Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation

Final Report

October 2021

This report has been prepared by EY and RAND Europe for the European Commission, Directorate-General for Migration and Home Affairs.

This study was carried out on behalf of the European Commission by

Main authors of the study

EY

- Katarina Bartz
- Nicoletta Colombo
- Ilia Gaglio
- Alana Gyszas
- Florian Linz

RAND Europe

- Michaela Bruckmayer
- Emma Disley

European Commission

Directorate-General for Migration and Home Affairs

Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation

Final Report

Directorate-General for Migration and Home Affairs

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Luxembourg: Publications Office of the European Union, 2021

PDF	ISBN 978-92-76-43474-0	doi: 10.2837/179127	DR-01-21-413-EN-N
PRINT	ISBN 978-92-76-43473-3	doi: 10.2837/883514	DR-01-21-413-EN-C

Table of Contents

Table of Tables

Table of Figures

List of Abbreviations

AI	Artificial Intelligence
Benelux	Belgium, The Netherlands, Luxembourg
CEPOL	European Union Agency for Law Enforcement Training
CIRAM	Common Integrated Risk Analysis Model
CISA	Convention Implementing the Schengen Agreement
COVID-19	Coronavirus disease 2019
DG HOME	Directorate-General for Migration and Home Affairs
DG JUST	Directorate-General for Justice and Consumers
DG TAXUD	Directorate-General for Taxation and Customs Union
DPAs	Data Protection Authorities
EBCGA/Frontex	European Border and Coast Guard Agency
EDPS	European Data Protection Supervisor
EIS	Europol Information System
EJN	European Judicial Network
EJTN	European Judicial Training Network
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EPPO	European Public Prosecutor's Office
EU	European Union
EUCPN	European Crime Prevention Network
EuroCOP	European Confederation of Police
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
ENU	Europol National Unit
FRA	Fundamental Rights Agency
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GO	General Objective
LEAs	Law enforcement authoritiesN
NECs	National EMPACT Coordinators
NFIP	National Football Info Points
OCG	Organised Crime Group
OLAF	European Anti-Fraud Office
PCCCs	Police Customs Cooperation Centres
SACs	Schengen Associated Countries
SFD	Swedish Framework Decision
SIENA	Secure Information Exchange Network Application
SIRENE	Supplementary Information Request at the National Entry Bureau
SIS	Schengen Information System
SOC	Serious and organised Crime
SOCTA	Serious and organised Crime Threat Assessment
SO	Specific Objectives
SPOC	Single Point of Contact
TESTA	Trans European Services for Telematics between Administrations
TFEU	Treaty on the Functioning of the European Union
THB	Trafficking in Human Beings

Member States

AT	Austria
BE	Belgium
BG	Bulgaria
CY	Cyprus
CZ	Czechia
DE	Germany
DK	Denmark
EE	Estonia
EL	Greece
ES	Spain
FI	Finland
FR	France
HR	Croatia
HU	Hungary
IE	Ireland
IT	Italy
LI	Liechtenstein
LT	Lithuania
LU	Luxembourg
LV	Latvia
MT	Malta
NL	The Netherlands
NO	Norway
PL	Poland
PT	Portugal
RO	Romania
SE	Sweden
SI	Slovenia
SK	Slovakia

Schengen Associated Countries

CH	Switzerland
IS	Iceland
LI	Liechtenstein
NO	Norway

OVERVIEW OF THE REPORT

Title	**Final Report**
Date	October 2021
Main content	• Overview of the work conducted as part of the project • Results of the analysis of: Cross-border law enforcement cooperation measures at European Union (EU) and national levels, investigative tools to fight serious and organised crime at the national level, the problem, the need for EU action, the future policy objectives, operational recommendations, and the analysis of the impacts of the policy options and comparison of these.

ABSTRACT

The present study to support the preparation of an impact assessment aims to provide non-binding, factual and not pre-emptive recommendations for possible additional EU measures in the area of intra-EU law enforcement cooperation and to assess and compare the impacts of identified policy options. Through detailed desk research and numerous data collection activities, the problems and drivers related to cross-border cooperation, the need for EU action, the relevant policy objectives, and operational recommendations for potential EU action were identified during Phase 1. The main causes of the current problems relate to access to and exchange of information and operational cooperation.

In Phase 2, the operational recommendations were further elaborated and clustered into two policy options in addition to the baseline scenario. Subsequently, an assessment of the impacts was performed for the three policy options, covering e.g. the criteria of effectiveness, efficiency and coherence. Based on this assessment, a ranking and comparison of the two policy options' performance vis-à-vis the baseline scenario was conducted, applying a Multi-Criteria-Analysis.

Finally, this study covered the identification of policy option 2 as the preferred policy option, which constitutes a legal proposal on minimum standards that is flanked by supporting (soft) measures.

The contents of this report are based on the information and evidence the Study Team was able to gather through secondary and primary sources as part of the assignment under the guidance of the European Commission.

Therefore, the report is to be understood as a non-binding, evidence-based analysis of information obtained via desk research and arguments provided by stakeholders to support the European Commission in line with the Tender Specifications of this project.

EXECUTIVE SUMMARY

This executive summary provides a brief recapitulation of the objectives and scope of this study, as well as the methodological approach used. Subsequently, it presents an overview of the main findings of this study.

Framework and methodology of the study

Objectives and scope of the assignment

The **primary objectives** of the study were to:

- Identify any shortcomings of - and gaps in - the EU framework for intra-EU law enforcement cooperation;
- Describe the current capacity to perform the tasks and achieve the objectives of all stakeholders with a role in the implementation and application of the EU framework, including through the identification and analysis of the most comprehensive and advanced practices for cross-border law enforcement cooperation at bi-/tri- and multilateral, as well as regional levels (i.e. going beyond the EU framework);
- Shed light on the use of investigative tools by law enforcement authorities (LEAs) at the national level and in cross-border settings to fight serious and organised crime (SOC), and assess if relevant EU rules could close potential gaps in national legislation and improve cross-border cooperation; and
- Make suggestions to simplify, clarify, streamline and modernise the current framework insofar as problems require such action and, if relevant, reduce its burden on stakeholders.

Overall, the study aimed to provide non-binding, factual and not pre-emptive recommendations, as well as an assessment and comparison of possible future EU action.

In order to meet the objectives listed above, the **scope of the study** was defined as follows:

Table 1 – Scope of the assignment (Executive Summary)

Category	Definition of the scope
Subject matter	The study covered: • EU binding and non-binding measures on intra-EU law enforcement cooperation (covering both mechanisms for cooperation and the cross-border use of investigative tools); • Bi-/tri-/ and multilateral agreements between Member States and Schengen Associated Countries (SACs) that establish specific rules and practices for law enforcement cooperation between the involved countries (covering both mechanisms for cooperation and the cross-border use of investigative tools); • National legislation on investigative tools that are used to fight SOC; • Operational issues faced by national LEAs cooperating with other Member States and SACs; • The main areas of analysis included: (1) Access to and exchange of information, (2) operational cooperation for public order and safety (e.g. cooperation in relation to sports and cultural events, accidents, and disasters), and (3) operational cooperation to fight SOC and terrorism. The study focused on: • Cooperation between neighbouring Member States and SACs, and also across the EU; • Cooperation between police-customs, police-police and customs-customs (in so far as customs agencies have criminal investigation powers); • Law enforcement cooperation, and not EU judicial cooperation. Mutual recognition instruments, such as the European Investigation Order and the European Arrest Warrant, mutual recognition of freezing orders and confiscation orders, and investigative tools such as Joint Investigation Teams were out of the scope of the study. The study also did not cover financial investigations and mechanisms facilitating the use of financial and other

Category	Definition of the scope
	information for the prevention, detection, investigation or prosecution of certain criminal offences; instruments on controls on cash entering or leaving the Union.
Timeline	The study covered the evolution of the cross-border law enforcement cooperation policy area in the EU, from the 1990 Convention Implementing the Schengen Agreement (CISA) up to the latest developments. At the same time, the study had a forward-looking perspective to account for expected relevant trends and developments in the years to come (until 2030).
Territory	All 27 EU Member States and the four SACs (Iceland, Lichtenstein, Norway and Switzerland).

