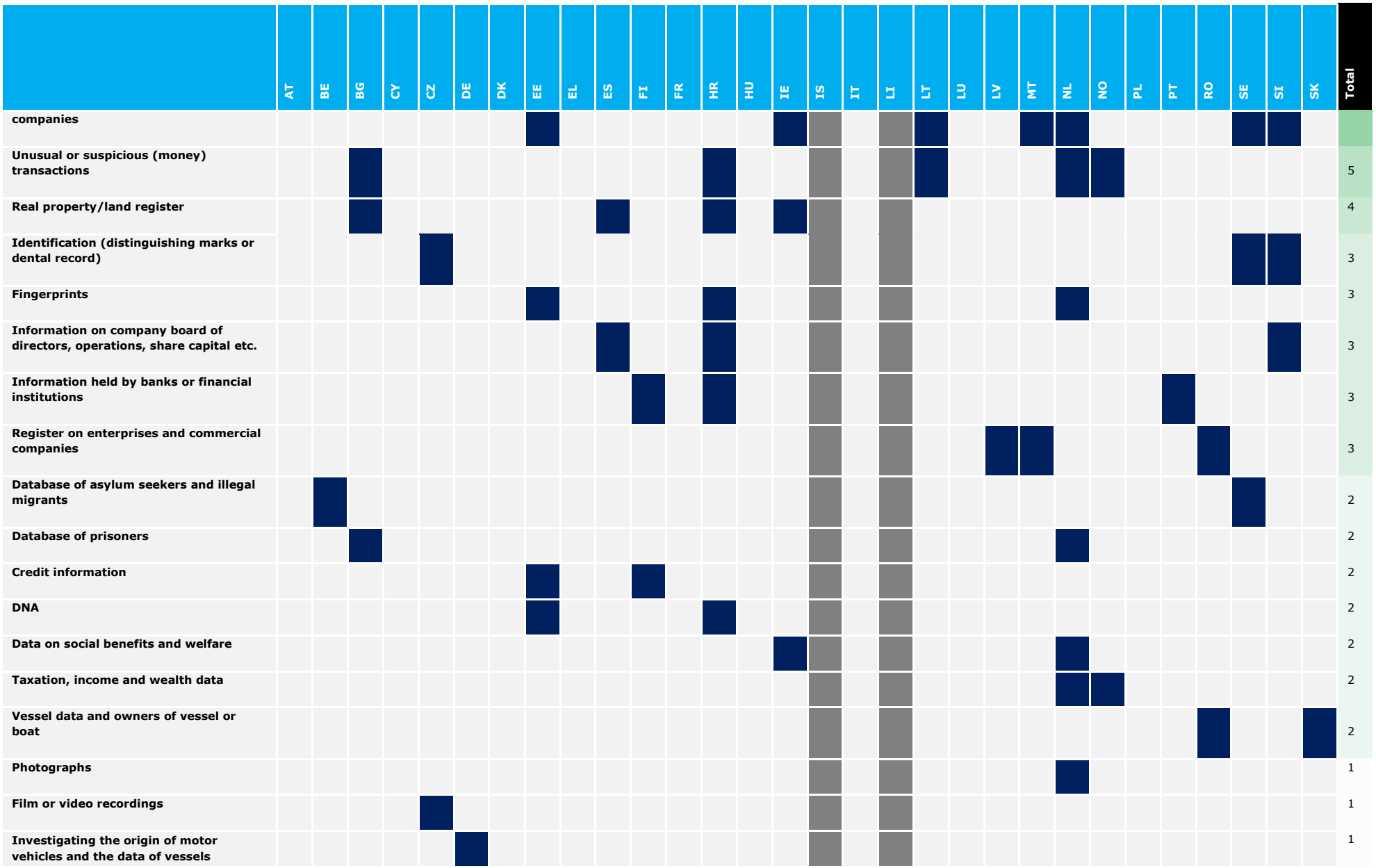

AT
BE
BG
CY
CZ
DE
DK
EE
EL
ES
FI
FR
HR
HU
IE
IS
IT
LI
LT
LU
LV
MT
NL
NO
PL
PT
RO
SE
SI
SK
Total
Personal information on individuals interacting with LEAs – i.e. address, phone numbers, etc. 1
Taxation, income and wealth data 1
Customs auditing reports etc. 1
Probation service client management system 1
Register of preventive measures 1
Register of wanted motor vehicles 1
Register of wanted numeric objects 1
Register of undesirable persons 1
Persons under special protection 1
National police system 1
Europol index system 1
False and Authentic Document Online 1
Persons regardes as public order violators (location bans) 1
Database of current investigations 1
Unidentified persons 1
Driving bans 1
Controlled purchase, sale or seizure of material goods 1
Organised crime groups 1
Real property/land register 1

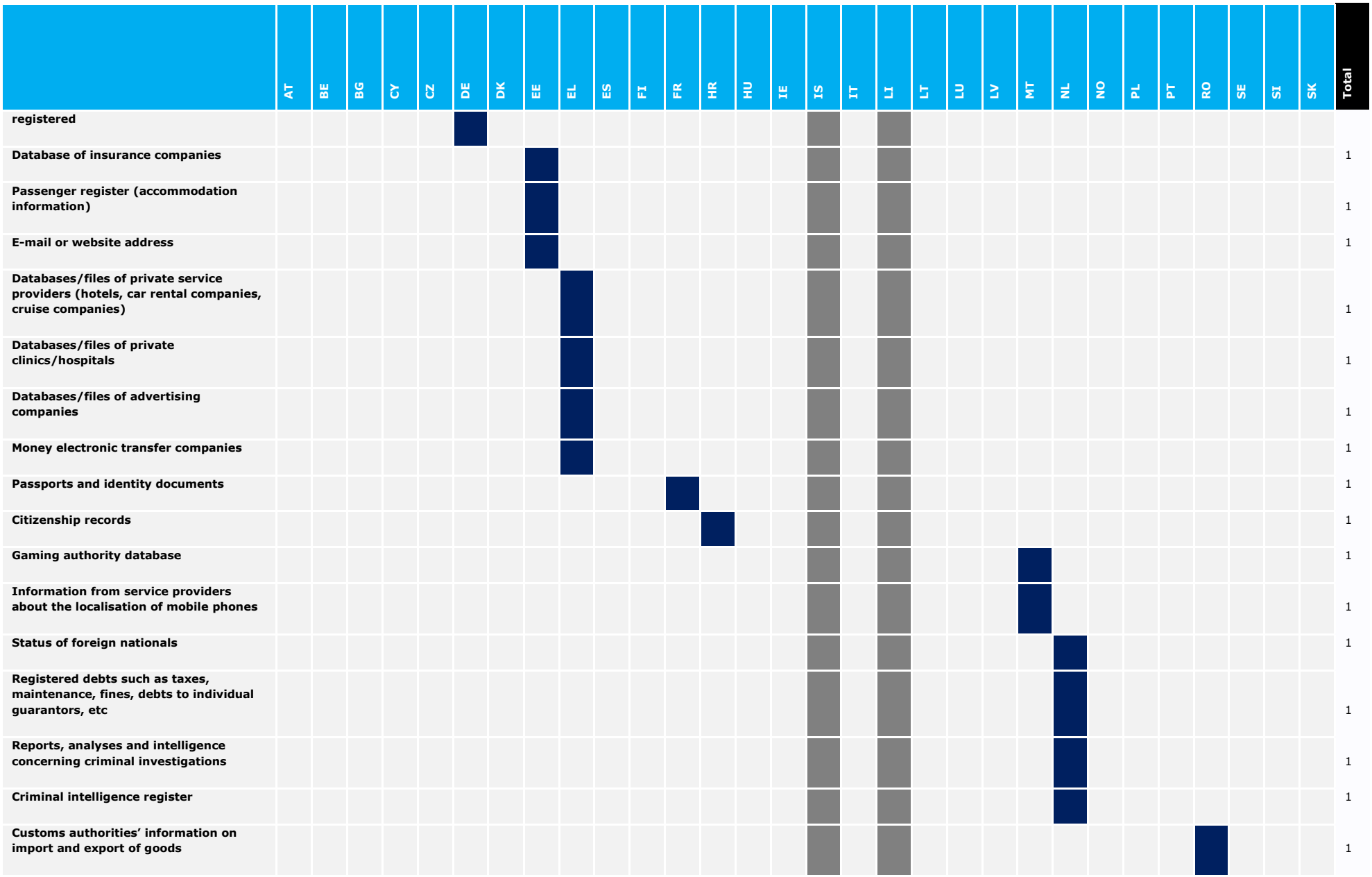
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Registration forms/data on foreign tourists from accommodation establishments																															1
Injunctions database: persons banned to leave the locality or not allowed to travel to certain localities																															1
'Banking fraud' database: persons suspected of having committed offences against banking system																															1
Digital facial recognition																															1
Information on address and accommodation																															1
Customs databases relating to the intracommunity delivery of goods																															1
Documentation of telecommunications monitoring																															1
Total	9	13	19	7	17	20	19	11	31	9	14	15	13	4	7	0	3	0	16	12	8	11	15	10	18	30	17	30	24	20	

Source: Elaboration by the Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation based on National Fact Sheets from the Manual on Law Enforcement Information Exchange

Types of data available to SPOCs from databases managed by another authority and indirectly accessible to the SPOC

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Identification of telecommunications subscribers																															10
Information (including personal data) held by telecommunication operators																															8
Passenger and freight lists of transport																															7


AT
BE
BG
CY
CZ
DE
DK
EE
EL
ES
FI
FR
HR
HU
IE
IS
IT
LI
LT
LU
LV
MT
NL
NO
PL
PT
RO
SE
SI
SK
Total
companies
Unusual or suspicious (money) transactions 5
Real property/land register 4
Identification (distinguishing marks or dental record) 3
Fingerprints 3
Information on company board of directors, operations, share capital etc. 3
Information held by banks or financial institutions 3
Register on enterprises and commercial companies 3
Database of asylum seekers and illegal migrants 2
Database of prisoners 2
Credit information 2
DNA 2
Data on social benefits and welfare 2
Taxation, income and wealth data 2
Vessel data and owners of vessel or boat 2
Photographs 1
Film or video recordings 1
Investigating the origin of motor vehicles and the data of vessels 1

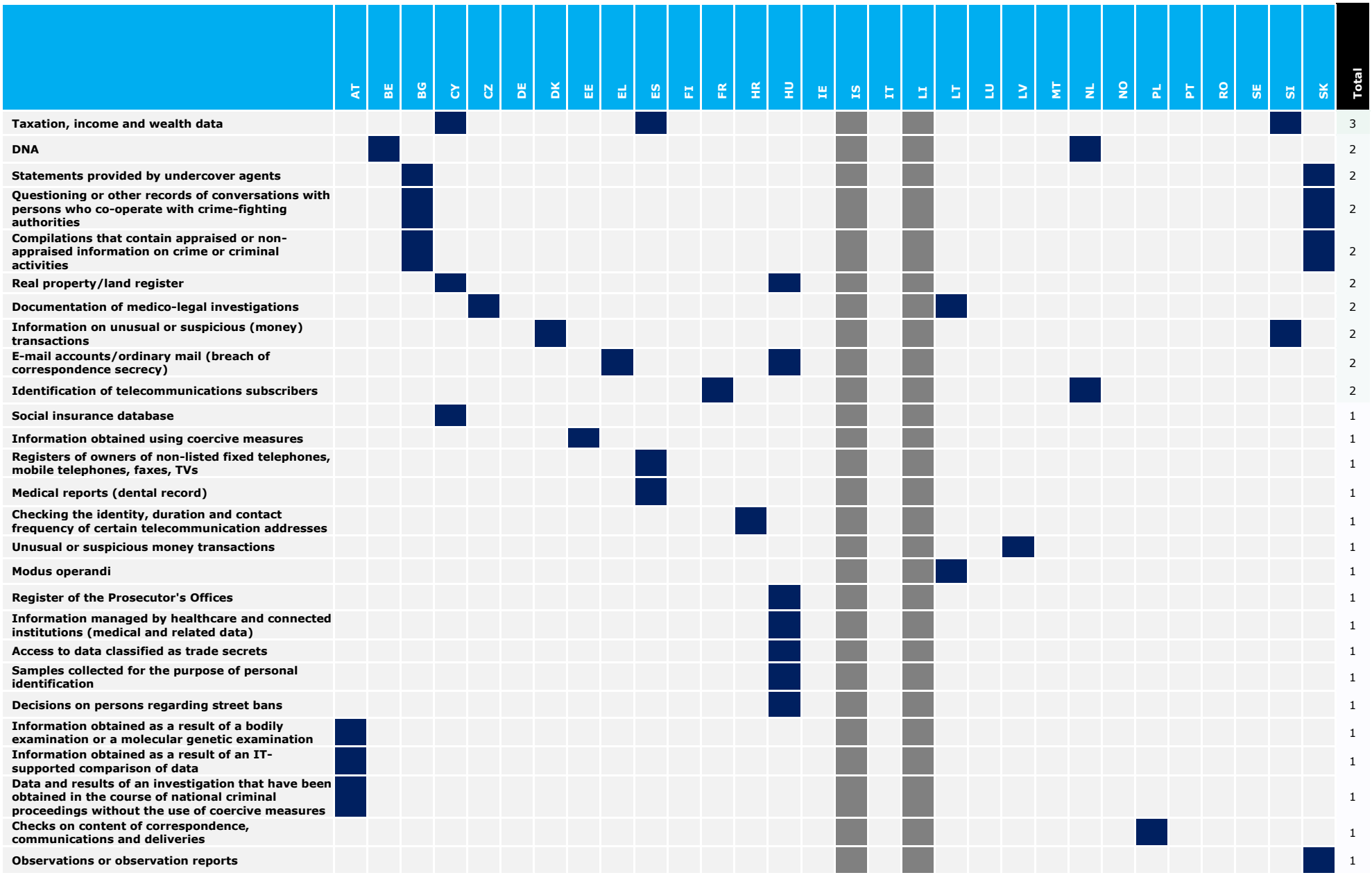

AT BE BG CY CZ DE DK EE EL ES FI FR HR HU IE IS IT LI LT LU LV MT NL NO PL PT RO SE SI SK Total
registered
Database of insurance companies 1
Passenger register (accommodation information) 1
E-mail or website address 1
Databases/files of private service providers (hotels, car rental companies, cruise companies) 1
Databases/files of private clinics/hospitals 1
Databases/files of advertising companies 1
Money electronic transfer companies 1
Passports and identity documents 1
Citizenship records 1
Gaming authority database 1
Information from service providers about the localisation of mobile phones 1
Status of foreign nationals 1
Registered debts such as taxes, maintenance, fines, debts to individual guarantors, etc 1
Reports, analyses and intelligence concerning criminal investigations 1
Criminal intelligence register 1
Customs authorities' information on import and export of goods 1

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Intellectual property rights																															1
Visa																															1
Management information system on cultural goods																															1
Information on transportation on inland waters																															1
Data concerning aircraft and owners of aircraft																															1
Persons convicted of crime (criminal records)																															1
Total	1	1	3	1	3	1	1	7	5	3	3	1	7	1	4	0	0	0	3	1	2	5	11	2	1	2	7	4	4	4	

Source: Elaboration by the Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation based on National Fact Sheets from the Manual on Law Enforcement Information Exchange