Source: Author's elaboration based on available evidence

Performance of the study: methodological approach and challenges encountered

The study objectives listed above were pursued through **eight tasks**, covering: a problem definition and examination of underlying causes (Task 1); a comparative overview of cross-border cooperation-related measures at the EU level, as well as an analysis of existing bi-/tri-/ and multilateral agreements by the Member States and SACs (Task 2); an overview of investigative tools used at the national level (Task 3); an analysis of the need for EU action (Task 4); the definition of the objectives of possible EU action (Task 5); a formulation of alternative policy options, including the baseline scenario (Task 6); a qualitative (and where possible quantitative) assessment of the likely impacts of the policy options vis-à-vis the baseline scenario of no EU action (Task 7); and a comparison and ranking of the policy options based on well-defined assessment criteria, followed by the identification and assessment of the preferred option (Task 8).

Throughout these tasks, multiple **data collection activities** were conducted, including detailed desk research, as well as broad field research activities. The **desk research** in this study covered a documentary review to map the most relevant EU objectives and policies in the field of cross-border law enforcement cooperation, as well as a detailed analysis of bi-/tri-/ and multilateral agreements. In addition, the desk research included a legal review and mapping of relevant legislation at the EU and national levels. As part of the **field research**, a combination of data collection instruments was used, namely[1]: stakeholder interviews (n=48), an online survey (n=239), four focus groups (n=48), an Open Public Consultation (n=20) and three workshops.

In general, the COVID-19 pandemic caused **specific challenges for the performance** of the field research activities. The fact that these activities had to be conducted remotely partly had a hampering effect on the discussions between the stakeholders. This was specifically visible in the technical workshops. In addition, the provision of quantitative data by the consulted stakeholders can be considered as very limited.

Summary of the study findings

Problem definition

In Task 1 of this study, the main problems and their causes (drivers) to be addressed by a possible future intervention were identified.

The task was based on an analysis of the **high-level security problems** that currently affect EU citizens/consumers, businesses, public institutions and other stakeholders, i.e. including increasing and evolving SOC, changing structures of Organised Crime Groups (OCGs) and networks, and increased EU mobility for work and leisure, creating opportunities of exploitation for OCGs.

The identification of high-level security problems was followed by an analysis of the **core problems** that a future policy intervention should directly address, notably:

- The access to and exchange of information among law enforcement authorities is subject to legal, technical and structural challenges;

[1] The information provided in brackets after some of the data collection instrument indicates the respective number of participants/respondents.

- The ongoing intra-EU mobility is not met with an adequate development of tailored joint operations; and
- EU and national implementation rules hamper cross-border operational cooperation for SOC.

For each core problem specific drivers were identified. Figure 1 presents the link between the high-level problems, the core problems and the drivers.

Figure 1 – Problem Tree (Executive Summary)

High level problems	Increasing and evolving SOC poses an ever larger and ongoing security threat and leads to social and financial detriment for citizens, companies and public institutions across the EU.	The growing intra-EU mobility creates additional challenges for the prevention and fight against all forms of criminal and safety threats.
Core problem	**1** – The access to and exchange of information among law enforcement authorities is subject to legal, technical and structural challenges.	
Drivers	• **Legal driver:** Law enforcement authorities face difficulties in interpreting and implementing relevant EU provisions. • **Technical driver:** Law enforcement authorities have insufficient knowledge of existing mechanisms, skill gaps and outdated IT infrastructure. • **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.	
Specific core problems	**2** – The ongoing intra-EU mobility is not met with adequate development of tailored joint operations.	**3** – EU and national implementation rules hamper cross-border operational cooperation for SOC.
Drivers	• **Legal driver:** There is a limited and at times asymmetric conferral of executive powers of law enforcement officers operating in the respective host States, as well as limited awareness of these powers on the ground. • **Technical driver**: Officers on the ground have limited remote access to relevant law enforcement databases. • **Structural driver:** National law enforcement authorities have limited financial and human resources to expand the use of joint operations. • Cooperation between law enforcement authorities in different countries, e.g. for the purpose of joint operations notably in border regions, is insufficiently informed by joint threat assessment/risk analysis.	• **Legal driver:** Law enforcement authorities are not able to efficiently use investigative tools in a cross-border context and face obstacles caused by differences in national rules.

Source: Author's elaboration based on available evidence

The study findings stemming from Task 2 (Comparative overview of cross-border cooperation-related measures at EU level & Analysis of existing bi-/tri-/ and multilateral agreements) and Task 3 (Overview of investigative tools at the national level) were considered thoroughly for the problem definition, as well as for the identification of potential measures under the policy options (Task 6). Overall, the analyses conducted in Tasks 2 and 3 show a large number and **significant variety of existing measures** (binding and non-binding) in the area of cross-border law enforcement, both at the EU and national levels, as well as the bi-/tri-/multilateral agreements.

The problem definition also included an analysis of the **EU dimension of the high-level problems**, which found that the forms of crimes covered in the study all constitute international issues. The analysis shows an increased mobility of criminals across national borders and highlights that technological advancements have created opportunities for new types of cross-border crime. It was also found that there is a clear EU dimension to the issues related to effective law enforcement operations, as the increased mobility of persons across Europe implies that e.g. sports, social and cultural events are attended by persons from across the EU 27 and the SAC. These findings are specifically important in relation to the need for EU action.

The need for EU action

The analysis of the need for EU action in the field of cross-border law enforcement cooperation (Task 4) was structured according to:

- **The relevant legal basis**: The legal basis for EU action in the field of intra-EU law enforcement cooperation is Title V, Chapter 5 of the Treaty on the Functioning of the European Union (TFEU). Pursuant to Article 87 (TFEU), "the Union shall establish police

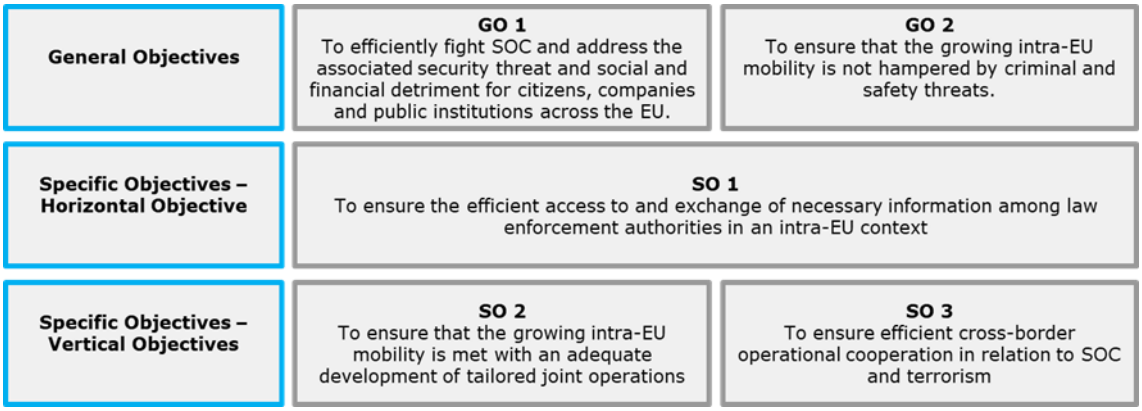
cooperation involving all the Member States' competent authorities, including police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences".

- **The necessity of EU action**: EU action is needed to properly address all three core problems. First, Member States and SAC alone would not be able to overcome the confusion regarding the proper EU legal basis and on the most appropriate tool/channel to use for information exchange. Moreover, Member States and SAC alone could neither properly ensure an appropriate and uniform level of capacity to use relevant databases, nor overcome current differences among Single Points of Contacts (SPOCs). Second, Member States and SAC would continue to face uncertainties stemming from different legal systems on the rights of officials when operating in foreign countries. Also, technical interoperability issues concerning both large-scale IT systems, as well as radio communication[2], that would eventually contribute to reducing the appeal of joint operations are expected not be sufficiently solved by individual states alone. Finally, the differences in national rules regarding rights and duties of officials as well the use of investigative tools would remain.
- **The added value EU action**: EU intervention could create added value by providing Member States and SAC with common minimum standards for intra-EU law enforcement cooperation. This would contribute towards a common playing field, which could not be achieved by the Member States and SAC alone. Indeed, the study found evidence that current national differences contribute to an inefficient exchange of information. Moreover, the cross-border nature of safety and security threats, as well as the challenges related to the increasing cross-border nature of SOC call for an EU intervention of some kind. The EU is expected to be well-equipped to ensure coherence of actions taken at the national level, address the legal fragmentation, prevent duplications and uncertainties and eventually ensure an efficient action to fight cross-border SOC and terrorism.

Policy objectives

Based on the findings of Tasks 1 to 4, the objectives of a potential future EU initiative were developed (Task 5), differentiating between general objectives (GO) and specific objectives (SO). The results of this task are summarised in Figure 2 below.

Figure 2 – Objective tree (Executive Summary)



Source: Authors' elaboration based on desk research

In a next step, these general and specific objectives were analysed regarding their coherence with other EU policies in the field of cross-border law enforcement cooperation. As an overall summary, the objectives were found to be **consistent with the following policies**: (i) the EU Security Union Strategy for the period 2020 to 2025; (ii) the Counter-Terrorism Agenda; (iii) the EU Strategy to tackle Organised Crime 2021-2025; (iv) Council Document 13083/1/20; (v) Commission Recommendation (EU) 2017/820; (vi) Commission Staff Working Document

[2] One the one hand, the notion "interoperability" refers to large-scale IT systems seamlessly communicating with each other, e.g. to exchange information. Further information is available at this link and this link. On the other hand, "interoperability" may also refer to the alignment of frequencies or frequency ranges of Member States' radio communication in order to facilitate operational communication, e.g. during joint investigations.

SWD/2020/327 final; (vii) Council Document 10062/19; (viii) Council Document 5503/21; and (ix) the Strategy towards a fully functioning and resilient Schengen area.

Operational recommendations

As part of Task 6, three policy options were elaborated to address the challenges identified in the problem definition, as well as to meet the objectives displayed in the objective tree above. The options are listed below, from the least to the most "extensive" option:

- *Policy Option 1:* Baseline Scenario/Status Quo (PO1 / BS);
- *Policy Option* 2: Legal proposal on minimum standards + supporting (soft) measures (PO2);
- *Policy Option 3:* Legal proposal aiming for stronger alignment + supporting (soft) measures (PO3).

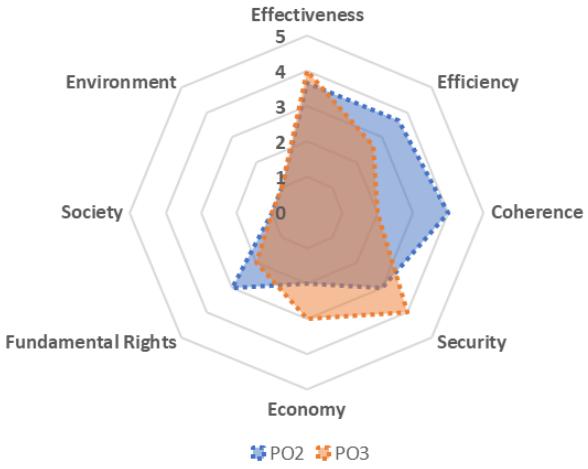
The developed policy options contain both legislative and non-legislative elements (or sub-options) dealing with the problems identified in different ways, while aiming to achieve the policy objectives set out in the section above. Whereas the two policy options developed (in addition to the baseline scenario) both individually address all aspects identified in the problem assessment and the specific objectives, the choice of legislative and non-legislative elements varies slightly between the two policy options.

Based on the analysis conducted, it appears that both the form of a Directive and the form of a Regulation could be relevant to address the problems identified. Both measures have the potential to harmonise the diverging approaches existing in the Member States, although to a different degree. However, the option of proposing a Regulation is not viewed as politically feasible. In this regard, amending the Swedish Framework Decision (SFD) (compared to CISA, Prüm or the Naples II Convention or proposing a new instrument) is recommended to introduce the legislative elements that address specific objective #1 (information exchange). For all legislative elements referring to operational cooperation (objectives #2 and #3), also amending existing legislation, e.g. Prüm, would seem to be advisable. The reason to consider two legal instruments is the political feasibility of the measures: Whereas measures on information exchange require qualified majority, measures on operational cooperation require unanimity.

Analysis of the impacts of the policy options

In Task 7, a detailed **assessment of the impacts** was conducted for all measures included in the three policy options elaborated under Task 6, covering eight criteria: effectiveness, efficiency, coherence and proportionality, as well as security, economy, fundamental rights (assessment of how the option safeguards fundamental rights[3] or any adverse effects), society and environment. The findings of the assessment of PO2 and PO3 vis-à-vis the baseline scenario are presented in Figure 3.

In accordance with the Commission's *Better Regulation Guidelines*, each measure under the baseline scenario (and therefore the policy option as a whole) was assessed to have no (further) positive or negative impact. Therefore, it was given a "0" for the assessment and is not presented visually. The figure to the right displays each of the two additional policy options' ratings with respect to the assessment criteria overall, whereas the



Source: Author's elaboration based on available evidence; Legend: 0 – no impact (baseline scenario); 1 – very small positive impact; 2 – small positive impact; 3- moderate positive impact; 4 – large positive impact; 5 – very large positive impact

[3] This assessment refers in particular to the following Articles in the EU Charter of Fundamental Rights: Art. 2, Art.3, Art. 6, Art. 7, Art. 8, Art. 17 and Art. 45. However, some elements of the options also have impacts e.g. related to vulnerable groups, children and elderly.

assessments in the main report make a further distinction between ratings in relation to each of the three specific objectives as concerns effectiveness, efficiency, and coherence.

Figure 3 shows that the assessments of PO2 and PO3 differ slightly from each other with respect to various criteria.

The differences between PO2 and PO3 in relation to their expected impacts on fundamental rights, society and the environment are expected to be limited. With specific regard to fundamental rights, however, the extension of the common minimum set of data required to be collected and shared by Member States according to PO3 is expected to potentially have negative impacts on vulnerable persons. Also, while the positive impact on the economy is assessed as 'moderate' for PO3, it is only assessed as 'small' for PO2. The same is valid for security, in relation to which PO3 is likely to have a 'large' positive impact, while PO2 is expected to have a 'moderate' positive impact.

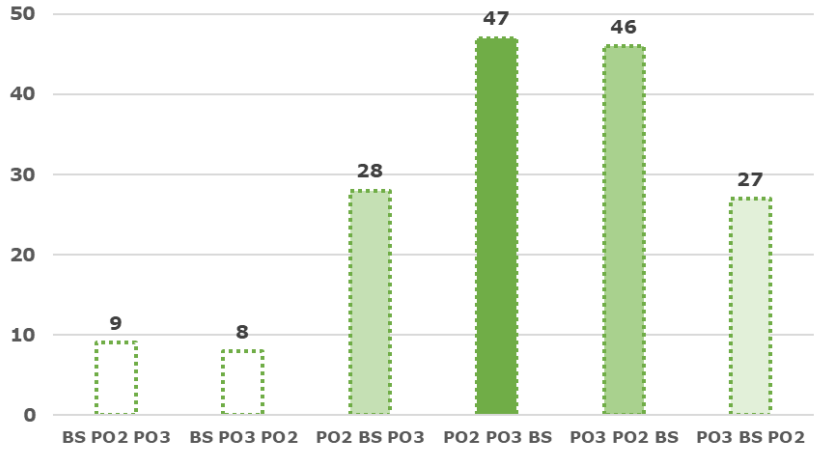
Ranking and comparison of the impacts of options and definition of preferred option

In order to rank and compare the policy options' performance vis-à-vis the baseline scenario, a Multi-Criteria-Analysis (MCA) was applied in full alignment with the European Commission's *Better Regulation Guidelines* (see Tool #63).