Types of data available to SPOCs from databases managed by judicial authorities

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Information held by banks or financial institutions																															21
Information (including personal data) held by telecommunication operators																															15
Documentation of search of premises, seizures, forfeited property or frozen assets																															7
Documentation of phone tapping, room bugging, covert and video surveillance operations																															7
Documented questioning of suspects, witnesses, plaintiffs, experts etc.																															5
Passenger and freight lists of transport companies																															4
Persons convicted of crime (criminal records)																															4
Reports (complaints) concerning crimes committed																															3
Documentation of crime scene investigations																															3


AT BE BG CY CZ DE DK EE EL ES FI FR HR HU IE IS IT LI LT LU LV MT NL NO PL PT RO SE SI SK Total
Taxation, income and wealth data 3
DNA 2
Statements provided by undercover agents 2
Questioning or other records of conversations with persons who co-operate with crime-fighting authorities 2
Compilations that contain appraised or non-appraised information on crime or criminal activities 2
Real property/land register 2
Documentation of medico-legal investigations 2
Information on unusual or suspicious (money) transactions 2
E-mail accounts/ordinary mail (breach of correspondence secrecy) 2
Identification of telecommunications subscribers 2
Social insurance database 1
Information obtained using coercive measures 1
Registers of owners of non-listed fixed telephones, mobile telephones, faxes, TVs 1
Medical reports (dental record) 1
Checking the identity, duration and contact frequency of certain telecommunication addresses 1
Unusual or suspicious money transactions 1
Modus operandi 1
Register of the Prosecutor's Offices 1
Information managed by healthcare and connected institutions (medical and related data) 1
Access to data classified as trade secrets 1
Samples collected for the purpose of personal identification 1
Decisions on persons regarding street bans 1
Information obtained as a result of a bodily examination or a molecular genetic examination 1
Information obtained as a result of an IT-supported comparison of data 1
Data and results of an investigation that have been obtained in the course of national criminal proceedings without the use of coercive measures 1
Checks on content of correspondence, communications and deliveries 1
Observations or observation reports 1

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Film or video recordings																															1
Total	6	3	8	5	5	0	4	2	3	5	2	4	3	13	1	0	1	0	8	0	5	1	5	3	2	1	3	0	5	10	

Source: Elaboration by the Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation based on National Fact Sheets from the Manual on Law Enforcement Information Exchange

ANNEX 6: QUESTIONNAIRE FOR CONSULTATIONS

Survey questionnaire for Law Enforcement Authorities

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
1	PERSONAL INFORMATION		Your first name*	open text	x	x	x	x	x	x	x	x
2	PERSONAL INFORMATION		Your last name*	open text	x	x	x	x	x	x	x	x
3	PERSONAL INFORMATION		Name of the organisation you belong to*	open text	x	x	x	x	x	x	x	x
4	PERSONAL INFORMATION		Your role*									
5	PERSONAL INFORMATION		Your email address*	open text	x	x	x	x	x	x	x	x
6	PERSONAL INFORMATION		Your country*	Drop down list of 27 + Schengen	x	x	x	x	x	x	x	x
7	THREAT LANDASCAPE	Challenges related to SOC	To what extent has the number of crimes evolved in the past 5-10 years in the following areas in your country?*	*Drugs *Illicit tobacco trade *Trafficking in human beings *Financial crimes *Cybercrime *Organised property crime	x	x	x	x		x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*Environmental crime *Trafficking of firearms *Illegal immigration *Terrorism *Other (please specify)								
8	THREAT LANDASCAPE	Challenges related to SOC	Can you please provide some figures related to crimes occurred over the past 5-10 years or indicate where we could find them?	open text	x	x	x	x		x	x	x
9	THREAT LANDASCAPE	Challenges related to SOC	In your view, to what extent do the following crime areas have a cross border dimension (i.e. require the EU-wide cooperation of law enforcement authorities to be properly addressed)?*	*Drugs *Illicit tobacco trade *Trafficking in human beings *Financial crimes *Cybercrime *Organised property crime *Environmental crime *Trafficking of firearms *Illegal immigration *Terrorism	x	x	x	x		x	x	x
9.A	THREAT LANDASCAPE	Challenges related to SOC	Could you please specify any other relevant crime area which you think it has a cross border		x	x	x	x		x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
			dimension?									
10	THREAT LANDASCAPE	Challenges related to SOC	How do you think the crime areas listed below will evolve over the next 5-10 years in your country?*	*Drugs *Illicit tobacco trade *Trafficking in human beings *Financial crimes *Cybercrime *Organised property crime *Environmental crime *Trafficking of firearms *Illegal immigration *Terrorism *Other (please specify)	x	x	x	x		x	x	x
11	THREAT LANDASCAPE	Challenges related to the security of EU citizens moving across the EU	In your view, how has the number of accidents linked to public order and safety evolved over the past 5-10 years in your country in the following areas?*	*International sport/music/cultural events *Flows of people moving for tourism *Flows of people moving for work	x	x	x	x	x	x	x	x
12	THREAT LANDASCAPE	Challenges related to the security of EU citizens moving across the EU	Can you please provide some figures related to accidents occurred over the past 5-10 years or indicate where we could find them?	open text	x	x	x	x	x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
13	THREAT LANDASCAPE	Challenges related to the security of EU citizens moving across the EU	In your view, to what extent do the following areas require cross-border law enforcement cooperation (i.e. require the EU-wide cooperation of law enforcement authorities to be properly managed)?*	*International sport/music/cultural events *Flows of people moving for tourism *Flows of people moving for work	x	x	x	x	x	x	x	x
13.A	THREAT LANDASCAPE	Challenges related to the security of EU citizens moving across the EU	Can you please specify any other type of event or activity which requires cross-border law enforcement cooperation in the area of public safety and/or public order?		x	x	x	x	x	x	x	x
14	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation SOC	How often do law enforcement authorities in your country undertake operational cooperation with law enforcement authorities in other countries in relation to the following crimes?*	*Drugs *Illicit tobacco trade *Trafficking in human beings *Financial crimes *Cybercrime *Organised property crime *Environmental crime *Trafficking of firearms *Illegal immigration	x		x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*Terrorism								
15	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation SOC	Out of all cases where your country undertook operational cooperation with other countries in relation to serious and organised crimes, what was the share of problematic cases?*	*Never had problematic cases *0-20% *20-40% *40-60% *60-80% *80-100% *All cases were problematic	x		x			x	x	x
16	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation SOC	What were the main reasons for the difficulties encountered?	*lack of clarity on the rules to be followed *missing or unclear points of contact *time delays *language barriers *different rules applicable to the same criminal act and investigative tools in the other country *high number of administrative requirements to comply with *lack of trust *other (please specify)	x		x			x	x	x
17	THE CURRENT EU FRAMEWORK	Operational cooperation	What were the main consequences of the	*Increase of time needed for the	x		x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	FOR LAW ENFORCEMENT COOPERATION	SOC	difficulties encountered?	investigations *Costs for complying with unexpected requirements *Impossibility to continue the investigation/case *Other (please specify)								
18	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation SOC	If difficulties encountered brought to time delays, can you please estimate these delays?	* 1-7 days * 2-4 weeks *2-3 months *More than 3 months *Don't know	x		x			x	x	x
19	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation SOC	If difficulties encountered brought to additional costs, can you please indicate the type of costs?	*Costs related to additional staff needed *Costs related to the compliance with unexpected requirements of the other country *Costs related to the purchase of new equipment *Other costs (please specify)	x		x			x	x	x
20	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT	Operational cooperation Public Order	How often do law enforcement authorities in your country undertake operational	*Crises and disasters *International sport/music/cultural events *Flows of people	x	x			x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	COOPERATION		cooperation with law enforcement authorities in other countries to ensure public order and safety?*	moving for tourism *Flows of people moving for work *Protection of public figures								
20.A	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation Public Order	Do you have any other relevant example of events or activities for which your country undertake operational cooperation with law enforcement authorities in other countries to ensure public order and safety?		x	x			x	x	x	x
21	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation Public Order	Out of all cases where your country undertook operational cooperation with other countries to ensure public order and safety, what was the share of problematic cases?*	*Never had problematic cases *0-20% *20-40% *40-60% *70-80% *80-100% *All cases were problematic	x	x			x	x	x	x
22	THE CURRENT EU FRAMEWORK	Operational cooperation	What were the main reasons for the	*Lack of clarity on the rules to be followed	x	x			x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	FOR LAW ENFORCEMENT COOPERATION	Public Order	difficulties encountered?	*Missing or unclear points of contact *Time delays *Language barriers *Different rules applicable to the same criminal act and investigative tools in the other country *High number of administrative requirements to comply with *Lack of trust *Other (please specify;								
23	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation Public Order	What were the main consequences of the difficulties encountered?	*Increase of time needed for the operation *Costs for complying with unexpected requirements *Impossibility to continue the operation *Other (please specify)	x	x			x	x	x	x
24	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation Public Order	If difficulties encountered brought to time delays, can you please estimate these delays?	* 1-7 days * 2-4 weeks *2-3 months *More than 3 months *Don't know	x	x			x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
25	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation Public Order	If difficulties encountered brought to additional costs, can you please indicate the type of costs?	*Costs related to additional staff needed *Costs related to the compliance with unexpected requirements of the other country *Costs related to the purchase of new equipment *Other costs (please specify)	x	x			x	x	x	x
26	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation - structures	To what degree do you use the following structures to cooperate with other law enforcement authorities in other countries?*	*Single Points of Contact (SPOCs) *Police Customs Cooperation Centres (PCCCs) *National SIRENE Bureaux *Europol National Units *Europol Liaison Officers *Football Points of Contact	x	x	x		x	x	x	x
27	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation - structures	Please list any other structures, not listed in the question above, that you use to facilitate cooperation with law	open text	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
			enforcement authorities in other countries?									
28	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation - structures	To what degree are the following structures effective in facilitating cross border cooperation between law enforcement authorities in your country and law enforcement authorities in other countries?*	*Single Points of Contact (SPOCs) *Police Customs Cooperation Centres (PCCCs) *National SIRENE Bureaux *Europol National Units *Europol Liaison Officers *Football Points of contact	x	x	x		x	x	x	x
29	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation - structures	To what degree do the following issues hamper cross border law enforcement cooperation using the structures listed above?*	*Confusion caused by the number of different points of contact in the countries (for example, liaison officers, Single Points Of Contacts - SPOCs, SIRENE Bureaux, ENUs, Police Customs Cooperation Centres - PCCCs, SIRENE Bureaux etc.) *Differences between countries in the way	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				that SPOCs are structured *SPOCs and PCCCs are not coordinated *Law enforcement practitioners are not aware of factsheets and manuals explaining the different roles and responsibilities *Factsheets and manuals providing implementation guidance are not kept up to date/are not clear, precise, committal enough to ensure proper implementation? *Lack of communication and coordination between different law enforcement authorities within countries *Lack of coordination between law enforcement and judicial authorities within countries								

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*Lack of coordination between policing and customs authorities within countries *Developments in relation to customs cooperation have occurred in parallel to the EU legal framework for law enforcement cooperation thus creating risks of duplications, inconsistencies and inefficiencies in operational situations								
30	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation - structures	Please provide further information and examples to illustrate the issues that hamper the use of the structures listed above.	open text	x	x	x		x	x	x	x
31	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange	How often do law enforcement authorities in your country undertake information sharing with law enforcement	*Drugs *Illicit tobacco trade *Trafficking in human beings *Financial crimes *Cybercrime *Organised property	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
			authorities in other countries in relation to the following criminal threats?*	crime *Environmental crime *Trafficking of firearms *Illegal immigration *Terrorism								
32	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange	How often do law enforcement authorities in your country undertake information sharing with law enforcement authorities in other countries for public order purposes?*	*Crises and disasters *International sport/music/cultural events *Flows of people moving for tourism *Flows of people moving for work *Protection of public figures *Other (please specify)	x	x	x		x	x	x	x
33	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange	Out of all cases where your country shared information with other countries, what was the share of problematic cases?*	*Never had problematic cases *0-20% *20-40% *40-60% *60-80% *80-100% *All cases were problematic	x	x	x		x	x	x	x
34	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT	Information exchange	What were the main reasons for the difficulties encountered?	*unclear rules to be followed *missing or unclear points of contact *time delays	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	COOPERATION			*language barriers *inadequate tools for the exchange of sensitive/confidential information *high number of administrative requirement to comply with *lack of trust *other (please specify)								
35	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange	What were the main consequences of the difficulties encountered?	*Increase of time needed for the investigations/acquisition of intelligence *Costs for complying with unexpected requirements *Impossibility to continue the investigation/case *Other (please specify)	x	x	x		x	x	x	x
36	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange	If difficulties encountered brought to time delays, can you please estimate these delays?	* 1-7 days * 2-4 weeks *2-3 months *More than 3 months *Don't know	x	x	x		x	x	x	x
37	THE CURRENT EU FRAMEWORK FOR LAW	Information exchange	If difficulties encountered brought to additional costs,	*Costs related to additional staff needed *Costs related to the	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	ENFORCEMENT COOPERATION		can you please indicate the type of costs?	compliance with unexpected requirements of the other countries *Costs related to the purchase of new equipment *Other costs (please specify)								
38	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange - platforms	To what degree do you use the following platforms to exchange information with law enforcement authorities in other countries?*	*SIENA *Schengen Information System (SIS))/SIRENE *Europol Information System (EIS) *Interpol exchange channels and databases	x	x	x		x	x	x	x
39	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange - platforms	Please list any other platforms, not listed in the question above, that you use to exchange information with law enforcement authorities in other countries	open text	x	x	x		x	x	x	x
40	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT	Information exchange - platforms	To what degree are the following platforms effective in facilitating the	*SIENA *Schengen Information System (SIS))/SIRENE	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	COOPERATION		exchange of information among law enforcement authorities in different countries?*	*Europol Information System (EIS) *Interpol exchange channels and databases								
41	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange - platforms	To what degree do the following issues hamper cross border law enforcement cooperation through the platforms listed above?*	*The EU legal framework for cross-border law enforcement cooperation is not consolidated (i.e. it is spread across several legislative instruments) *Council guideline papers on info exchange are found not clear, precise and complete enough to offer added value in the implementation of the EU texts *The complexity (overlaps, discrepancies, gaps) in the EU legal framework for information exchange *The EU legal framework for cross-border law	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				enforcement cooperation is not consistently implemented across the countries (i.e. the countries implement it differently) *Access to these platforms differs between countries *Differences between countries in how regularly these platforms are monitored/ response times to requests sent via these platforms *Heterogeneity in law enforcement actors, tools, and capacities in relation to cross-border cooperation creates confusion and burdens on the concerned stakeholders *Confusion due to the number of different exchange platforms and databases for EU information exchange *Data protection								

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				requirements limit exchange of information with law enforcement authorities in other countries								
42	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange - platforms	Please provide further information and examples to explain your answers about the issues that hamper the use of the platforms for exchange of information listed	open text	x	x	x		x	x	x	x
43	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/ risk analysis	How often do you/your department undertake cross-border threat assessment/risk analysis?*	*Always *Very frequently Occasionally *Very infrequently *Never *Don't know				x				
44	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/ risk analysis	What were the main reasons for undertaking cross-border threat assessment/risk analysis?	*To feed the design of national law enforcement strategies and actions *To plan joint operations/patrols *To regularly update the national intelligence picture *Other (please				x				