The MCA was carried out in three steps, including: Step 1: Set-up of the framework of criteria, and an assessment grid; Step 2: Establishment of an outranking matrix; and Step 3: Assessment through a permutation matrix.

Based on steps 1 and 2, the outranking matrix was transformed to a policy permutation matrix in which pairings and the coefficients from the outranking matrix (step 2) were summed up. The permutation matrix provides a clear overview of which policy option is most favourable, as well the relative 'favourability' of different permutations of policy options. The results of step 3 are presented in the figure to the right showing that permutation #4 (PO2-PO3-BS, dark green) is most advantageous.

Figure 4 – Score of POs (based on permutation matrix)



Source: Author's elaboration based on available evidence

This means that, based on the assessment, **PO2 should be implemented**. If this is not possible, e.g. due to political reasons, the Commission could aim at implementing PO3. In case this would also not be possible, the Commission should remain with the baseline scenario. The fact that permutations #4 and #5 have almost the same score is noteworthy, meaning that from a pure MCA perspective, there is only a marginal difference between the Commission initiating the policymaking process on the grounds of PO2 or PO3.

Based on the assessments and MCA outlined above, **PO2 is defined as the preferred option**. According to the analysis conducted under Tasks 7 and 8, PO2 is expected to have a large positive impact in terms of effectiveness, efficiency, and coherence. Therefore, it is expected that PO2 will have a large impact on the efficiency of EU cross-border law enforcement cooperation as such. Overall, PO 2 is considered proportionate in view of the problems identified in this study, as well as their magnitude, and likely future development.

However, it should be noted that the **political feasibility** of new measures in the area of law enforcement cooperation is often challenging and should be taken into account for future steps.

1 INTRODUCTION

This is the Final Report in relation to the request for service HOME/2020/ISFP/FW/EVA2/0018 for a *Study to support the preparation of an impact assessment on the European Union (EU) policy initiatives facilitating cross-border law enforcement cooperation*. The study was conducted by EY and RAND Europe.

1.1 Objectives and scope of the assignment

The present study aimed to provide non-binding, factual, fed by evidence and not pre-emptive 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 **primary objectives of the study** were to:

- Identify any shortcomings of - and gaps in - the EU framework for intra-EU law enforcement cooperation;
- Describe the current capacity to perform the tasks and achieve the objectives of all stakeholders with a role in the implementation and application of the identified EU framework for intra-EU law enforcement cooperation, including through the identification and analysis of the most comprehensive/advanced practices for cross-border law enforcement cooperation at bi-/tri- and multilateral, as well as regional levels (i.e. going beyond the EU framework);
- Shed light on the use of investigative strategies and tools by law enforcement authorities (LEAs) at the national level and in cross-border settings to combat and tackle organised crime, and assess if EU rules could close potential gaps in national legislation and improve cross-border cooperation as far as the investigative tools available to LEAs to effectively fight organised crime are concerned;
- Make suggestions to simplify, clarify, streamline and modernise the current framework, as well as other policy measures, insofar as the identified problems require such action and, if relevant, reduce its burden on stakeholders.

The results of this study will support the Commission with the necessary evidence to prepare a Staff Working Document (Impact Assessment) to inform any possible decision concerning future measures, notably the legislative proposal for an **EU Police Cooperation Code**[4] planned towards the end of 2021, as stated in the Strategy towards a fully functioning and resilient Schengen area[5].

Table 2 provides an overview of the **scope of the study**.

Table 2 - Scope of the assignment

Category	Definition of the scope
Subject matter	The study covers: • EU binding and non-binding measures on intra-EU law enforcement cooperation (covering both mechanisms for cooperation and the cross-border use of investigative tools); • Bi-/tri-/ and multilateral agreements between the Member States and Schengen Associated Countries (SACs) that establish specific rules and practices for law enforcement cooperation between the involved countries (covering both mechanisms for cooperation and the cross-border use of investigative tools); • National legislation on investigative tools to fight serious and organised crime (SOC); • Operational issues faced by national LEAs cooperating with other Member States and SACs;

[4] As discussed in the section on the operational recommendations (section 5), the Police Cooperation Code may not necessarily take the form of *one* legislative instrument.
[5] European Commission (2021). Communication from the Commission to the European Parliament and the Council. A strategy towards a fully functioning and resilient Schengen area, COM(2012) 277 final.

Category	Definition of the scope
	• The main areas of analysis included: (1) Access to and exchange of information, (2) operational cooperation for public order and safety (e.g. cooperation in relation to sports and cultural events, accidents, and disasters), and (3) operational cooperation to fight SOC and terrorism. The study focused on: • Cooperation between neighbouring Member States and SACs, and also across the EU; • Cooperation between police-customs, police-police and customs-customs (in so far as customs agencies have criminal investigation powers); • Law enforcement cooperation, and not EU judicial cooperation. Mutual recognition instruments, such as the European Investigation Order and the European Arrest Warrant, mutual recognition of freezing orders and confiscation orders, and investigative tools such as Joint Investigation Teams are out of the scope of the current study. The study also does not cover financial investigations and mechanisms facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences; instruments on controls on cash entering or leaving the Union.
Timeline	The study covered the evolution in the EU in relation to the cross-border law enforcement cooperation policy area from the 1990 Convention Implementing the Schengen Agreement (CISA) up until the latest developments. At the same time, the study has a forward-looking perspective to account for expected relevant trends and developments until 2030.
Territory	All 27 EU Member States and the four SACs (Iceland, Lichtenstein, Norway and Switzerland).

Source: Author's own elaboration

1.2 Methodological approach

This section provides a short overview of the analytical framework, the data collection process and the main challenges encountered during the implementation of the assignment. The study pursued the objectives presented in section 1.1 through eight tasks:

Table 3 – Tasks of the study

Task	Description
Task 1	A problem definition, examining the underlying causes, as well as its possible evolution, considering the anticipated trends/developments in the absence of EU action
Task 2	• A comparative overview of cross-border cooperation-related measures (binding and non-binding) at the EU level, including investigative tools for police and customs cooperation • A thorough analysis of existing bi-/tri-/and multilateral agreements implemented by the Member States and SACs on cross-border cooperation, with a view to identify good/best practices especially as concerns investigative tools
Task 3	An overview of the investigative tools used at the national level to fight organised crime and an analysis of their actual use and effectiveness
Task 4	An analysis of the need for EU action in the field of cross-border law enforcement cooperation
Task 5	A definition of the objectives for possible EU action in the area of law enforcement cooperation
Task 6	Formulation of alternative policy options, including the baseline scenario
Task 7	A qualitative (and to the extent possible quantitative) assessment of the likely impacts of the policy options vis-à-vis the baseline scenario of no EU action
Task 8	A comparison and ranking of the policy options based on well-defined assessment criteria, followed by the identification and in-depth assessment of preferred option

Source: Author's own elaboration

Data collection process

As part of the **desk research** in this study, the following analyses were conducted:

- A **documentary review** to map the most relevant EU objectives and policies in the field of cross-border law enforcement cooperation. In addition, the documentary review included studies and papers to inform the problem definition and impact assessment[6].
- A **legal review** to map relevant legislation at the EU and national levels, as well as including bi-/tri-/ and multilateral agreements.