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				specify)								
45	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/ risk analysis	If you/your department undertake cross-border threat assessment/risk analysis, are these elaborated with other relevant national stakeholders?	*Yes *No *Don't know				x				
46	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/ risk analysis	If yes, what type stakeholders? (select all that apply)	*Police *Customs *Financial Investigation Units *Other (please specify)				x				
47	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/ risk analysis	Does your department involve stakeholders from other concerned countries in the implementation of cross-border threat assessments/risk analysis?	*Yes *No *Don't know				x				
48	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT	Cross-border threat assessment/ risk analysis	If yes, what type stakeholders in the other countries are usually involved in	*Single Points of Contacts *Police Customs Cooperation Centres				x				

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	COOPERATION		cross-border threat assessments/risk analysis? (select all that apply)	*Specialised investigation units *Specialised analytical departments *Public safety/order specialists (especially the ones (who have been) involved in joint patrols, joint operations) *Football contact points *Customs *Other (please specify)								
49	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/ risk analysis	Are cross-border threat assessment/risk analysis shared with the neighbouring country(ies) in view of joint analytical documents?*	*Yes *No *Don't know				x				
50	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/ risk analysis	If yes, with which country(ies)?	open text				x				
51	THE CURRENT EU FRAMEWORK FOR LAW	Cross-border threat assessment/	Can cross-border threat assessment/risk	*Yes *No				x				

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	ENFORCEMENT COOPERATION	risk analysis	analysis be used to schedule the precise location and timing of joint operations?*	*Don't know								
52	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/ risk analysis	If not, why?	open text				x				
53	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/ risk analysis	Can you please shortly describe how cross-border threat assessments/risk analysis is implemented? (e.g. type of information requested, types of analysis performed)	open text				x				
54	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/ risk analysis	Out of all cases where you/your department undertook cross-border threat assessment/risk analysis, what was the share of problematic cases?	*Never had problematic cases *0-20% *20-40% *40-60% *60-80% *80-100% *All cases were problematic				x				
55	THE CURRENT EU FRAMEWORK FOR LAW	Cross-border threat assessment/	What were the main reasons for the difficulties	open text				x				

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	ENFORCEMENT COOPERATION	risk analysis	encountered?									
56	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Investigative tools for cross border crimes	How often are the following investigative tools used in cross-border investigations involving cooperation between law enforcement authorities in your country and those in other countries?*	*Cross border surveillance (physical) *Interception of communication *Covert investigations - undercover officers *Controlled deliveries *Informants *Hot pursuit *Special intervention units *Joint Patrols *Joint Police Offices *Witness protection	x	x	x			x	x	x
57	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Investigative tools for cross border crimes	What other investigative tools, not listed above, are used in cross-border investigations involving cooperation between law enforcement authorities in your country and those in other countries?	open text	x	x	x			x	x	x
58	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT	Investigative tools for cross border crimes	To what degree are the following tools effective in generating	*Cross border surveillance (physical) *Interception of communication	x	x	x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	COOPERATION		intelligence and evidence and/ or leading to the disruption of crimes in cross-border investigations involving cooperation between law enforcement authorities in your country and those in other countries?*	*Covert investigations - undercover officers *Controlled deliveries *Informants *Hot pursuit *Special intervention units *Joint Patrols *Joint Police Offices *Witness protection								
59	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Investigative tools for cross border crimes	To what degree do the following act as barriers to the effective use of the investigative tools listed above in cross border cases?*	*Differences in national legislation regarding the offences for which an investigative tool may be authorised *Differences in national definitions regarding the length of time for which a special investigative tool may be authorised/ regularity of review *Other differences in national legislation regarding definition and scope of investigative tools	x	x	x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*Financial costs of conducting cross-border operations utilising special investigative tools *Differences between countries in technologies (for example, different communications systems, different surveillance technologies) *Challenges in trust between countries *Restrictions on the ability to use investigative tools due to data protection regulations *Restrictions on the ability to use investigative tools due to fundamental rights protections *Lack of knowledge and training among law enforcement practitioners about how to apply for or implement investigative tools								

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
60	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Investigative tools for cross border crimes	Please provide further details to explain your answers above and to illustrate concrete examples of barriers to use of investigative tools in cross border cases.	open text	x	x	x			x	x	x
61	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	General	To what degree does the EU legal framework provide the necessary mechanisms for law enforcement authorities in your country to cooperate with other countries?*	*Schengen acquis - 1990 Convention implementing the Schengen Agreement of 1985 (CISA) *Swedish Framework Decision (Council Framework Decision 2006/960) *Naples II Convention (1998) *Prüm Decision (Council Decision 2008/615/JHA) *Council Decision 2007/412/JHA concerning security in connection with football matches with an international dimension *Council Decision	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				2006/560/JHA of 24 July 2006 on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States								
62	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	General	Has your country adopted other measures to enable cross border cooperation besides those provided by the EU legal framework?*	*Yes *No *Don't know	x	x	x		x	x	x	x
63	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	General	If yes, why?	*The EU legal Framework does not properly address the needs of my country *The EU legal framework is too complex and difficult to implement *It is easier to use measures and practices which stem from a national strategy than those offered by the EU framework *Other (please	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				specify)								
64	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	General	To what degree are the following non-binding documents useful to ensure the proper implementation of the Swedish Framework Decision, the Schengen acquis (CISA Convention), Prüm decision on joint operations and other documents they refer to?*	*Updated Catalogue of Recommendations for the correct application of the Schengen Acquis and Best practices: Police cooperation (15785/3/10); *Guidelines on the implementation of the Swedish Framework Decision (13034/14); *Draft Guidelines for a Single Point of Contact (SPOC) for international law enforcement information exchange (10492/14); *Manual on cross border operations (13887/20) and its National Factsheets (13920/20); *Manual on Law Enforcement Information Exchange (5825/20)	X	X	X		X	X	X	X
65	THE CURRENT EU FRAMEWORK	General	Can you please explain your	open text	X	X	X		X	X	X	X

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	FOR LAW ENFORCEMENT COOPERATION		previous assessment and indicate aspects of the documents that require improvement									
64.A	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	General	Do you have any other example of Council guideline papers of relevance? Please specify.		X	X	X		X	X	X	X
66	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	General	Do you see additional barriers (not already listed above) to cross border law enforcement cooperation and to the effective use of investigative tools in cross border cases? If yes please specify	open text	x	x	x		X	x	x	x
67	MULTILATERAL AGREEMENTS	Number and type	Has your country entered into any bi/tri/multilateral agreements regarding law enforcement operational cooperation or information exchange with law	*Yes *No *Don't know	x	x						x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
			enforcement authorities in other countries?*									
68	MULTILATERAL AGREEMENTS	Number and type	If so, how many separate agreements has your country entered into?	1 2 3 4 5-10 More than 10 I don't know	x	x						x
69	MULTILATERAL AGREEMENTS	Number and type	What type of stakeholders are involved in the implementation of these agreements?	*Only police *Only customs *Police and customs *I don't know *Other, please specify	x	x						x
70	MULTILATERAL AGREEMENTS	Number and type	Can you please list the agreements and provide the reference to the legal documents?	open text	x	x						x
71	MULTILATERAL AGREEMENTS	Number and type	How frequently or infrequently are these bi/tri/multilateral agreements used in practice?	*Very frequently (used in the majority of cross-border investigations with the signatory countries) *Occasionally (used in some cross border investigations) *Very infrequently (used in a small	x	x						x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				minority of cross border investigations) *Never *Don't know								
72	MULTILATERAL AGREEMENTS	Scope and objectives	What was the reason your country decided to enter in the bi/tri/multilateral agreements?	open text	x	x						x
73	MULTILATERAL AGREEMENTS	Scope and objectives	What value did it add above existing EU and national frameworks facilitating cross border cooperation?	open text	x	x						x
74	MULTILATERAL AGREEMENTS	Scope and objectives	Are the following included in the bi/tri/multilateral agreements that your country has entered into?	*Information sharing *Joint Patrols *Joint offices or joint Units *Hot (cross-border) pursuit *Cross border surveillance *Joint threat assessment/risk analyses in view of tailored joint operations *Communications *Access to national databases	x	x						x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*Competence/ authority on transport networks *Joint training *Authority to exercise police powers in another MS								
74.A	MULTILATERAL AGREEMENTS	Scope and objectives	Is there any additional feature of the bi/tri/multilateral agreements that your country has entered into that was not listed above? Please specify.		x	x						x
75	MULTILATERAL AGREEMENTS	Good practices and areas for improvement	To what extent are these bi/tri/multilateral agreements effective in facilitating cross border cooperation between law enforcement authorities in your country and law enforcement authorities in other countries?	Very high extent High extent Moderate extent Small extent Not at all Don't know	x	x						x
76	MULTILATERAL AGREEMENTS	Good practices and areas for	To what extent do you agree with the following statements	*In my country there are too many bi/tri/multilateral	x	x						x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
		improvement	about the bi/tri/multilateral agreements that your country has entered into?	agreements, causing complexity *The bi/tri/multilateral agreements are outdated *The bi/tri/multilateral agreements should be used more *The bi/tri/multilateral agreements are procedurally heavy *The bi/tri/multilateral agreements do not provide the powers needed for effective cross border cooperation *Overall, the bi/tri/multilateral agreements work well *These agreements do not cover joint threat assessment/risk analyses in view of tailored joint operations; *When agreements provide for joint threat assessment/risk analyses, they are not been used in practice.								

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
77	MULTILATERAL AGREEMENTS	Good practices and areas for improvement	Are there any aspects of the bi/tri/multilateral agreements that your country is part on which you would recommend as good practice to other countries?	open text	x	x						x
78	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Tools in use	How frequently do law enforcement authorities in your country use the following investigative tools to investigate serious and organised crime at the national level?*	*Controlled delivery (i.e. allowing suspicious shipments or cargo to leave, pass through or enter a jurisdiction with the knowledge and supervision of authorities) *Hot pursuit *Surveillance – Audio surveillance (e.g. Phone tapping; VOIP; Listening devices) *Surveillance – Visual surveillance (e.g. Hidden video-surveillance devices; body-worn video devices ; CCTV) *Surveillance – Tracking surveillance	x	x	x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				(e.g. GPS/transponders; mobile phones; radio-frequency identification devices (RFID); biometric info technology) *Surveillance – Data surveillance (e.g. computer/internet (spyware); mobile phones; keystroke monitoring) *Undercover operations *Use of informants – Members of the public *Use of informants – Victim of a crime *Use of informants – Members of an Organised Crime Group (OCG) *Use of informants – Other police officers *Witness protection								
79	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT	Tools in use	In what crime areas are the following tools used in your country?*	*Controlled delivery (i.e. allowing suspicious shipments or cargo to leave, pass through or enter a	x	x	x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	ORGANISED CRIME			jurisdiction with the knowledge and supervision of authorities) *Hot pursuit *Surveillance – Audio surveillance (e.g. Phone tapping; VOIP; Listening devices) *Surveillance – Visual surveillance (e.g. Hidden video-surveillance devices; body-worn video devices ; CCTV) *Surveillance – Tracking surveillance (e.g. GPS/transponders; mobile phones; radio-frequency identification devices (RFID); biometric info technology) *Surveillance – Data surveillance (e.g. computer/internet (spyware); mobile phones; keystroke monitoring) *Undercover/covert operations								

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*Use of informants – Members of the public *Use of informants – Victim of a crime *Use of informants – Members of an Organised Crime Group (OCG) *Use of informants – Other police officers *Witness protection								
80	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Tools in use	What types of measures are required to implement the following investigative tools across borders?*	*Controlled delivery (i.e. allowing suspicious shipments or cargo to leave, pass through or enter a jurisdiction with the knowledge and supervision of authorities) *Hot pursuit *Surveillance – Audio surveillance (e.g. Phone tapping; VOIP; Listening devices) *Surveillance – Visual surveillance (e.g. Hidden video-surveillance devices; body-worn video devices ; CCTV)	x	x	x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*Surveillance – Tracking surveillance (e.g. GPS/transponders; mobile phones; radio-frequency identification devices (RFID); biometric info technology) *Surveillance – Data surveillance (e.g. computer/internet (spyware); mobile phones; keystroke monitoring) *Undercover/covert operations *Use of informants – Members of the public *Use of informants – Victim of a crime *Use of informants – Members of an Organised Crime Group (OCG) *Use of informants – Other police officers *Witness protection								
81	INVESTIGATIVE TOOLS USED AT THE NATIONAL	Tools in use	Please list any investigative tools, not listed in the	open text	x	x	x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	LEVEL TO COMBAT ORGANISED CRIME		previous question, which are allowed and used in your country to tackle serious and organised crime at the national level and specify for what crime area they are used									
82	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Tools in use	Can you please indicate relevant national documents where the tools and the related applicable rules are described?	open text	x	x	x			x	x	x
83	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Effectiveness of tools	To what degree do you consider the following tools to be effective in combating organised crime or other serious crimes when investigating organised crime groups?*	*Controlled delivery (i.e. allowing suspicious shipments or cargo to leave, pass through or enter a jurisdiction with the knowledge and supervision of authorities) *Hot pursuit *Surveillance – Audio surveillance (e.g. Phone tapping; VOIP; Listening devices)	x	x	x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*Surveillance – Visual surveillance (e.g. Hidden video-surveillance devices; body-worn video devices ; CCTV) *Surveillance – Tracking surveillance (e.g. GPS/transponders; mobile phones; radio-frequency identification devices (RFID); biometric info technology) *Surveillance – Data surveillance (e.g. computer/internet (spyware); mobile phones; keystroke monitoring) *Undercover/covert operations *Use of informants – Members of the public *Use of informants – Victim of a crime *Use of informants – Members of an Organised Crime Group (OCG) *Use of informants –								

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				Other police officers *Witness protection								
84	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Effectiveness of tools	Are there any investigative tools currently available in your country that you would like to change - if so, how?	open text	x	x	x			x	x	x
85	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Effectiveness of tools	Are there any investigative tools NOT currently available in your country that you would like to be able to use?	open text	x	x	x			x	x	x
86	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Effectiveness of tools	Do you consider existing national safeguards as appropriate to protect the rights of the individuals when using the investigative tools listed above?*	*Yes *No *Don't know	x	x	x			x	x	x
87	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT	Effectiveness of tools	If not, can you please explain why?	open text	x	x	x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	ORGANISED CRIME											
88	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Need for EU Action	To what extent, in your view, is there a need for EU intervention to improve cross-border law enforcement operational cooperation to the following types of crimes?*	*Drugs *Illicit tobacco trade *Trafficking in human beings *Financial crimes *Cybercrime *Organised property crime *Environmental crime *Trafficking of firearms *Illegal immigration *Terrorism	x		x			x	x	x
89	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Need for EU Action	To what extent, in your view, is there a need for EU intervention to improve cross-border law enforcement operational cooperation to ensure public order and safety?*	*Crises and disasters *International sport/music/cultural events *Flows of people moving for tourism *Flows of people moving for work *Protection of public figures	x	x			x	x	x	x
90	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Need for EU Action	To what extent, in your view, is there a need for EU intervention to improve cross-border	Very high extent High extent Moderate extent Small extent Not at all	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
			information exchange among law enforcement authorities?*	Don't know								
91	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Need for EU Action	To what extent, in your view, is there a need for EU intervention to improve cross-border threat assessment/risk analysis?*	Very high extent High extent Moderate extent Small extent Not at all Don't know				x				
92	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Need for EU Action	If you see the need for EU intervention, can you please explain what would be the added value of the intervention compared to what countries could achieve alone?	open text	x	x	x	x	x	x	x	x
93	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	What type of measures the EU can adopt to improve cross-border threat assessment/risk analysis?	open text				x				
94	NEED FOR EU ACTION AND POSSIBLE	Policy Options	To what extent do you think the following options can	*Consolidation, streamlining and clarification of the EU	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	SOLUTIONS		contribute to improving cross-border law enforcement cooperation between countries?*	legal framework providing the basis for law enforcement cooperation *Modernisation of the EU legal framework providing the basis for law enforcement cooperation (e.g. by providing provisions to cover the use of recent technological developments) *Definition of minimum EU standards for organised crime investigations *Creation of a single set of rules for the same actions, whether carried out by the police or by customs authorities *Setting up new operational initiatives for law enforcement cooperation *Design of new recommendations, guidelines and good practices for law								