As part of the **field research**, data were collected through the following methods:

- Overall, 48 **stakeholder interviews** were conducted for this study, covering: ten interviews with EMPACT drivers and two group interviews with EMPACT support managers, 20 interviews with EU bodies, four interviews with academia and think tanks, as well as well as twelve group interviews with Member State representatives for the case studies.
- An **online survey** targeting national stakeholders to collect inputs for the identification of problems in the area of cross-border law enforcement cooperation, as well as for the definition of the need for EU action. The survey results were also used to describe the baseline scenario and identify possible measures for the policy options. Overall, 239 respondents answered the survey (216 from national LEAs representatives, 13 from national judicial authorities and 10 from national data protection authorities).
- Four **focus groups** with 48 participants, covering a more detailed discussion of bi-/tri- and multilateral agreements, namely: the Benelux agreement (BE, NL, LU), the DE-CZ agreement, the CH-FR agreement and the Nordic Countries agreement (DK, FI, IS, NO, SE).
- An **Open Public Consultation**, gathering inputs from a broad group of stakeholders. Overall, 20 respondents participated in the Public Consultation.
- Three **workshops/meetings**, including a Law Enforcement Working Party (LEWP) meeting, as well as two technical workshops.

Annex I provides a more detailed overview of the methodology for this assignment, the consultation tools used, as well as the types of stakeholders consulted.

Challenges encountered

In general, the COVID-19 pandemic caused specific challenges for the performance of field research activities. The fact that these activities had to be conducted remotely had a hampering effect on the discussions between the stakeholders. This was specifically visible in the technical workshops, where it was in some cases challenging to initiate a lively discussion between the participants.

Moreover, the collection of reliable quantitative data was challenging. Whereas in relation to some aspects (e.g. the number of messages sent via SIENA or economic damage caused by organised crime groups) specific evidence could be obtained and extrapolated until 2030 (based on qualitative assumptions), the information base concerning costs indicators is very limited – both in relation to the existing problems, as well as the impacts of the policy options.

Most importantly, this can be attributed to the general lack of quantitative data in the area of cross-border law enforcement cooperation, e.g. with regard to operational costs and cost reduction potentials. Since law enforcement authorities are, naturally, focused on achieving the best possible outcomes from a law enforcement perspective, there seems to be a widespread

[6] In this regard, the Schengen Evaluation Reports have been accessed. A randomised coding system has been used for references to these reports, as the national reports are not publicly available. The coding system has only been used with regard to information that stems from the Schengen Evaluation Reports. Therefore, the report also contains non-classified info that is clearly linked to the (open) name of a specific Member State.

lack of knowledge about the associated costs – at least among the stakeholders consulted as part of this study.

In order to mitigate this challenge, the study team conducted numerous interviews with EU bodies and Member State representatives and queried specifically for quantitative information about the existing problems and the impacts of the policy options (including costs and benefits). The study team could, however, only obtain quantitative evidence in occasional instances and often based on anecdotes or mere *gut feeling* of interviewees ("This would be very costly." "This would increase the costs dramatically." "There is great potential to reduce costly inefficiencies."). In addition, interviewees that were targeted by the study team in a number of cases only replied very late within the study process.

Therefore, the quantitative evidence included in this report concerning costs should be treated very carefully and used only within the wider context of this study.

1.3 Report structure

The report has been structured following the Terms of Reference (ToR) and considering our technical proposal. Hereafter, the report is structured in the following chapters:

- Chapter 2: Problem definition (Task 1);
- Chapter 3: The need for EU action (Task 4);
- Chapter 4: Policy objectives (Task 5);
- Chapter 5: Operational recommendations on action needed at the EU level (Task 6);
- Chapter 6: Analysis of the impacts of the policy options (Task 7 and 8);

Further supporting evidence is provided in the **following Annexes** submitted with this report:

- Annex I: Further information supporting the content of this report, including a description of the methodology and an overview of existing national rules;
- Annex II: EU and regional measures for cross-border law enforcement cooperation (Task 2) and investigative tools used to fight SOC at national level (Task 3);
- Annex III: Further study results on the problem definition and assessment;
- Annex IV: Further supporting evidence and study results for the development of policy options and the assessment of the expected impacts;
- Annex V: Synopsis report of the consultation activities;
- Annex VI: Analysis of the Open Public Consultation.

2 PROBLEM DEFINITION

2.1 Overview of the problems

This section presents the main problems to be addressed by a possible future intervention and the causes (drivers) of these problems.

The section starts with a description of the **high-level security problems** that currently affect EU citizens/consumers, businesses, public institutions and other stakeholders (i.e. cross-border SOC and evolving challenges related to ensuring public order and safety), followed by an analysis of the **core problems** that a future policy intervention can directly address:

- The access to and exchange of information among law enforcement authorities is subject to legal, technical and structural challenges;
- The ongoing intra-EU mobility is not met with an adequate development of tailored joint operations;
- EU and national implementation rules hamper cross-border operational cooperation for SOC.

Figure 5 includes all the elements of our understanding of the problem in a problem tree. The subsequent sections present in detail each block of the tree.

Figure 5 – Problem Tree

High level problems	Increasing and evolving SOC poses an ever larger and ongoing security threat and leads to social and financial detriment for citizens, companies and public institutions across the EU.	The growing intra-EU mobility creates additional challenges for the prevention and fight against all forms of criminal and safety threats.
Core problem	**1** – The access to and exchange of information among law enforcement authorities is subject to legal, technical and structural challenges.	
Drivers	• **Legal driver:** Law enforcement authorities face difficulties in interpreting and implementing relevant EU provisions. • **Technical driver:** Law enforcement authorities have insufficient knowledge of existing mechanisms, skill gaps and outdated IT infrastructure. • **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.	
Specific core problems	**2** – The ongoing intra-EU mobility is not met with adequate development of tailored joint operations.	**3** – EU and national implementation rules hamper cross-border operational cooperation for SOC.
Drivers	• **Legal driver:** There is a limited and at times asymmetric conferral of executive powers of law enforcement officers operating in the respective host States, as well as limited awareness of these powers on the ground. • **Technical driver**: Officers on the ground have limited remote access to relevant law enforcement databases. • **Structural driver:** National law enforcement authorities have limited financial and human resources to expand the use of joint operations. • Cooperation between law enforcement authorities in different countries, e.g. for the purpose of joint operations notably in border regions, is insufficiently informed by joint threat assessment/risk analysis.	• **Legal driver:** Law enforcement authorities are not able to efficiently use investigative tools in a cross-border context and face obstacles caused by differences in national rules.

Source: Author's elaboration based on available evidence

The cross-border element of threats posed by SOC in the EU is becoming increasingly important : Organised crime groups are operating as well-connected international networks in a fluid and systematic manner. Moreover, new and emerging crime opportunities are not limited to single Member States or SAC. This calls for coordination among Member States in order to ensure effective and efficient law enforcement.

2.2 High-level problems

This section presents the evidence related to the two high-level problems depicted in the problem tree above.

2.2.1 High-level problem 1: The evolution of cross-border SOC and the increasing associated harms

As made clear in the 2021-2025 EU Strategy to Tackle organised Crime[7] and the 2020 EU Security Union Strategy[8] 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. This has a significant negative impact on the area of freedom, justice and security, and undermines the free flow of persons across internal borders within the Schengen area.

Increasing and evolving serious and organised crime

The 2021 **Serious and organised Crime Threat Assessment (SOCTA) 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.[9] Information compiled by Europol in the 2021 SOCTA also indicates that there is a growing threat from cyber-dependent crime – both in terms of the number and sophistication of attacks.