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				enforcement cooperation								
95	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	Please provide further details to explain your answer	open text	x	x	x		x	x	x	x
96	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	Please list any other changes or steps do you think should be taken to improve cross-border law enforcement cooperation between countries	open text	x	x	x		x	x	x	x
97	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	To what extent do you think EU intervention to harmonise the definitions and procedures relating to the following investigative tools would improve cross border cooperation?*	*Controlled delivery (i.e. allowing suspicious shipments or cargo to leave, pass through or enter a jurisdiction with the knowledge and supervision of authorities) *Hot pursuit *Surveillance – Audio surveillance (e.g. Phone tapping; VOIP; Listening devices) *Surveillance – Visual surveillance (e.g. Hidden video-	x	x	x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				surveillance devices; body-worn video devices ; CCTV) *Surveillance – Tracking surveillance (e.g. GPS/transponders; mobile phones; radio-frequency identification devices (RFID); biometric info technology) *Surveillance – Data surveillance (e.g. computer/internet (spyware); mobile phones; keystroke monitoring) *Undercover/covert operations *Use of informants – Members of the public *Use of informants – Victim of a crime *Use of informants – Members of an Organised Crime Group (OCG) *Use of informants – Other police officers *Witness protection								

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
98	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	Please provide further details to explain your answer	open text	x	x	x			x	x	x
99	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	Please list any other investigative tools you think should have common definitions or approaches at the EU level?	open text	x	x	x			x	x	x
100	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Need for EU Action	To what extent do you think there is a need for EU action to harmonise and standardise the cooperation measures and standards currently included in bi/tri/multilateral agreements?*		x	x						x
101	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Need for EU Action	Please provide further details to explain your answer	open text	x	x						x
102	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	EU action might bring law enforcement authorities in your		x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
			country to get additional powers. To what extent do you think this requires additional safeguards to be adopted in your country?*									
103	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	Could you please illustrate the types of safeguards that you think should be adopted?	open text	x	x	x		x	x	x	x
104		General	Please include any additional contribution you would like to make to the study	open text	x	x	x	x	x	x	x	x
105		General	Would you like to be involved in the next consultation activities related to this study (interviews and focus groups)?*	*Yes *No	x	x	x	x	x	x	x	x
					94	87	72	32	50	80	80	94

Source: Elaboration by the Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation

ANNEX 7: DISCARDED OPTIONS

In line with the *Better Regulation Guidelines*, a long list of policy options was prepared following the problem assessment, the assessment of the EU's right to act and the identification of relevant policy options, taking into account the evidence of specific problems, as well as good practices and suggestions by stakeholders.

The long list of options was subject to a screening in order to identify the most effective and viable sub-options, which were subsequently clustered into two comprehensive policy options (in addition to the status quo / baseline policy option).

The screening was based on effectiveness and feasibility criteria.

The findings of the assessment are presented in the table below. The sub-options that are of legislative nature are marked in **bold**.

List of discarded sub-options (measures / elements)

Identifier	Potential sub-options	Reason for discarding the sub-option
1. The access to and exchange of necessary information among law enforcement authorities is subject to legal, technical and structural challenges		
1.1 Law enforcement authorities face difficulties in interpreting and implementing relevant EU provisions		
The scope of application of some EU measures is unclear, including between (i) the SFD vs. CISA (i.e. preventative and/or repressive operations) and (ii) the SFD vs. the Naples II Convention (whether only police or also customs authorities can use both these measures)		
The distinction between law enforcement authorities entitled to use the SFD and the Naples II Convention (notably police vs. customs) has proved ambiguous, since the competencies vary between law enforcement agencies and countries.		
2	**Provision of a definition of what competences the law enforcement authorities to which the new Law Enforcement Code is applicable need to have.** **The Naples II Convention would be repealed and the current scope of the SFP would apply also to customs.** *Exemplary definition: The new Law Enforcement Code should apply to Police and all other law enforcement authorities authorised by national law to detect, prevent and investigate offences or criminal activities, to exercise authority and take coercive measures or to execute criminal penalties and to prevent threats to public security. In addition, the new Law Enforcement Code should apply to all Customs authorities primarily responsible for the supervision of the Union's international trade, thereby contributing to fair and open trade, to the implementation of the external aspects of the internal market, of the common trade policy and of the other common Union policies having a bearing on trade, and to overall supply chain security. Customs authorities shall put in place measures aimed, in particular, at the following:* *(a) protecting the financial interests of the Union and its Member States;* *(b) protecting the Union from unfair and illegal trade while supporting legitimate business activity;* *(c) ensuring the security and safety of the Union and its residents, and the protection of the environment, where appropriate in close cooperation with other authorities; and* *(d) maintaining a proper balance between customs controls and facilitation of legitimate trade.*	Evidence is not available to support the repeal of the Naples II Convention
It is not clear to which extent Articles 39 (CISA) and 46 (CISA) are still applicable and how to use these articles in relation to Article 12 of the SFD.		

3	**New provision, following the definition of the SFD (Art. 12). Subsequent full repeal of Articles 39 (CISA) and 46 (CISA) and Article 12 SFD.** *Definition in Article 12 of the SFD: [To be added]*	The problem addressed through this sub-option is addressed through sub-option no. 1, which is included in PO2 and PO3. This sub-option would only have been relevant if a completely new legislative instrument would have been developed, which is not the case (SFD will be amended).
The distinction between urgent and non-urgent cases provided for in the SFD and the SFD forms to be used (on a voluntary basis) for information exchange is unclear and (unnecessarily) complex		
The forms included in the SFD are time-consuming, labour intensive and not self-explanatory (both the form for the requesting MS and the requested MS). To be able complete the forms efficiently, LEAS need to know what information is available in other MS.		
5	Development and implementation of a functionality within SIENA that resembles Interpol's i24/7 channel, including (1) a hit/not threshold; and (2) in case of a hit, the possibility to request further information	Sub-option merged with option no. 46; discarded as an individual sub-option due to insufficient effectiveness as a measure on its own
9	Development of a "central LEA app" – linked, but not limited to SIENA – that is aligned with MS' national legislation regarding functionalities, access rights etc., which the MS would be free - but not required - to use. The app could provide functionalities such as contact details of and direct messaging to relevant counterparts in other MS, a search functionality for cross-border case requests, a Wiki and glossary, training content (see above), including access to good practices, a Q&A board / discussion forum	While there was clear appetite for such an app, the sub-option was discarded following the discussions in the 2nd technical meeting in May 2021 due to a lack of political feasibility.
10	**Introduction of a requirement to use a "central LEA app" (see non-legislative option),** which: • Enables mobile access; • Facilitates direct information exchange; • Provides LEA Knowledge Management. In principle, the use of the app would be required in all situations referring to the preparation, implementation, and debriefing of cross-border law enforcement activities	While there was clear appetite for such an app, the sub-option was discarded following the discussions in the 2nd technical meeting in May 2021 due to a lack of political feasibility.
The notions of "non-urgent cases" and "other cases" as defined in the SFD forms (annexed to the SFD) for requesting/requested countries are unclear		
11	**Amendment of the two SFD forms for information exchange to remove the category "other cases"**	Discarded due to inadequate expected effectiveness. The SFD forms are repealed under the retained policy options.
12	**Amendment of the two SFD forms for information exchange to provide a definition of non-urgent cases**	Discarded due to inadequate expected effectiveness. The SFD forms are repealed under the retained policy options.
13	Commission guidance on the definition of the term "non-urgent" cases, including the provision of examples of "non-urgent cases"	The term "other cases" will be removed as part of the retained policy options, as this is expected to lead to greater effectiveness, hence leaving no need to clarify non-urgent cases.
The respect for the principle of equivalent access is not always ensured, especially regarding urgent cases		
14	Commission Communication, addressing how to handle information requests. If the authorisation of a judicial authority is required for information requested by another Member State, then the requested law enforcement authority is encouraged to take on the responsibility to ask for this judicial authorization, instead of simply denying the provision of the data requested	Discarded due to inadequate expected effectiveness.

15	**New provision, establishing that if the authorisation of a judicial authority is required for information requested by another Member State, then the requested law enforcement authority shall take on the responsibility to ask for this judicial authorization, instead of simply denying the provision of the data requested**	Discarded due to inadequate expected effectiveness.
The respect for the principle of availability is not always ensured		
16	Commission Communication on how to fill in the SFD form request form. The MS will be encouraged that the request sets out the factual reasons to believe that the relevant information and intelligence is available in another MS and explain the purpose for which the information and intelligence is sought in another MS and the connection between the purpose and the person who is the subject of the information and intelligence in order to avoid "fishing" (by e.g. sending a request for a cross-border check with a copy to all MS)	Discarded due to inadequate expected effectiveness. The SFD forms are repealed under the retained policy options.
17	**Amendment of the SFD request form (and, subsequently, the form in SIENA). The request shall set out factual reasons to believe that the relevant information and intelligence is available in another MS and explain the purpose for which the information and intelligence is sought in another MS and the connection between the purpose and the person who is the subject of the information and intelligence in order to avoid "fishing" (by e.g. sending a request for a cross-border check with a copy to all MS)**	Discarded due to inadequate expected effectiveness. The SFD forms are repealed under the retained policy options. A similar sub-option has been retained, which does not make reference to the SFD form.
The choice of channel for information exchange lies with the Member States, leading to a duplication of requests in some cases		
n/a	n/a	n/a
1.2 Technical driver: Law enforcement authorities have insufficient knowledge of existing mechanisms, skill gaps and outdated IT infrastructure		
National LEAs have limited awareness and knowledge of relevant databases		
It is currently not clear to law enforcement officials what channels should be used for information exchange in what circumstances. Law enforcement officers thus spend a lot of (undue) time to understand what channels should be used in specific cases		
20	Commission Communication encouraging the MS to include training on the channels for information exchange in the basis police training and provide guidance on the channels via Intranet [*Good practice from one MS: Guidelines regarding the channels for information exchange (accessible for staff members of the Integrated Police via the Intranet and is included in the basic police training)*.]	**Discarded as an individual sub-option. Merged with sub-option 34.**
22	**New provision, establishing that the requested Member State should, in those cases when SIENA is not used, reply through the same channel as was used for the request**	Discarded due to inadequate expected effectiveness. PO2 and PO3 include an element according to which SIENA is the preferred or default option, which is expected to achieve higher effectiveness.
Inadequate knowledge by national LEAs' officers of how to use the platforms for law enforcement cooperation available to them		
25	Development and implementation of an awareness raising and training campaign within the EU law enforcement community, e.g. via CEPOL: • Web-based and printed leaflets, including workflows / flow charts; • Short guidance videos in which workflows are explained in illustrative fashion; • Training with mock versions of platforms • A dedicated law enforcement training app that makes content accessible	Discarded due to the expected lack of political feasibility of the training app.
There is limited availability of training for law enforcement staff involved in cross-border information exchanges and cooperation		
Current training is not held on a regular basis and does not take into account the latest changes in the EU law enforcement legislative framework		
n/a	n/a	n/a

The available training is often (only) voluntary		
29	New requirement for the MS to provide a minimum number of hours of training on cross-border law enforcement aspects for officers annually	Discarded, as this would not be limited to those involved in cross-border cases and would be too far-reaching in view of the problems identified.
30	Commission Communication encouraging the MS to establish schemes that provide (non-monetary) incentives for officers to participate in relevant training, e.g.: • Career development; • Gaining expertise and experience; • Development of specialist roles; • Professional networking and connections.	Discarded due to the expected lack of political feasibility in combination with low effectiveness
No specific training is foreseen for newcomers in the International Police Cooperation departments, including in the PCCCs and the SPOCs		
34	**New provision, establishing that the MS shall systemically provide an induction on cross-border law enforcement for newcomers.** [*Good practice from one MS: Common training approach for all police cadets with a view to improve the implementation of existing bilateral agreements, joint curricula in professional English, bilateral cooperation and cross-border regional cooperation, two pilot trainings in border regions or joint trainings/exercises on joint patrols, cross-border surveillance or hot pursuits*]	Discarded, as this would not be limited to those involved in cross-border cases, as it covers all newcomers. Sub-option 34 is determined to respect subsidiarity, while equally addressing the problems.
Language barriers hamper the cross-border exchange of information		
National LEA staff dealing with international matters often report information in "rusty" English		
36	Enhanced provision of English language training addressed at law enforcement officers by CEPOL.	Discarded, as this would not be limited to those involved in cross-border cases and would be too far-reaching in view of the problems identified.
The use of use of rudimentary search tools hampers the adoption of transliteration and "fuzzy logic" search		
The lack of transliteration and fuzzy logic search options in national databases prevents officers to get a full picture about the person they are looking for in the systems through a unique query. This leads to an increased workload which slows down the search process		
40	Commission Communication encouraging the MS to establish of a law enforcement algorithm in national databases / a search engine that enables displaying search results that are similar to what is being queried (proxy results)	Discarded, as this would not be limited to cross-border cases and would be too far-reaching in view of the problems identified.
41	**New provision, establishing that the MS shall establish of a law enforcement algorithm in national databases / a search engine that enables displaying search results that are similar to what is being queried (proxy results)**	Discarded, as this would not be limited to cross-border cases and would be too far-reaching in view of the problems identified and not respect the principle of subsidiarity.
Law enforcement officers on the ground do not always use secure communication means		
n/a	n/a	n/a
1.3 Structural driver: National and regional information hubs set up by law enforcement authorities have different roles, means and capabilities which make their cooperation sub-optimal		
SPOCs/PCCCs do not always play their coordination role and lack resources to face the increasing number of requests		
Existing manuals do not provide clear indications of how SPOCs shall be structured and organised.		