Perhaps more importantly in relation to the future need for law enforcement cooperation, the **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".[10]

The way in which the COVID-19 pandemic has been exploited by OCGs demonstrates the inherently adaptive and flexible nature of SOC. As the SOCTA points out – and as highlighted in the 2021 Council Conclusions[11] – in the COVID-19 crisis OCGs were quick to change their *modi operandi* to exploit opportunities in the dynamic and uncertain environment, targeting individual citizens, businesses and the public sector by, for example, distributing counterfeit and substandard personal protective equipment or performing phishing campaigns and ransomware attacks on healthcare organisations.[12]

The evolving nature of OCGs and 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, Annex III),[13] which makes them difficult to disrupt and

[7] 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).
[8] 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.
[9] Europol (2021) Serious and organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.
[10] Ibid, p. 28.
[11] 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.
[12] 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.
[13] Europol (2021) Serious and organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.

dismantle, and which means **that these groups are more able to flex and adapt to exploit new opportunitites**. For this reason, the 2021 SOCTA[14] 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.[15] 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.[16] 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.

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.[17] Annual revenues from nine main criminal markets[18] in the EU were estimated at between EUR 92 billion and EUR 188 billion in 2019[19] – between 0.7%-1.4% of the EU27 Gross Domestic Product (GDP) (Table 1, Annex III).[20]

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 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.[21] organised crime also undermines personal and state security, and threatens safety, stability and development - at the individual, local, national and transnational levels.[22]

Organised crime also results in direct costs to citizens' health and security.[23] For example, in relation to Trafficking in Human Beings (THB), victims (including children) are recruited into sexual exploitation and forced labour.[24] 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.[25].

[14] Europol (2021) Serious and organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.
[15] Europol (2021) Serious and organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.
[16] Europol (2015) *Exploring Tomorrow's organised Crime*. The Hague: Europol.
[17] 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.
[18] Illicit drugs, THB, Smuggling of migrants, Fraud, Environmental crime, Illicit firearms, Illicit tobacco, Cybercrime, organised property crime.
[19] RAND Europe & EY for the EC (2021) Mapping the risk of serious and organised crime infiltrating legitimate businesses.
[20] The EU GDP was EUR 13,900 billion in 2019. Eurostat (2020) *Which EU Countries had the highest GDP in 2019?* link.
[21] Europol (2021) Serious and organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.
[22] UNODC and UNICRI (2005) Trends in Crime and Justice: The evolving challenge of transnational organised crime, 25–54.
[23] RAND Europe & EY for the EC (2021) Mapping the risk of serious and organised crime infiltrating legitimate businesses.
[24] RAND Europe & EY for the EC (2021) Mapping the risk of serious and organised crime infiltrating legitimate businesses.
[25] 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.

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 Art. 25 and 28 of the Schengen Border Code[26], 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 Corona virus – which was thus by far the most common reason given.

The Commission has, on several occasions[27], stressed that improved law enforcement and the use of police checks is a preferred compensatory measure to internal border control.

2.2.2 High-level problem 2: Additional challenges for the prevention and fight against all forms of criminal and safety threats

By enabling the free movement of 420 million people, the Schengen area constitutes one of the largest free travel areas in the world.[28] The growing intra-EU mobility 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 discussed below.

EU mobility for work and leisure is increasing

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.[29] 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.[30] 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.[31] There has also been an increase in the number of EU citizens travelling for educational or training purposes.[32] 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.[33] Similarly, at SACs/EU air borders, Frontex estimated that there is an increase in passenger flows of about 5% per year across Europe.[34] Despite that the COVID-19 pandemic has reduced pan-European mobility in 2020 and 2021, the flows of persons will likely continue to increase in importance again in the near future.

[26] 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.
[27] COMMISSION RECOMMENDATION of 12.5.2017 on proportionate police checks and police cooperation in the Schengen area C(2017) 3349 final.
[28] European Commission (2021), A strategy towards a fully functioning and resilient Schengen area. Brussels: European Commission. Available at link.
[29] European Commission (2017) Boosting Growth and cohesion in EU border regions. Brussels: European Commission. Available at link .
[30] Eurostat (2020). *People on the move – statistics on mobility in Europe.* As of 8 April 2021: Available at link, p. 26.
[31] Eurostat (2020). *People on the move – statistics on mobility in Europe.* As of 8 April 2021. Available at: link, p. 28.
[32] European Commission. 2020. *Erasmus+ Annual Report 2019*. Luxembourg: Publications Office of the European Union. As of 8 April 2021: link, p. 32.
[33] Eurostat (2020) *EU citizens living in another Member State - statistical overview.* As of 8 April 2021: link.
[34] Frontex (2020) *Risk analysis for 2020*. Luxembourg: Publications Office of the European Union, p. 36.

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

Specifically at border regions, cooperation is needed, for example, to undertake transport control,[35] detain or pursue suspects crossing borders (travelling by car[36] or on public transport such as trains,[37] for example) and search for missing persons.[38] There is a need for law enforcement officials to be able to conduct "normal" and policing activities around and across borders regions.[39]

In addition to border regions, cooperation is needed in relation to **demonstrations** attended by international participants, **state visits and summits**, the protection of VIPs,[40] and **sports and music events** with international audiences.[41] As illustrated by one survey respondent, 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".[42] The need for cooperation is thus an important part of the security policy at mass events.[43] The **need to manage the pandemic** is another issue, which has created an increased need for cooperation at the border over the last year,[44] 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.

Current law enforcement cooperation for public safety could be improved

The survey respondents expressed mixed views about whether the risks to public safety are increasing.[45] However, as outlined above, the need for cooperation was confirmed and clearly identified. Mass gatherings and public places remain a key target for terrorist attacks[46] - highlighting the threat to public safety and the need for continued cooperation.

Moreover, the survey results and workshops highlighted some specific areas where there is scope for improvement to cross-border cooperation. This includes the use of **joint patrols** at border regions.[47] While recognised as good practice,[48] there is evidence that they are under-used.[49] One survey respondent explained that "proper cooperation in border regions requires joint scenario planning and exercises, and crisis management training."[50]

Ideally, in the case of large sporting events that bring together spectators from many countries, there should be **law enforcement cooperation in advance** (to share intelligence about planned offences or high risk subjects), **during** (to provide additional resources and bring national know-how), and **after** (to respond to any offences committed). However, this is not always the case. 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.[51]

---

[35] Focus Group on FR-CH bilateral agreement.
[36] Focus Group on DE-CZ bilateral agreement.
[37] Focus Group on Benelux trilateral agreement.
[38] Survey: Q 92, 1 representative from a PCCC.
[39] Focus Group on Benelux trilateral agreement.
[40] 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.
[41] Survey: Q 13A, 2 representatives from public order departments/NFIP and 1 representative from a SPOC.
[42] Survey: Q 92, 1 representative from a public order department/NFIP.
[43] Council Document 13887/20 - Manual on cross-border operations. Available at: link.
[44] Survey: Q 13A, 1 representative from a PCCC and one representative from a specialised investigative Unit; Q 92, 1 representative from a SPOC.
[45] Survey: Q 11, the proportion of LEAs' respondents answering "not at all" or "to a small extent" in relation to the increase in the following public order threats was: flows of people for tourism 49% (n=25); flows of people for work 48% (n=24); international events 67% (n=36).
[46] Europol. 2020. EU Terrorism Situation and Trend Report.
[47] Council Document 13887/20 - Manual on cross-border operations. Available at: link.
[48] Council Document 13887/20 - Manual on cross-border operations. Available at: link.
[49] Technical workshop held on 24 March.
[50] Survey: Q 92, 1 representative from a specialised investigative Unit and 1 representative from a SPOC.
[51] 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). Available at: link.

Information sharing – especially in relation to day-to-day rapid sharing of information at borders – could also be improved.[52] This includes difficulties in the exchange of information or personal data for minor offences, which might lead to improper risk assessment for public order and sport events.[53] Besides a need for better access to databases, survey participants pointed out that information systems for exchanging data and sharing of information of different Member States should be more interoperable and communicate with each other.