44	Mapping of the different types of law enforcement agencies involved in the national SPOCs (to be shared with other countries) and sharing of national good practices and concrete examples on the types of competences a SPOC should have, as well as tools concerning the establishment and efficient use of a SPOC, provided online	Discarded due to inadequate expected effectiveness. This sub-option would not adequately solve the identified problems
n/a	n/a	n/a
The functioning of the SPOCs, e.g. to promptly respond to the information requests received, is limited		
n/a	n/a	n/a
SPOCs/PCCCs are not always equipped with the necessary information management tools (e.g. a case management system with common dashboard and automatic/semi-automatic data upload and cross-check)		
Lack of interconnectivity between the PCCC and SPOC information systems		
n/a	n/a	n/a
Lack of an efficient case management system		
n/a	n/a	n/a
National law enforcement databases are not connected with each other (e.g. due to technical interoperability)		
51	Commission Communication encouraging the MS to interconnect national law enforcement databases	Discarded, as this would not be limited to cross-border cases and would be too far-reaching in view of the problems identified and not respect the principle of subsidiarity.
Information from (i) different units within the SPOCs and (ii) from the PCCCs (and equivalent structures at the border area) is not always integrated in the SPOC information management system		
Information from (i) different units within the SPOCs and (ii) from the PCCCs (and equivalent structures at the border area) is not always integrated in the SPOC information management system		
n/a	n/a	n/a
Direct and user-friendly access to all relevant EU and international databases and platforms is not the norm in the SPOCs and the PCCCs		
SPOCS and PCCCs lack access to all relevant EU and international databases and platforms		
	[Covered above in sub-options 43 and 44]	
The specific national stakeholders entitled to access and use EU and international databases and platforms vary between the Member States		
In some countries regional and local law enforcement authorities (especially customs) cannot access EIS, SIS, SIENA, VIS, Interpol's databases and other international law enforcement information exchange channels directly, due to its centralised access rights on national level		
54	Commission Communication encouraging the MS to ensure that also regional and local law enforcement authorities, including customs, have access to EIS, SIS, SIENA, VIS and Interpol's databases	Discarded due to inadequate expected efficiency and political feasibility to be adequately implemented voluntarily by the Member States.

ANNEX 8: AD HOC WORKSHOPS (SUMMARIES)

Ad hoc workshop of 24 March 2021 *[As drafted by the independent contractor]*

Summary of the discussions[332]

Attendees

- For the European Commission:
  - o DG HOME: Robertus Rozenburg (HOME D.1), Cecilia-Joanna Verkleij (HOME D.1), Patrick Hamon (HOME D.1), Antoine Billard (HOME D.1), Mickael Roudaut (HOME D.1), Aleksandra Tukisa (HOME D.1), Florence Fensie (HOME D.1), Adrianna Miekina (HOME A.4), Massimiliano Minì (HOME D.5)
  - o DG JUST: Eleni Chronopoulou (JUST C.3)
- For the Council of the European Union: Jarek Lotarski (Legal Service), Radovan Schida (General Secretariat)
- For the Contractor: Katarina Bartz, Francesca Migliavacca, Emma Disley, Ilia Gaglio, Florian Linz, Sara Filippo
- For countries: national representatives from Law Enforcement Authorities of all EU Member States and Schengen associated countries (except Iceland and Liechtenstein)

Acronyms

CISA	Convention Implementing the Schengen Agreement
CMS	Case Management System European Criminal Records
ECRIS	Information System Europol Information System
EIS	European Travel Information and Authorisation System
ETIAS	European car and driving licence information system
EUCARIS	Internal Security Fund
ISF	National Football Information Point
NFIP	Police and Customs Cooperation Centres
PCCCs	Swedish Framework Decision
SFD	Secure Information Exchange Network Application
SIENA	Schengen Information System
SIS (II)	Single Point of Contact
SPOCs	Visa Information System
VIS	

[332] The representative from the Netherlands expressed a reserve clause on conclusions presented in this document.

Opening remarks from the European Commission

- **Security has been a priority for the European Commission** (hereafter the Commission) **from its very beginning**. A lot has already been done over the past years, like for instance: the revision of the Schengen Border Code, the revision of the Schengen Information System (SIS II) and the very recently adopted interoperability regulations.[333] However, operational cross-border cooperation between Law Enforcement authorities inside the EU continues to face challenges, and there is still room for further improvement. The findings of the Schengen evaluations in the field of police cooperation, and recent Council analytical papers, further confirm this.
- The EU legal framework is highly fragmented and somewhat outdated. The bedrock for law enforcement cooperation has been and remains the 1990 Convention Implementing the Schengen Agreement (CISA). This has been complemented by the Prüm Decisions,[334] widening the scope for operational cooperation also to public order and safety matters, and by some sectorial Council Decisions such as the one on Liaison officers for football matches. Member States and Schengen Associated Countries have built on this foundation to further develop their cooperation through bi/tri/multi-lateral agreements. While these agreements may be subject to regular renegotiations by participating countries, the EU legal framework has not undergone a systematic and thorough update. Subsequently, the EU and bi/multilateral provisions are found to have drifted apart one from the other to various degree.
- **Significant principles of cross-border cooperation have been set out in nonbinding Council guidance** such as for Single Point of Contact (SPOCs) and Police and Customs Cooperation Centres (PCCCs), and at times these non-binding provisions are found to be lacking the necessary enforcement powers.
- There is a need for European action at the external borders and within the EU. Even though each Member State is responsible for fighting criminal threats on its own territory, their increasing cross-border dimension calls now, perhaps more than ever, the need for EU action. Therefore, the Commission announced a legal initiative by the end of the year to modernise existing intra-EU Law Enforcement cooperation. The study that EY and RAND Europe are undertaking will provide evidence to the Commission to inform future decisions in this regard and aim, among others, to answer questions like: is the access to information by SPOCs or PCCCs fit for purpose? What do we need to better address security risks during mass events? Do we need a significant step-up in the collective fight against cross-border crime? Answering these questions is part of a wider consultation process composed of surveys, interviews and case studies each covering a different angle of the subject matter. The Technical workshop is part of the consultation process and aims to better understand what works, what does not and what could be done in order to improve the current situation. A second workshop will be held in May to discuss about possible options for the future.

Presentation of the study and preliminary findings

- **There is not a clear-cut distinction between law enforcement authorities entitled to use the Swedish Framework Decision[335] (SFD) and those entitled to use the Naples II**

[333] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration.

[334] The Prüm Decisions refer to Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA.

[335] 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.
The Annex IV of Council *Guidelines on the implementation of Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the*

Convention. In ES, the national legislation which transposes the SFD states that both Police and Customs can implement measures included in the SFD and in the Naples II. In IT, the Naples II Convention can be implemented only by Customs authorities and law enforcement authorities with Customs duties. When ratifying the Convention, Member States have defined the authorities that could implement it. Even though Customs usually refer to the Naples II Convention and Police to the SFD, this clear distinction does not apply to all countries.

- It would be important to understand if the issues identified are affecting a significant proportion of cross-border cases or just a minority of them . The Contractor explained that the study will try to quantify where possible the scale of the issues identified, and stressed that the feedback provided by stakeholders will be key to this end. It has also been underlined the existence of objective limitations in retrieving data about the identified issues. There are no statistics on the number of cases not initiated or dismissed because of difficulties in the cooperation.

Presentation of the preliminary results of the analysis of the problems related to cross-border law enforcement cooperation

- The Contractor illustrated the core problem identified, the related drivers and issues.

Access to and exchange of information is sub-optimal

- Several participants have experienced issues relating to the access to and exchange of information with other Member States.
- Reported issues include:
    - o Duplication of requests via different channels;
    - o Requests sent before the needed checks in the relevant EU and international databases;
    - o Inappropriate choice of the channel to exchange information;
    - o The existence of a chain of requests when a country needs to send a request for information to another not neighbouring country. A country can send a request to another country based on the SFD but the receiving country may not accept it as the SFD has not been implemented in the same way;
    - o No access to the Europol Information System (EIS) for the Schengen Associated Countries since they are not EU Member States;
    - o Police authorities might have limited access to Customs' databases and vice versa due to secrecy provisions (e.g. when contacting a foreign Customs authority to request criminal records of a given suspect, in some countries Customs cannot proceed because they do not have access to police databases).

Other problems

- Overall, the problems and issues identified by the study reflect the current situation with few participants that highlighted the existence of additional issues such as:
    - o Existence of different traditions in the national administrative systems. For instance, some Member States have a complex administrative system, with a number of agencies and institutions with different responsibilities. Such complexity at the national level might create difficulties during cross-border operations.

European Union (doc. 9512/1/10 REV1, 17 December 2010), list all LEAs that declared themselves competent under the SFD. This includes a number of customs authorities.

Break-out session 1 - Access to and exchange of information

What are the issues at stake? Are there practical examples/cases that can illustrate the issues identified?

- The **main issues** concerning the access to and exchange of information relate to:
  - o **Limited awareness and knowledge of relevant EU and/or national databases and platforms for information exchange**. There are still difficulties in the choice of the most appropriate communication channels, and this creates additional workload for the staff working in the SPOC. Concretely this reflects in:
    - Duplication of requests in different channels such as the i24/7, the Interpol information exchange system, and the Secure Information Exchange Network Application by Europol (SIENA);
    - Use of inappropriate channels (e.g. request from one SIS II country to another to locate a person is sent via i24/7);
    - Police-to-police requests instead of other equally effective mechanisms, such as the European car and driving licence information system (EUCARIS), the European Criminal Records Information System (ECRIS) and the Visa Information System (VIS).
  - o **Limited cross-matching of national law enforcement databases with EU databases**. In view of the increasing interoperability of EU databases in the future, it is important to improve information exchange between Schengen Associated Countries and Europol. Moreover, another practical obstacle is represented by the fact that Member States, which are full members of Europol, can restrict the access to their national data in two ways: they could apply high classification levels (such as "EU restricted" or more) on the information or they can require Europol to ask for their consent prior to sharing the information. In the daily practice, this means that countries which are partners but not full members of Europol (Schengen Associated Countries and Denmark) often experience restrictions in the access to data and information. Even if there is currently a discussion between Europol Member States about how to reform Europol's regulation, Schengen Associated Countries have not been involved in these negotiations. It would be important to amend the regulation in order to acknowledge the close relationship that Schengen Associated Countries have with EU Member States, thus enabling their effective participation within Europol. In this way, it would be possible to distinguish between Member States, Schengen Associated Countries and general Third Countries;
  - **o** Limited access to EU and/or national databases relevant to law enforcement cooperation;
  - o Limited availability of secured information channels as well as limited mobile access to law enforcement databases;
  - o Fragmentation of the EU framework for cross-border cooperation. There are around 31 binding and 18 non-binding measures concerning international Law Enforcement cooperation. This level of fragmentation makes it difficult for practitioners to have a holistic picture of the available tools;
  - o Mixed opinions on the existence of uncertainties in the exchange of information created by the different scope of application of the SFD and the CISA.
  - **o** There are some problems in the implementation of the SFD:
    - Unclear definition of time limits (urgent, non-urgent and other cases);
    - The form is too cumbersome;
    - The form is not used;
    - Principle of availability is not respected (notably in police-judicial cooperation context). It could happen that local police officers or departments are not aware of EU regulation and of the principle of

availability. For instance, in a given Member State, there could be a SPOC and several state/local police forces which sometimes are not aware of the functioning of the system;

- Obstacles linked to different national transposition measures. The provisions of the SFD are transposed by all Member States but differences in the national transposition can affect the way requests for information coming from other Member States are managed;
- Cases of "fishing". Examples of one Member State sending an urgent request to all Member States under the SFD without any indication of the country they are seeking for an answer. This creates unnecessary workload for the SPOCs;
- Requests for additional information. When sending a request to another Member State, there are sometimes issues as the counterpart may request additional documentation (e.g. a European Investigation Order or Mutual Legal Assistance request). Member States can share information according to the SFD but in many cases they prefer to stay on the safe side and to request for additional documentation;

o No issues have been raised regarding the requirements set in the Prüm Decisions on the supply of information in order to prevent terrorist offences. Usually information concerning terrorist offences is exchanged through specific information channels and mechanisms which are identified based on available guidelines and operational instructions (e.g. Draft SPOC Guidelines for cross-border law enforcement information exchange, 6721/14, and Proposal for a Practical Advisor for Law Enforcement Information Exchange, 6243/18), rather than pursuant to the Prüm Decisions.

In light of likely future security, technological, social, policy and economic developments, how would the driver and the related issues evolve in case no further EU action is taken?

- Current issues related to the access to and exchange of information will **likely become more relevant** in the next 5-10 years in case no further EU action is taken.
- **Technological, security and policy developments** will significantly affect the evolution of the existing issues. Among the examples reported:
  - o The use of artificial intelligence is likely to have a strong influence on criminals and police modus operandi;
  - o The use of cryptocurrencies poses new challenges to law enforcement, especially regarding handling these assets once they have been seized;
  - o The increasing volume of data and information to be stored (e.g. means of proof for court) is challenging the current capacity of the databases of law enforcement authorities.

Is there a need for EU intervention to address this driver and the related issues?

- **There is a need for EU intervention** to address the issues related to the access to and the exchange of information.
- The EU intervention should focus on:
  - o The interconnection and streamlining of available systems for the exchange of information. Member States may currently adopt different communication channels since the EU measures in this regard are not binding. Different Member States may adopt distinct communication channels depending on the crime areas. Some databases can be accessed only when performing a research in a specific crime area. This generates some limitations and might be a point of attention. According to the Prüm Decisions, in order for one Member State to be able to undertake direct

exchanges with other Member States, 26 bilateral interfaces are required. However, it is not required to establish a connection with all Member States and therefore not all Member States are connected and share DNA, fingerprints and other kind of data;

- o The overall consistency of the EU legal framework;
- o Awareness and capacity of national law enforcement authorities.

What types of policy measures could be considered to address the issues included under this driver?

- A clearer definition and regulation of the SPOCs through binding instruments could help Member States to allocate the resources needed for integrating the different channels in coordinated structures.
- Mixed views on the opportunity for the Commission to indicate a preferred communication channel (e.g. SIENA) to be used by all countries to exchange certain types of information with two participants considering this a good way to simplify cross-border cooperation and one in favour of leaving room to national law enforcement authorities to decide. Without suggesting the Commission to indicate a preferred communication channel, it has also been suggested to define harmonised criteria on the choice of the channels in order to avoid duplications;
- Promotion of a common business requirements for the Case Management System (CMS) among SPOCs;
- Ensure the presence of a SPOCs in all countries and ensure they can access all national and international databases;
- Organisation of specific trainings at the national level and through CEPOL webinars.

Plenary discussion on the outcomes of the break-out sessions

What are the issues at stake?

Main findings

1. **Access to and exchange of information**
   - Key issues include limited awareness of and access to relevant EU and national databases as well as limited interoperability of national systems;
   - Some issues specifically relate to the implementation of the SFD, notably the form included within is too cumbersome and the definition of urgency/timeframe is not clear;

Police-to-police requests instead of other equally effective mechanisms (such as EUCARIS, ECRIS, VIS etc).

The main findings discussed during the break-out sessions have been confirmed and no comments were raised.

Are there practical examples/cases that can illustrate the issues identified?

Main findings

1. **Access to and exchange of information**
   - Schengen Associated Countries do not have direct access to Europol's databases;
   - Unnecessary transmission of information through different channels (duplication or requests through I-24/7 and SIENA). Use of inappropriate channel (request from one SIS II country to another to locate a person is sent via I-24/7);
   - Requirements for the SPOC CMS (interconnection with different channels, national and EU databases, automation of checks).

No additional examples have been provided.

In light of likely future security, technological, social, policy and economic developments, how would the driver and the related issues evolve in case no further EU action is taken?

Main findings

1. **Access to and exchange of information**
   - Current problems will become more relevant in case no further EU action is taken;
   - The worsening of current problems is mainly attributed to new and evolving technological developments likely to affect the access to and exchange of information.

Is there a need for EU intervention to address this driver and the related issues?

Main findings

1. **Access to and exchange of information**
   - Current problems need to be addressed at the EU level.

The main findings discussed during the break-out sessions have been confirmed and no comments were raised.

What types of policy measures could be considered to address the issues included under this driver?

Main findings

1. **Access to and exchange of information**
   - In order to improve access to and information exchange, the EU intervention shall ensure full interconnection and streamlining of available systems for the exchange of information, the overall consistency of the EU legal framework, and the full awareness and capacity of national law enforcement authorities. To a lesser extent, it should also ensure the integration of modern requirements into fundamental rights and data protection rules;

The main findings discussed during the break-out sessions have been confirmed and no major comments were raised except for the following:

- With regard to the possibility to extend the scope of surveillance activities to additional crime areas such as tobacco smuggling, it would be better and more important to extend the competences of certain law enforcement authorities instead of broadening the scope of a single investigative tool.

Concluding remarks from the Commission

- The meeting achieved its intended goal to define the issues faced today by law enforcement authorities.
- The consultation activities for the study are still ongoing and all participants are invited to take part, especially to the online survey.
- The Contractor will submit the study interim report on mid-April. This will include the analysis of the problem and then the study will focus on the possible future policy options.
- Another workshop will be organised in May to discuss the impacts of the possible policy options.

Ad hoc workshop of 25 May 2021 *[As drafted by the independent contractor]*

Summary of the discussions[336]

Attendees

On behalf of the European Commission: Adrian Perez-Martinez, Aleksandra Tukisa, Anna Moscibroda, Antoine Billard, Eleni Chronopoulou, Florence Fensie, Jesper van Putten, Jolande Prinssen, Julian Siegl, Mario Cuschieri, Massimiliano Mini, Mickael Roudaut, Oana Hidveghi, Olivier Micol, Patrick Hamon, Pestelli Vanni, Sandra Moeller, Robertus Rozenburg.

On behalf of the countries: National representatives from Law Enforcement Authorities of all EU Member States and Schengen associated countries (except Iceland and Liechtenstein).

Acronyms

CISA	Convention Implementing the Schengen Agreement
CMS	Case Management System
LEA	Law Enforcement Authority
MS	Member State
PCCCs	Police and Customs Cooperation Centres
SFD	Swedish Framework Decision
SIENA	Secure Information Exchange Network Application
SIS (II)	Schengen Information System
SOC	Serious and Organized Crime
SPOCs	Single Points of Contact
UMF	Universal Message Format

Welcome and presentation of the agenda

The contractor welcomed all participants and thanked them for their participation. In the following, the contractor introduced the housekeeping rules for the workshop, including the relevant technical functionalities of the tools to be used and the communication rules. As a closing to this introduction, all participants were invited and highly encouraged to be active and involved in the discussions ahead.

As a next point, Slido (as well as its relevant functionalities) was introduced as the tool for launching poll questions (by emphasising that the choices uploaded by the participants will not be statistically analysed on an individual level). Again, the contractor emphasised the importance of interaction for the policy options to address current problems efficiently and effectively.

Subsequently, the collection of national stakeholder's points of view on the possible EU measures to address current problems affecting cross-border law enforcement cooperation as well as the discussion of likely impacts of these measures were presented as the overall objective of the workshop.

As a last point of the welcoming, the contractor underlined the fact that law enforcement authorities (LEA) of all member states (MS) and Schengen associated are represented in the workshop, which was jointly organised by Rand, EY, as well as the Commission.

[336] The representative from the Netherlands expressed a reserve clause on conclusions presented in this document.

Opening remarks by the Commission

The Commission welcomed all meeting participants and introduced the group of participants in further detailing, covering 200 experts from the police, customs, SPOCS, PCCCs, investigators, authorities, specialists in joint cooperation and the national representatives from MSs and Schengen associated countries.
The Commission referred back to the workshop two months ago (24 March) and pointed out the focus of this workshop: to discuss what could be improved in cross-border law enforcement cooperation and possible options that could best address the issues and facilitate the daily life of end-users, as well as the likely impacts and the efficiency and effectiveness of the options. In addition, the (political) feasibility should be part of the discussion as well.

In a next step, the Commission representative referred to the existing basis of this study, covering 37 EU measures complemented by 75 mutual agreements, as well as to the fact that each MS is responsible for its own country security and fighting against terrorism within the EU. At the same time, the Commission stressed the importance of facilitating the exchange of information through SPOCs and PCCCs in order to better address cross-border crime.

For closing the opening remark, the Commission emphasised its listening mode for the workshop due to the fact that the study is conducted independently by EY and RAND.

Presentation of the study and (preliminary) findings
After the presentation of the study as well as the preliminary findings, the participants of the meeting were given the possibility to address their questions in a **Q&A**. The following points were mentioned/discussed in this context:

The problems identified in the problem definition are considered as relevant by the participants. However, most of these problems are already known to be such, not only in the EU, and shared by many stakeholders. The fact that there have already been developed a lot of (operational) practices to address these problems should not be neglected. The improvements aimed at with the policy options presented are relevant and considered as positive. They should, however, also take into account what is already there as potential solutions. This argument was supported by more than one participant. In this context, one participant added that some options are considered to be constitute a positive change, such as the access to SIENA for all main LEAs, but their implementation might create internal challenges/obstacles in the MS.

Regarding the policy options, one participant is asking for more detail. This request could already be addressed during this meeting, when the policy options and respective measures were presented in further detail during the breakout sessions.

The Commission answered the wish of two participants to get access to the interim report, confirming that the final report will be accessible for all participants of the meeting on the DG HOME website.

In this regard, more than one participant underlined the importance of providing quantitative evidence, both for the problems as well as the policy options identified. The Commission answered this point by assuring that the final report will have a solid basis in this regard.

One of the participants referred to the material scope of the study, asking how public order is of interest for police cooperation. In the participant's view, public order is an administrative liability while public safety refers to the security of citizens which falls into the scope of police liability. The Commission addressed this question by quoting the relevant EU article as a reference on the EU's

definition on public order and public safety (Art. 17 (1) of Council Decision 2008/615/JHA (Prüm Decision).

Breakout sessions

During the breakout sessions, the participants discussed the measures presented on the respective slides of the Powerpoint presentation by the contractor as well as their likely impacts. In the following, the discussion points will be summarised and structured according to the main strengths and weaknesses of the measures presented as well as to additional key comments raised during the discussion.

Breakout session 1 – Access to and exchange of necessary information

Main outcome of the breakout session

Set-up and competences of the SPOC and PCCCs

The **main strengths of the measures presented** concerning the set up and competences of the SPOCs and PCCCs are:

- Time savings: A definition of common competences of the SPOC and the PCCCs would, in the view of the participants lead to time savings when requesting/submitting information (e.g. due to facilitated workflows and centralised communication by using the SPOC)
- Clarity of competences, responsibilities and clear rules
- Increased monitoring of possibilities for the SPOCs concerning the cases
- The access to national and international databases and platforms for SPOCs and PCCCs is considered as highly relevant
- High relevance of possibility to ask for judicial authority support 24/7
- Common (minimum) standards of a SPOC/PCCC Case Management System as well as the functionality of cross-checking would facilitate workflow, both nationally and internationally

The **main weaknesses of the measures** concerning the set up and competences of the SPOCs and PCCCs are:

- The feasibility of some of the measures related to PCCCs were questioned by some participants depending on the national set up and the overall role of PCCCs, both varying significantly between MS
- Following the point above, some participants stressed the point of structural differences of SPOCs, PCCCs and judicial authorisation between MS. A fact that might be, at times, hampering the smooth and efficient cross-border cooperation. It may also touch upon national competences
- High importance of actual data availability for appropriate functioning of the databases, platforms and CMS

Additional key comments:

- The participants suggested to consider the need for further coordination at the European level between the SPOCs, the PCCCs and other law enforcement units (e.g. liaison officers)
- Additional measures should also be considered to improve the use of resources at the national level allocated to the SPOCs. For instance, the SPOC shall be sufficiently staffed and trained to perform their tasks effectively, supported by an IT-system that enables efficient processes and swift responses

- Bilateral agreements depend on a common understanding and it might be difficult to reach the same kind of trust on a multilateral / EU level.
- Participants raised the point of automated processes, which is highly needed, due to the increasing volume of information requested, exchanged and stored.
- Appropriate EU funding for establishing a SPOC workflow system is considered to be helpful
- SPOC/PCCC Case Management Systems in the MS

The **main strengths of the measures presented** concerning the SPOC/PCCC Case Management Systems in the MS are:

- Intelligent tool including statistical data would facilitate workflow, both within the SPOC/PCCCs as well as between them
- Minimum essential requirements for CMS for all MS
- Time savings (e.g. speeding up the management of requests), access to information in real time
- Better data quality and data quality control → improved quality of work
- Avoidance of duplications
- Establishment and enforcement of a common/similar workflow in different MS
- The added value of this measure is considered to be relatively large

The **main weaknesses of the measures presented** concerning the SPOC/PCCC Case Management Systems in the MS are:

- Costs for MS in developing the CMS
- Feasibility linked to national specificities (the integration of specific solution within the national systems might be politically and technically challenging, depending on the current individual solution used in the MS)

Additional key comments:

- One central national workflow/CMS for all information exchanges
- Automation of data cross-check
- Universal message format (UMF) to be used
- Data protection considerations
- Access rights by different units need to be defined
- Access rights to EU databases need to be defined
- Interoperability between PCCCs' CMS and the one of the SPOCs
- Access to technical support
- Information exchange via SIENA and other communication channels

The **main strengths of the measures presented** concerning the information exchange via SIENA and other communication channels are:

- Time savings
- Increased clarity on which communication channel should be used when (currently existing confusing in this regard leads to uncertainties and potentially double work)
- Increased level of security

The **main weakness of the measures presented** concerning the information exchange via SIENA and other communication channels is:

- Complexity of access rights

Additional key comments:

- Necessary to consider further the use of other communication channels and the criteria for the use of the channels/matrix
- Need to clarify the rules for the usage of SIENA for intra-EU communication
- Use of Interpol when third countries are involved
- SIENA is currently not monitored 24/7 by all MS, as it should be in view of the participants
- Reference to the handling codes
- Some of the measures proposed for SIENA are already in place or upcoming (and thereby to be discarded as part of this legal proposal)
- Use of secure communication means
- As a general comment made by the participants, the use of secure communication means is a horizontal issue that needs to be addressed across all policy options
- The idea of a LEAs app was considered as interesting by some participants
- Training activities

The **main strengths of the measures presented** concerning training activities are:

- Additional material provided by CEPOL
- It is crucial for officials to be able to translate the content of trainings into practice. Therefore, the training should not be too complex and burdensome. An enabler in this regard could be the introduction of more harmonised legal requirements and measures at the EU and national levels.

The **main weakness of the measures presented** concerning training activities are:

- Training should not be too general but targeted, both in terms of the form and the content (e.g. efficient use of SIENA)
- Limited availability of time for the officers on the ground

Additional key comments:

- There is a need to consider the specificities of national situations and needs of specific LEAs
- The focus of the training should be on practical needs, due to restricted time of officers (concentrate on the most important)
- Agreement on the need for language trainings (i.e. English) in order to communicate with other SPOCs
- There should be both, training at EU level (CEPOL) and at national level (with leading role of SPOC) for international cooperation

Comments by country representatives

LV agrees with the proposal. It is extremely important to define minimum essential mandatory requirements for the SPOC set up, position within the country, presence of judicial authority as well as essential requirements to the case management system used by SPOCs and relevant access to EU/international/national databases.
BE indicates the measure is comprehensive, one point to be specified is the one about "be informed about or be responsible", in their experience when cooperating with other countries there are strong barriers between SPOCs, PCCCs and liaison officers, that do not share databases nor CMS, are not aware of what the others do, there are no clear rules on which of the three is responsible for what. As a consequence, if you send a request to a PCCC they will provide an answer but may not be aware that a previous investigation on the topic was conducted by the SPOC, with previous exchanges of information. So there should be coordination and they should work together as a one flow of information exchange.

CZ confirms that also other units deal with international cooperation, in particular specialised units such as counter-terrorism units, with their own ways of communication, as well as the customs, and all this information should be kept together. Also the lack of resources is a big issue, to deal with all the requests the SPOC would need a lot of resources, or would not be able to manage them, and this is an issue for all the countries, without qualified people, technologies, such as an integrated workflow, the issues in international cooperation are not manageable. Also training is important, end-users should be trained by the SPOC on how to tackle issues in international cooperation, as its officers should have the best knowledge and should share it, to make end-users more aware of the possibilities of cooperation.
ES mentions that the SPOC should integrate all the relevant LEAS in the country, as per the guidelines. Moreover, the SPOC must channel the requests for all stakeholders respecting the national and international mandates as well, defining sharply the contact points, without other alternative and irregular means of information exchange.
BG thinks that SPOCs should also be responsible for bilateral/regional cooperation, together with PCCCs. The minimum requirements for SPOC structure are mentioned in the SPOC Guidelines for international law enforcement information exchange in the framework of the DAPIX Working Group (nowadays IXIM Working Party). Agrees that SPOCs should also have a main role in training police officers, for example on which channels should be used for international cooperation.
DE notes that some of these points are not applicable to Germany for its constitutional background as federal republic, because they have 16 police forces (one for each Länder) and the Federal Police, and an integrated CMS and access to all databases are limited, so the measures should be adaptable by MS to their own national legislation and constitution. Moreover, merging PCCCs and SPOC in one structure would limit the capabilities of PCCCs.
BE affirms that it was not pleading for merging PCCCs and SPOCs, but to make sure that their respective workflows are coordinated and integrated. So that SPOC knows what PCCCs and LOs do and vice versa, without duplications and have parallel information exchanges. Being informed about each other's actions is the minimum, ideally there should be some common CMS to automatically see this. But each should keep their competencies and specialty. On the question of whether the SPOC should be responsible for, the organisational level is an internal issue of the MS, for example in Belgium the SPOC, LOs and PCCCs are part of the same directorate, but the LOs are independent while the PCCCs are part of the SPOC.
NL indicates that it is not clear which databases the Commission has in mind for the point on full access EU LE databases – and to what extent there will be access to these databases.
LU indicates that the problem is always national implementation and national interpretation.
LV agrees with the colleagues regarding national implementation and interpretation. The national implementation of different guidelines creates sort of misunderstanding, misleading on the use of communication channels, info exchange etc. And it is hard to allocate adequate resources, organise training taking into account the current workload and a huge amount of work to be done manually.
DE points out that an additional core issue - already in context of the set-up of SPOCs - is automation. The increasing amount of international data exchange (in comparison with limited human resources in the SPOCs) shows a clear need to establish automated processes.
LV indicates that the SPOC shall be the main coordinator for international info exchange.
LT proposes that in order not to duplicate information between SPOC and PCCC, there should be one common management system which allows you to cross check info.
CZ indicates that SPOCs must have an overview and that it is probably not possible SPOCs manage every request, but must know about it. So the request may be done by PCCC, but information must be available - both to SPOC and all PCCCs. This avoids duplication and loss of information. Common systems solve this. On the point of having a judicial authority available 24/7, also this may be related to internal organisation of MS, but it is important to emphasise the importance of the availability of judicial measures for the SPOCs, for example in CZ some measures allow for centralisation and some others, such as arrest, not, as the legal base make it not possible to