2.2.3 The EU dimension of the problems

Cross-border crime is, by definition, an international issue. **Most European countries agree that organised crime is a problem in their country**.[54] SOC in the EU involves criminals of over 180 nationalities, but 60% of the suspects of crime in 2017 were nationals of EU Member States.[55]

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 exchanges.[56] The steady increase in cross-border passenger and freight traffic means that only selective border controls are possible.[57] Within the Schengen area, internal border controls have been dismantled, meaning that travel and communication within the EU has become easier.[58] **Technological advancements have created opportunities for new types of cross-border crime,** as well as for modernising traditional forms of crime.[59] For example, the illicit drugs market has become increasingly global and makes use of digital technologies, such as selling drugs online.[60] 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.[61]

There is also a clear EU dimension to the issues related to effective policing, **as 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 SAC**, meaning that effective preventive and responsive actions need to involve cross-border cooperation.

With the creation of the Schengen area, countries agreed to work together to sustain European internal security.[62] The COVID-19 pandemic has illustrated how important cross-border cooperation is in times of crisis. During the pandemic, some countries implemented border controls in an attempt to prevent the spread of the Corona virus.[63] The increased use of borders between Member States is not in line with the objective of the European Commission's 2021 *Strategy towards a fully functioning and resilient Schengen area,* which aims to reduce the use

[52] Survey: Q 92, 1 representative from a specialised investigative Unit and 1 representative from a SPOC commented "Information exchange should be speeded up for the benefit of officials on the street".
[53] Technical workshop held on 24 March.
[54] 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.
[55] Europol (2017) Serious and organised Crime Threat Assessment (SOCTA): Crime in the age of technology, European Union.
[56] 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.
[57] Wagner J. (2021) Transnational organised Crime (TOC). In: Border Management in Transformation. Advanced Sciences and Technologies for Security Applications. Springer, Cham. Available at: link.
[58] 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. Available at: link.
[59] Grabosky, P. (2013) Organised Crime and the Internet, The RUSI Journal, 158:5, 18-25, DOI: 10.1080/03071847.2013.847707.
[60] Spapens, T. (2015) Transnational organised crime. *International Encyclopedia of the Social & Behavioral Sciences (Second Edition),* pp. 596-601. Available at: link.
[61] Peter Grabosky (2013) organised Crime and the Internet, The RUSI Journal, 158:5, 18-25, DOI: 10.1080/03071847.2013.847707.
[62] European Commission (2021), A strategy towards a fully functioning and resilient Schengen area. Brussels: European Commission. Available at link.
[63] European Commission (2021), A strategy towards a fully functioning and resilient Schengen area. Brussels: European Commission. Available at link.

of borders between the Member States.[64] To achieve this objective, it is imperative that internal security within the Schengen area is sustained. Effective cross-border law enforcement cooperation that ensures the security of its citizens is crucial for achieving this objective.

2.2.4 The evolution of the problems

Serious and OCGs, 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 serious and OCGs and LEAs.** Criminals are, indeed, dynamic and quick to exploit the latest technological developments. As they manage to quickly adopt and integrate new emerging technologies into their *modus operandi*, serious and OCGs are able to ensure business continuity and can further expand their criminal activities.[65] 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.

Below we illustrate how specific developments are expected to affect the evolution of SOC and situations critical to public order and safety in the next five to ten years.[66]

As concerns SOC, the criminal use of technological developments varies depending on the specific crime area. In the following, illustrative examples in three crime areas[67] 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 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

[64] European Commission (2021), A strategy towards a fully functioning and resilient Schengen area. Brussels: European Commission. Available at link.
[65] Europol (2017) Serious and organised crime threat assessment. Available at link.
[66] For further details on the evolution of the problems please see supporting information in Annex III. This Annex includes (i) a detailed section about key relevant social and technological developments, including a matrix on the expected impacts of social and technological developments on SOC and situations critical to public order and safety, (ii) a detailed section on the expected impacts on SOC, including a table on the expected impact of social and technological developments per crime area and (iii) a detailed section on the expected impacts on public order and safety.
[67] 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.

recovery funds, which some Member States established to stabilise their economies.[68] In Germany, for instance, around 25,000 suspected cases of coronavirus aid fraud were investigated in spring 2021.[69]

- **Drug trafficking:** Apart from small disruptions during the first lockdown, the drug trafficking has continued as usual.[70] 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.[71] For instance, encrypted software based on Pretty Good Privacy and commercial encryption are commonly used among drug sellers and buyers.[72] 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.[73] At the same time, **the national markets are increasingly interconnected** both within the EU and with the rest of the world.[74] 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.[75] 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 and riot at football matches.[76] 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.[77] 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.[78] 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 databases and IT systems, but also the frequencies or frequency ranges of radio communication in place.[79]

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.[80] As regards cross-border labour mobility, two million out of 190 million employed persons lived and worked outside their home Member State in 2020[81], and this number has also been

[68] Europol (2021) Serious and organised Crime Threat Assessment: A corrupting influence, European Union.
[69] Deutsche Welle (2021) COVID aid: Germany uncovers over 25,000 cases of fraud. Available at link
[70] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[71] EMCDDA (2021) European Drug Report 2021. Trends and Developments. Available at link.
[72] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[73] Eurostat (2021) Gross domestic product at market prices. Available at link.
[74] Eurostat (2021) Extra-EU imports of main CPA groups, 2015-2019. Available at link.
[75] Europol/European Monitoring Centre for Drugs and Drug Addiction (2019) EU Drug Markets Report 2019. Available at link.
[76] BBC News (2016) Euro 2016: Who is to blame for the Marseille violence. Available at link.
[77] BBC News (2015) Paris attacks: What happened on the night. Available at link.
[78] EU Commission (2020) A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond. Available at link.
[79] Technical workshop held on 24 March 2021.
[80] 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.
[81] Eurostat (2021) People on the move. Available at link.

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.[82] 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.[83] 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.

2.3 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 in section 2.2 concerning the high-level problems, 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.

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 the three main areas of analysis of this study, namely (i) information exchange, (ii) public order and safety, and (iii) fight against SOC. 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.

2.3.1 Core problem 1: The access to and exchange of necessary information among law enforcement authorities is subject to legal, technical and structural challenges

LEAs are involved in frequent cross-border information exchanges related to operations against SOC,[84] **as well as for the purpose of ensuring public order and safety.**[85] Despite the high frequency of such exchanges, several drivers and issues have been identified as hampering their overall effectiveness and efficiency.

[82] Eurostat (2021) Nights spent at tourist accommodation establishments – monthly data. Available at link.
[83] BBC News (2021) Swindon railway station as gateway for drug trafficking. Available at link.
[84] 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).
[85] Survey: Q 32, 65% (n=32) of LEAs respondents reported information sharing took place always or very frequently in relation to events, 59% (n=25) in relation to crisis and disasters and 46% (n=17) in relation to the protection of public figures.

Table 4 - 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 • Language barriers hamper the efficient cross-border exchange of information

Source: Author's own elaboration

Legal driver: Law enforcement authorities face difficulties in interpreting and implementing relevant EU provisions

The scope of some EU measures is unclear and law enforcement authorities face difficulties in interpreting and implementing relevant EU provisions

The fragmentation of the EU legislative framework has led to uncertainties as regards the use of the proper legal basis.[86]

[86] Schengen evaluation reports: C3, C6, C17, C19, C24, C27, C28. Survey: Q41, 62% (n=44) of LEAs respondents reported that cross border law enforcement cooperation through platforms such as SIENA, SIS, EIS and Interpol is hampered by 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 SACs regarding the implementation of relevant EU provisions, Q42, 1 representative from a SPOC and 2 customs' representatives; Q 64, 1 NEC. Technical workshop held on 24 March.