centralise decision in one judge or public prosecutor sitting in the SPOC, so the solution should allow to find rapidly the right one. So the solution is to make judicial support available.
DE clarifies that having clear rules would support officers under pressure in choosing the right channel to ask questions to international partners, and make it quicker to receive an answer, as it would not be needed to transfer the question to the right office.
CH mentions that access to most relevant databases at one spot reduces the time.
DK suggests that making data available for all Member States is also important. There are databases that should be feed by MS but are not. In the SIENA system, many MS sent requests to everybody, even for minor cases, while with this base of available data they could be more specific in choosing the MS and not contact everybody if not necessary, making time savings. So important to share data with Europol and in the EIS. There is a Council Decision about the information system saying that MS should share more information, so if data is available, they could save some time in SPOCs.
BG indicates that if the SPOC officers (or even LE officers) have direct access to the relevant EU databases (SIS, ECRIS, EUCARIS, future Prüm revision) the information exchange will speed up and there are recommended Do's and Don'ts in the Practical Advisor to the Manual on Law Enforcement Information Exchange.
ES is concerned about the incentives for PCCCs to use these services that are normally centralised. PCCCs should be coordinated by the SPOC, using for example the same CMS.
CZ indicates that Eucaris is not an Interpol database. Any police officer has access to SIS, so no need to mention as special with PCCC. Another point is Europol database - there are restricted access and not for PCCC, Concerning Eucaris - in our circumstances again all officers have access. Most crucial with PCCC is to have safe channel to exchange the information and to share and be co-ordinated with SPOC. PCCC is in fact one of the channel.
BG indicates that concerning the PCCC - their competences, information exchange channel, access to the databases depends on the bilateral/trilateral agreement among the MS
CZ mentions that SPOCs have a specific role, e.g. for Europol databases, which is not for all officers. Or due to expert knowledge about the SIS or Interpol databases. Not to make queries, but to explain the outcome. Moreover, the SPOC operates 24/7. This is must already. SPOC works 24/7 in all countries. The question is whether all authorities or channels are covered.
CH raises the question if there is any SPOC that does not operate 24/7. **ES** confirms that **ES** offers a 24/7 service. **BG** agrees that concerning the 24/7 operating of SPOC it should be taken into account that not all ENU are 24/7 operational because there is no obligation in the current Europol regulation.
SI mention that duplication can be avoided but there would be costs for MS to implement CMS.
NL points to potential privacy issues.
ES indicates that there could be information from three different sources mixed, with different kinds of protections, so it would be important to check this is compliant with relevant legislation.
DE suggests there could be issues with access rights to different services represented in PCCCs.
BE mentions that there is a technical solution to the fact that different services are in PCCCs, certain aspects and certain information in the CMS can be made not accessible to everybody, so different components can access only their part. Moreover, the universal message format should be taken into account, there is project at EU level on this, the information exchanged between MS should be structured in a certain way to make the CMS work well, helping to deal with the messages.
CZ adds that 1) CMS should have automatic functions (e.g. automatic query on incoming request in the databases), 2) CMS shall be integrated with all channels, 3) CMS should be common to SPOCs and PCCCs to ensure that there is a sharing of information and avoidance of duplications, 4) there should be 24/7 technical support, 5) there should be also statistical tools.
ES confirms that the structure of the messages is provided by SIS forms, SIENA and Interpol messages are free-form, and hard to pattern, but solutions as UMF can be used for entities exchange.
BG confirms that parts of proposed measures for SIENA are already in place.

SE indicates that the Covid-19 pandemic has clarified the need for one or more tools to secure virtual meetings for customs and other law enforcement authorities with the ability to join the tool/s, regardless of their location nationally. As we understand it Europol has a task to forward a proposal for solutions (building on SIENA). SE Customs use SIENA very frequently.
SI mentions that SIENA is developing all the time. The problem which we see is that it is not monitored 24/7 in all MS.
ES think the bulk of the design of those tool falls into SPOCs, as long as SIENA web services APIs are provided by Europol. Maybe redesigning the SIENA interface is a tall task ...
CZ explains that SIENA is a complex tool, and its application as a secure communication channel could be questioned. So the focus should be only on one solution, but on the need for police cooperation to have a secure channel of communication. SPOCs use secure channels but police officers use whatever they find. SIENA have different meanings, it is a full application, and it is restricted so could not be linked easily with other systems for all police officers to use it. The secure communication between PCCCs is done also via sTESTA which is probably more general - only the "cable" not the full "app" as it is SIENA. Major point is to make clear rules which channel is used and bring structure to those not structured so far (as SIRENE has complete structured messages e.g.).
NL indicates that a crucial aspect is that we still wish to exchange information through for example our liaison officers throughout Europe. And we should not forget the 24/7 channel from the Budapest Convention. We do however have the opinion that information exchange over Europol should prevail Interpol.
DE explains that PCCCs have to use specific secure channels, and not everybody is aware of it.
BG indicates that the general rules for the choice of the channel, to comply with the mandates of Europol, Interpol, SIS and all other channels for cooperation and information exchange should be taken into account. SIENA is very user friendly for information exchange in English, the default language. As far as she knows, there are a lot of initiative in the SIENA roadmap that will simplify information exchange between LEAs, but it could not be default channel for cooperation, Europol has operational agreements with third countries, so SIENA can be used also with them, but the choice is on the MS.
ES explains that SIENA is more than the interface, and we can exploit the channel and its advantages without using the interface. The structure of the messages can be provided technically in the CMS, via templates, SIS style. Good starting point is devising a catalogue of usual communications amongst MS, and normalise those more frequent.
CZ confirms the need to harmonise the use of channels in MS. Which does not mean prioritise just one, but making clear rules of use for all, to which channel should be used and for what. Technical solutions then can be found. Also the speed/way of reply is now different for channels and this shall be also considered. We need harmonisation and common standards, which would help.
FR responds that due to an intensive exchange of information with neighbouring third countries (Maghreb), they would not recommend to establish SIENA as a default channel since we need to copy EU MS in these exchange via INTERPOL, or they will not see the exchanges happening with third countries.
ES responds that for FR, that could be solved if the CMS is able to integrate communications from different sources in the same case files.
BE explains that for FR, the rule could be that SIENA is preferred channel for purely intra-EU communication, but that once a third country is involved, Interpol becomes the preferred channel?
ES explains that for CZ the problem is that sometimes the channel is identified with a certain unit, with different resources and backlogs. Integration of the channels under same structures could relieve the load.
CZ responds that to the recent point on secure tool - this definitely covers the needs of officers for tool for secure individual communication. However there is question how to ensure, that with this secure bilateral communication between individual officers we do not miss some information which otherwise will go via e.g. SPOC.

CZ points out that there are many interesting parts from different MS and agencies and suggests that all best practices could be put together in one. Furthermore, CZ points to the topic of complex training. At present, there are mostly specialised trainings which often serve as the only channel or are the only training available in a specific area. CZ explains that there is sometimes even competition for certain tools or channels which is confusing for police officers in the streets. Police officers on the ground need solutions and do not care how it will be done.
BG asks that there should be trainings both on EU level (CEPOL) and on national level (with leading role of SPOC) for international cooperation
BE confirms that they are in favour of EU trainings provided by CEPOL or others, it is lacking at the moment. But the national implementation of EU legislation is always different, so we have to respect these differences, there should not be a unique handbook for trainings, but more targeted parts and courses, for instance on the use of SIENA, that could be integrated in the national framework.
CZ explains that it is good to have a framework at EU level that is implemented than at national level. There should be differentiated trainings for officers depending on their role, as there are different needs, those in the streets receive a lot of information and trainings and thus trainings should focus on the practical needs of the officers, trying to keep it simple. Also helping would be an overall harmonisation of cooperation rules, a common framework would make also training simpler. The use of English should be necessary knowledge. Thus the training must be different for different groups and focus must be very practical.
BG indicates that there should be dedicated trainings both for law enforcement authorities and for the SPOC officers (currently there is ATHENA 2 project) for all tools/legal acts/channels for LE cooperation.
CH points to different functions with different needs. Not all law enforcement officers work internationally or with other languages. Some work with their neighbouring countries who speak the same language.
CZ indicates that police cooperation is necessary and this needs to be made clear to all officers, not to care only on their district, create an atmosphere and feeling going beyond technical and legal solutions to make it work.

Second plenary session
Following the breakout sessions, a summary of the results of each breakout session was presented and put to discussion by the contractor in the plenary (Please see the specific results for each breakout session above)

As horizontal points, a clarification of definitions and processes, supporting soft measures, such as training activities, as well as increased funding from the EU for cross-border police cooperation were mentioned as helpful via the chat function.

Some participants clarified that by answering the poll questions, the MS representatives have not endorsed any policy options. The poll answers should be rather understood as experts' views that were given spontaneously and therefore as an informal exchange.

Final remarks by the Commission
After closing the second plenary session, the Commission thanked the participants for their participation and recapitulated the objective of the meeting, namely the identification of the likely impacts of the policy options presented by the contractor. The Commission also underlined that the options will be further elaborated and assessed based on the input provided by the workshop participants.

As a next step, the Commission provided a short outlook on the next steps, including the commitment to provide the MS with the workshop presentation.

The Commission closed its final remarks by referring to the finalisation of the study this summer which the MS will be provided access to, once it will have been published.

As a final step, the contractor also thanked the participants for their participation and officially closed the meeting.

7th Heads of SPOC meeting minutes –- 26.05.2021 *[drafted by the chair of the meeting – Italy]*

"The EU COM introduced the initiative concerning the "Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation". The EY-RAND experts first presented the objective/scope of the study which is based on the analysis of the legislative framework for cooperation and on the existing investigation tools. The study will evaluate the need for possible additional measures and compare the potential impact. The activities conducted referred to an online survey, a technical workshop held on the 25th May 2021 and consequent discussions with experts involved.

The territory under analysis includes 27 MS plus 4 Schengen associated Countries, the timeline refers to the period 1990 (CAAS undersigned that year) – 2021 while the stakeholders are EU agencies and Bodies/networks, National Authorities plus Academia and "think tanks".

Being the study activity a very complex effort we suggest a careful reading of the presentation, but for the extremely interesting part related to the SPOCs we briefly highlight some passages of the appreciated presentation. The survey allowed to underline that the SPOC is the most common structure used for polcoop info exchange, in minor extent also the PCCCs were pointed out by the survey participants. As for the channels used, Interpol and SIRENE seem to play the relevant role while SIENA is considered the most effective. Some barriers in granting the info exchange efficiency were detected as follows: fact sheets/Manuals awareness and content clarity, communications hampered by lack of good cooperation between SPOC and PCCS, LEA and Judicial Authorities, Police and Customs. Confusion on the use of channels were once again underlined as well as the complexity of the Legal framework.

The discussions of participants suggested as a way forward the consolidation/modernization of the existing fragmented legal acts, the setting up of basic and clear rules and the drafting of minimum standards.

The Chairman welcomed the initiative, which respond to the need for simplification and modernisation in a more coherent contest of the current legal basis and of the procedures, which are still hampering the cross border cooperation.

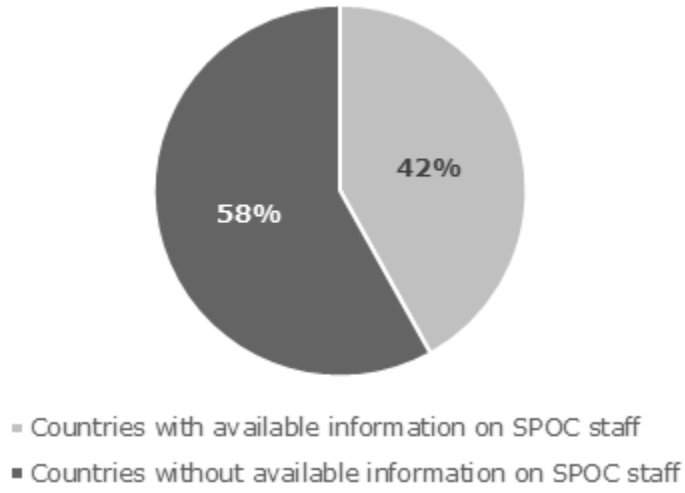
The participants unanimously agreed for the value of the initiative and expressed the need for being updated on the process developments. The ATHENA team confirmed its availability in keeping close contacts with the EU Commission for providing any further updates to the Heads of SPOC".

ANNEX 9: COMPLEMENTARY INFORMATION ON THE EXPECTED EFFECTS OF THE POLICY OPTIONS IN THE MEMBER STATES

Access to and exchange of necessary information

Set-Up and competences of the SPOC and PCCC

SPOC's staff



Source: EY/RAND Europe Study's elaboration based on Schengen evaluation reports

- In 13 countries, data on SPOC staff is available.
- In 18 countries, no data on SPOC staff is available.
- All countries would be affected if were to be established as "one stop shops" for LEA cooperation, if SPOCs were to have full access to EU and international law enforcement databases or if they were to have full access to relevant national case management systems.

Main features of SPOC's CMS

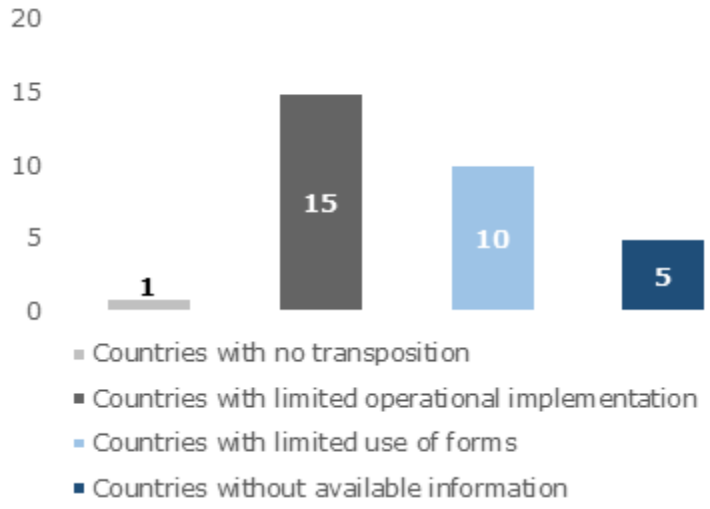
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK
Model	A	D		B	E	A	D	E	A	A	E	C	D	D						D	B	A	D		E		B	E	C	
CMS in place	Yes	Yes			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes		Yes	Yes		Yes	Yes	Yes
CMS linked with LEAs	No				No		Yes		No		No	No	Yes	No		Yes	Yes		Yes	Yes	Yes	No	No			No		No	Yes	Yes
CMS linked with PCCC	No	No			Yes		Yes		No		No	No	No	No			Yes			No			No		No	No			Yes	Yes
CMS linked with SIRENE II					Yes		Yes		No	Yes	No		Yes	Yes		No	Yes		Yes		Yes	No	No		Yes	Yes		Yes	Yes	Yes
CMS linked with Interpol					Yes		Yes		No	Yes	No		Yes				Yes		Yes		Yes	No	No		Yes	No		Yes	Yes	Yes
CMS linked with Europol					No		Yes	No	No		No		Yes	No		No	Yes		Yes		Yes	No	No		Yes	No		No	Yes	No
Cross-check functions					No				No		No	No		Yes		No	Yes		Yes	No	No		No		No				No	Yes
Automatic upload														No					Yes											Yes
Notification of deadlines						No		No	No		No	Yes					Yes		No			No	No		No	No				
Statistical functionality							No					No					Yes											No		

Source: EY/RAND Europe Study's elaboration based on desk research (dark grey cells indicate that no information is available)

- Five different SPOC workflow structures exist at national level,[337] with 5 countries reported to have the most advanced model.
- 9 countries reported that the CMS of the SPOC has access to that on the rest of LEAs, 5 to that of PCCCs.

Information exchange via SIENA and other communication channels

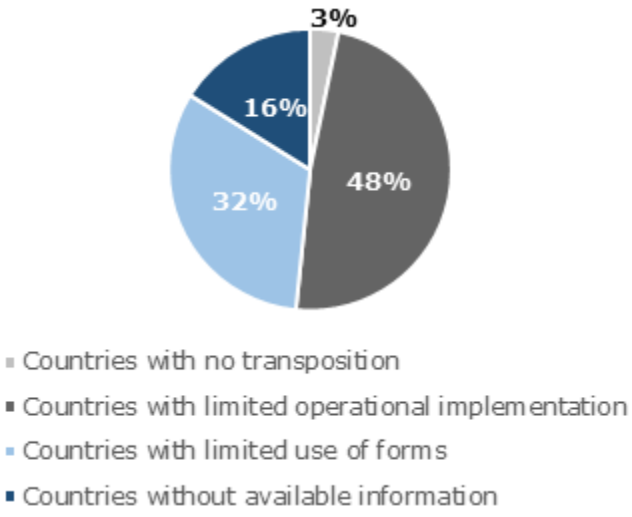
Implementation of the Swedish Framework Decision



Source: EY/RAND Europe Study's elaboration based on Schengen evaluation reports

[337] Model A: a different office for each channel, different training and a different case management system (CMS); Model B: a different office for each channel, different training/assignments, and two offices share the same CMS; Model C: SPOC sends and receives messages, while other offices handle the different channels. Different training for each office and each office has its own CMS; Model D: One CMS, one office but separate assignments and training depending on the channel; Model E: One SPOC handles all messages through one CMS and all staff have the same training. See Note from the Presidency of the Council of the EU to the Working Party for Schengen Matters (SIS/SIRENE)/Mixed Committee (EU-Iceland/Norway and Switzerland/Liechtenstein on Single Point of Contact (SPOC) - Possible mean for decreasing SIRENE workload (8031/19).

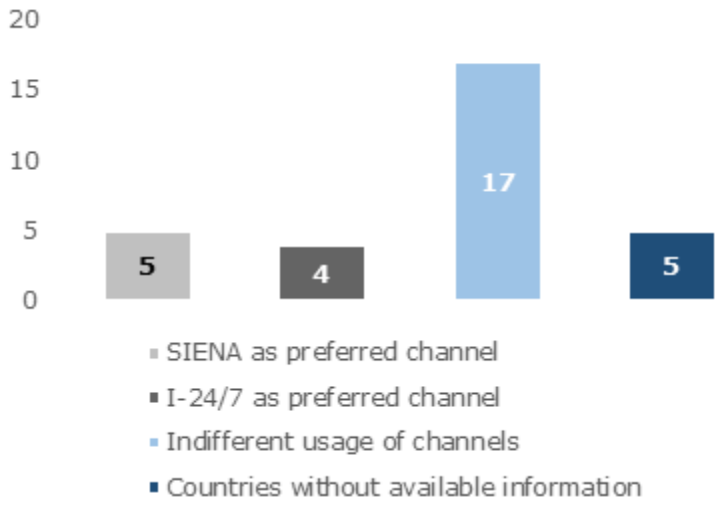
Implementation of the Swedish Framework Decision



Source: EY/RAND Europe Study's elaboration based on on Schengen evaluation reports

- 15 countries report limited use of the forms of the SFD. If new, simpler, and more user-friendly forms were to be introduced, these 15 countries might be particularly affected.
- 10 countries report limited operational implementation of the SFD. If new, simpler, and more user-friendly forms were to be introduced, these 10 countries might be particularly affected.

Preferred communication channel



Source: EY/RAND Europe Study's elaboration based on Schengen evaluation reports

Preferred communication channel

Source: EY/RAND Europe Study's elaboration based on Schengen evaluation reports

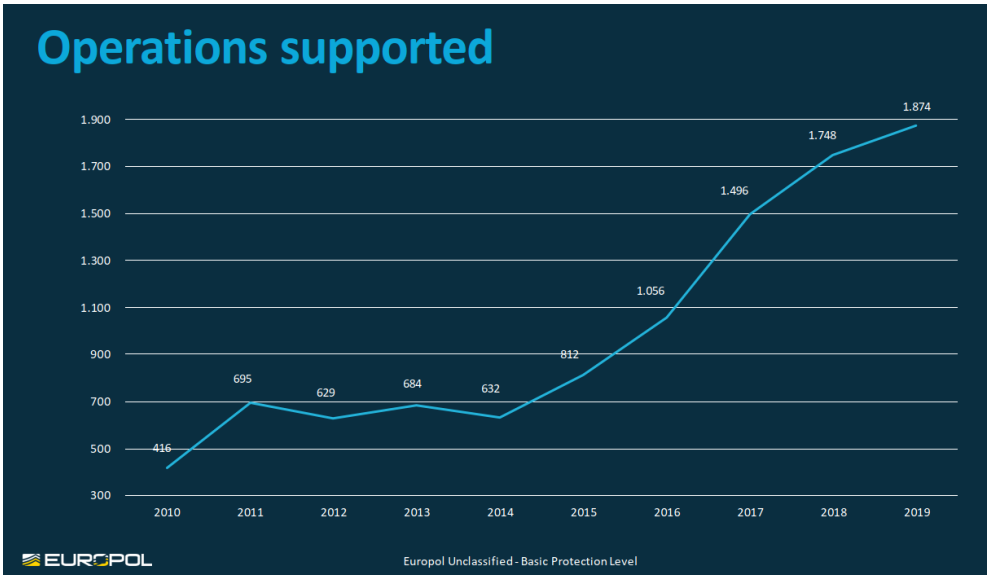
- If SIENA was established as the preferred/default channel for information exchange, this would imply changes for 4 countries who currently prefer the I-24/7 channel.

- For those 17 countries which are indifferent between communication channels establishing SIENA as the preferred / default channel would imply smaller changes as for those who clearly prefer the I-24/7.

- For 5 countries which use SIENA as the preferred communication channel, no change is expected.

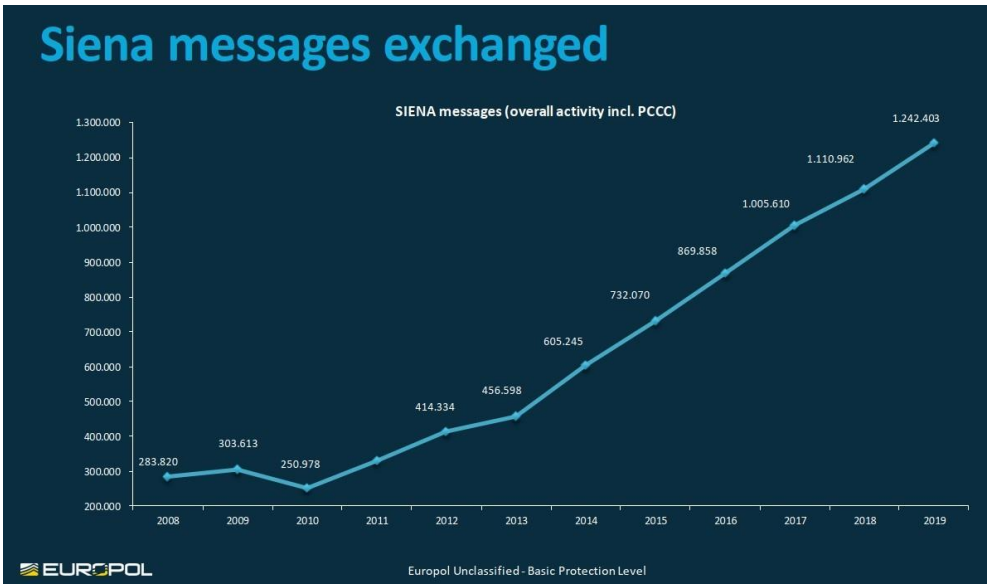
- If English was established as the default language for the use of SIENA and if newer, simpler and more user-friendly forms were to be established, all countries would be affected.

Number of supported operations



Source: Europol[338]

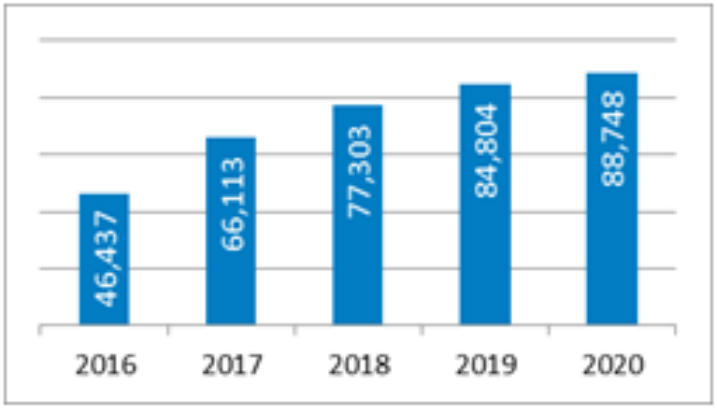
Number of exchanged messages in SIENA



[338] Europol (2020) *Welcome to Europol An Operational Overview.*

Source: Europol[339]

Number of initiated cases per year



Source: Europol, SIENA Annual Report 2020[340]

Effects of the envisaged measures on different types of stakeholders

Based on the assessment above, the following table provides an indicative view on the extent to which different types of stakeholders are expected to be affected by the elements concerning each of the specific objectives of the policy option.

Impacts on different types of stakeholders

			Access to and exchange of information
Public authorities	**Law Enforcement Authorities**	**SPOCs**	
		PCCCs	
		Other	
	Judicial Authorities		
	Data Protection Authorities		
NGOs			
Citizens / Businesses			

Source: EY/RAND Europe Study's elaboration

Cells that are marked in darker green denote a stronger positive impact on the different types of stakeholders, whereas cells that are denoted in yellow denote less strong positive impact.

The table shows that law enforcement authorities and citizens/businesses are slightly positively affected in the baseline scenario. However, only minor positive impacts are expected for other public authorities, as well as NGOs.

[339] Europol (2020) *Welcome to Europol An Operational Overview.*
[340] Europol (2020) *SIENA Annual Report 2020.*

ANNEX 10: COMPLEMENTARY INFORMATION ON THE POLITICAL FEASIBILITY OF ENVISAGED MEASURES

Throughout different stages of the study supporting this impact assessment, numerous types of documents have been reviewed and stakeholders have been consulted for contributions and feedback in order to co-develop and fine-tune the policy options (e.g. through interviews, focus groups, the online survey, technical workshops, and the public consultation).

This means that the elements of the policy options were, *inter alia*, drafted based on the contents of specific Council Conclusions and, for instance, the outcomes of various Heads of SPOC meetings, as well as based on the direct feedback voiced by individual representatives of Member States and other stakeholder groups.

Similar is valid for the assessment of the impacts of the policy options: The primary source was the feedback obtained directly from Member State representatives through the methodologies implemented as part of the study.

However, due to the very tight timeframe of this study, the study process did not leave room for the Member States (or other stakeholders groups) to voice a politically negotiated and officially agreed position regarding the impact of the different elements of the policy options. Moreover, it turned out to be very challenging to obtain factual reliable quantitative and qualitative information about the impacts of the policy options on specific Member States and the respective stakeholders affected.

Therefore, the assessments of the impacts of the policy options have been carried out based on the best information available, including based on expert judgment and the experience of the Study Team.

Moreover, gauging stakeholders' high-level support for specific elements of the policy options has been challenging within the study process. It should be noted that different types of stakeholders may have different positions.

For instance, the extent to which Member States may support the establishment of a common minimum set of data for exchange depends on a wide variety of factors such as:

- *Legal situation in the Member States:* What types of data are already collected and being made available for exchange? Does the envisaged dataset necessitate and extension of that list or is this already sufficiently addressed in the current legal situation?

- *Political preference of the government:* If additional data needs to be collected and made available for exchange, is this regarded as politically opportune? To what extent would this be aligned with existing data protection rules, as well as safeguards for fundamental rights? Moreover, even those Member States that currently do collect those datasets that should be made available, may not be willing to share them with other Member States and SAC.

- *Perceived complexity to implement certain elements of the policy options in practice:* To what extent and how do legislative, technical, and operational changes have to be implemented in order to enable making available a certain set of data to other Member States? What is a realistic timeline and budget that needs to be allocated and spent in this regard?

- *Type of stakeholder queried for feedback on a specific element:* What are the different positions of LEAs (including e.g. SPOCs and PCCCs), judicial authorities, data protection authorities, NGOs and civil society organisations?

Although a complex and challenging endeavour, the study team was able to gauge stakeholders' *personal* high-level views on the policy options throughout the study process in an indicative way (meaning not based on official positions established by stakeholders). The respective indications of support for overarching and more specific elements of the policy options by various types of stakeholder groups have been provided in the following table using a rating from weaker (white) to stronger support (dark green).

The table should only be read as an indication of the Study Team's understanding of general trends concerning the potential high-level support of stakeholders for (specific aspects of) the policy options. The table is not based on official positions provided by the Member States. In fact, it is very likely that specific stakeholders in specific Member States have a differing view from what is indicated in the table when it comes to the legal, technical and structural specificities of the elements of the policy options.

Stakeholders' high-level support for the policy options

Stakeholders in the Member States / Topics	Public authorities					NGOs & civil society
	Law Enforcement Authorities			Judicial Authorit	Data Protect. Authorit	
	SPOCs	PCCCs	Other			
Overarching topics						
Access to and exchange of information						
Specific topics						
Legislative improvements						
Provision of clarifications						
Introduction of new requirements						
Streamlining of existing requirements						
Alignment of different legal instruments						
Technical improvements						
Definition of technical requirements & functionalities						
Establishment of quality control mechanisms						
Structural improvements						
Establishment of organisational requirements						
Establishment of governance requirements						
Other improvements						
Provision of training						
Provision of awareness raising						
Provision of funding						
Implementation of further studies						

Source: EY/RAND Europe Study's elaboration

Cells that are marked in darker green denote a stronger positive impact on the different types of stakeholders, whereas cells that are denoted in yellow denote less strong positive impact

The table shows that, overall at large, the Study Team has sensed a general trend towards high-level support among stakeholders. LEAs seem to be, generally spoken, more supportive of the elements of the policy options than judicial authorities. With specific regard to data protection authorities, it is crucial to note that the support is contingent on the extent to which the protection of personal data is safeguarded throughout all measures foreseen under the policy options. Generally spoken, NGOs and civil society organisations are supportive of the policy options as long as fundamental rights are safeguarded, and LEAs do not come into the possession of excessive, unjustified amounts of

information about citizens and businesses that do not concern actual criminal investigations and/or legal proceedings before court.