More specifically:

- **SFD and CISA**. Stakeholders from some Member States indicated that the different scope of the SFD and the CISA (respectively "conducting criminal intelligence operations" and "preventing and detecting criminal offences") is not always clear.[87] The wording used in the two pieces of legislation makes it unclear if and to what extent the CISA (Art. 39 and 46) is still applicable. As a consequence, both measures are used by practitioners, despite that the SFD was expected to replace the CISA as the key legal basis for information sharing relevant to law enforcement cooperation. Practitioners who were used to refer to the SFD in the past still refer to a great extent to Art. 39 CISA.[88] This results in a limited contribution of the SFD towards simplification and streamlining of the EU framework, questioning the need to have two pieces of legislation (the SFD and the CISA) instead on just one piece of legislation with a broader and more comprehensive scope. This was confirmed also by stakeholders consulted,[89] who argued that in most countries the SFD is hardly used, as the availability of many options for cooperation or information exchange limits its added value, and it overlaps with CISA, with many articles worded in a similar way.
- **SFD and the Naples II Convention**. The analysis of these EU measures, including a legal and operational assessment, showed that although customs authorities usually refer to the Naples II Convention and police authorities to the SFD, this does not apply to all EU Member States and SAC. This means that, depending on how the country has implemented the two pieces of legislation, the same type of LEA can exchange information according to different rules and procedures.

There is no requirement to ensure that a common minimum set of data is made available for exchange

The SFD does not include any requirement to ensure that a common minimum set of data is made available for exchange. Hence the type of data exchanged vary significantly across countries. For instance, while information on criminal activities, wanted or missing persons, and stolen vehicles are exchanged by most Member States, only in few cases exchanged information includes documentation of phone tapping, room bugging, covert and video surveillance operations. The lack of common requirements about minimum data to be exchanges implies that the information received often includes details and data that are not necessary to address the specific request they sent. In other instances, specific data that would be needed is not included in the data exchange. This results in unnecessary time to process all answers to the same request.

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

The deadlines provided for in the SFD to address urgent requests for information are usually not met when a judicial authorisation is required to deliver the requested information.[90] Indeed, the more the authorities concerned, the more procedural steps have to be followed, hence the need for additional time to cope with all procedures. The issue has been also pointed out by three representatives from national judicial authorities who reported that the EU legal basis for information exchange in law enforcement cooperation is complex, creating burdensome, laborious and not to clear processes to be followed.[91] This issue is further exacerbated by the fact that what is regarded as an information request for police staff in one country might be regarded as an information request for judicial authorities in another country. Hence, different authorities may be concerned depending on the specific national institutional framework, further undermining the overall efficiency of the process.[92] This issue is particularly challenging since

[87] Schengen evaluation reports: C3, C6, C17, C19, C24, C27, C28. Survey: Q42, 1 representative from a SPOC; Q 64, 1 NEC.
[88] Huybreghts, G. (2015). The Schengen Convention and the Schengen acquis: 25 years of evolution. ERA Forum. 16. 10.1007/s12027-015-0402-3. Available at: link.
[89] Interview: 1 SPOC's representative.
[90] Survey: Q 16, 1 representative from a SPOC; Q 66, 1 customs' representative. Council Document 14755/1/12, Swedish Framework decision (SFD) implementation - Assessment of compliance pursuant to Article 1(2): BG, CY, EL, ES, FR, IT, LT, PL, PT, SI, SK.
[91] Survey: Q 15, 3 national judicial authorities' representatives.
[92] Huybreghts, G. (2015). The Schengen Convention and the Schengen acquis: 25 years of evolution. ERA Forum. 16. 10.1007/s12027-015-0402-3.

there is no obligation to have a judicial authority available 24/7 within the SPOCs, thereby slowing down the judicial authorisation process, where it is 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 distinction between "urgent cases", "non-urgent cases" and "all other cases" of requests for information is unclear and would benefit from clarification. Guidelines on the implementation of the SFD[93] provide details for the identification of "urgent cases", however, no definition of "not urgent" and "other cases" is provided. Non-urgent cases are therefore deductively identified as those not fitting the "urgency criteria". Such a "negative" deductive process takes time, hence the need to simplify the distinction between "urgent cases", "non-urgent cases" and "all other cases".

Moreover, **the forms for submitting and requesting information** included in the SFD are rarely used.[94] The forms are considered time-consuming and labour intensive, and the Member States prefer a free-text exchange of messages.[95] Hence, although the SFD forms were expected to boost a standardised and efficient exchange of information, their limited use results in a limited added value of this instrument in terms of harmonisation of communication procedures.

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). 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 conditions that are in accordance with its national law on their use by the receiving competent law enforcement authority.

Technical driver: Law enforcement authorities have 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 a common dashboard and automatic/semi-automatic data upload and cross-check)

The SPOCs often face 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.[96] For instance, some SPOCs have limited access to relevant national databases.[97] Since they cannot access directly the databases of other law enforcement units, they need to ask officials within those departments to collect and share the information. This delays the overall exchange process.[98] 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 interoperability between national law enforcement databases.[99]

[93] Council Document 13034/14 - Guidelines on the implementation of SFD. Available at: link.
[94] Schengen evaluation reports: C1, C31, C3, C4, C8, C19, C12, C13, C16, C17, C24, C25, C30, C27, C28. Technical workshop held on 24 March.
[95] Council Document 14755/1/12, Swedish Framework decision (SFD) implementation - Assessment of compliance pursuant to Article 11(2): BG, HU, LT, LV. Available at: link. Technical workshop held on 24 March.
[96] Schengen evaluation reports: C1, C3, C4, C15, C18, C20, C21, C23, C25, C29.
[97] Schengen evaluation reports: C10, C11, C12, C25. Commission Staff Working Document Accompanying the document Report from the Commission to the Council and the European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanism pursuant to Article 22 of Council Regulation (EU) No 1053/2013 First Multiannual Evaluation Programme (2015-2019) SWD/2020/327 final. Available at: link.
[98] Council Document 14755/1/12.
[99] Schengen evaluation reports: C5, C6, C8, C9, C10, C11, C12, C13, C15, C18, C19, C20, C25, C27, C28, C29. Technical workshop held on 24 March. Commission Staff Working Document Accompanying the document Report from the Commission to the Council and the European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanism pursuant to Article 22 of Council Regulation (EU) No 1053/2013 First Multiannual Evaluation Programme (2015-2019) SWD/2020/327 final. Available at: link.

Differences between SPOCs and PCCCs in the Member States

The national organisational set-ups of SPOCs and PCCCs differ between Member States, both in relation to their responsibilities and tasks. While in some Member States, SPOCs and PCCCs are set up very similarly and are, in practice, "interchangeable", the setup in other Member States provides SPOCs and PCCCs each with unique functions.

In this respect, for instance, one Member State clarified that the national SPOC is only a competent authority, but in PCCCs several competent authorities act within the scope of their tasks. A PCCC is in this country not a unitary authority or department. PCCCs are responsible for the information exchange and support activities in their respective border areas. The PCCCs are not so-called "field offices" or outsourced cells of the central office (SPOC), but specialised bodies to support the information exchange between the relevant agencies at the border.

PCCCs typically act as "transmission service providers" for other local or regional bodies. This means that they process and transmit relevant data from the border region to the responsible unit within their country. Their tasks include cross-checking relevant data with international information systems, documenting processes, collecting data and inserting them into the national police information network.

Therefore, in this particular country, SPOCs and PCCCs are fundamentally diverging from each other in terms of their responsibilities.

However, as this study seeks to inform solutions from an EU perspective, a certain degree of abstraction from national specificities has been used in order to provide the Commission with the necessary information at the necessary level of detail and granularity.

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

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**[100] **techniques and "fuzzy logic"**[101] **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.

Law enforcement officials on the ground do not always use secure communication means

Finally, as also pointed out by some stakeholders, the exchange of information on the ground is hindered by a **lack of common standards to exchange information in a secure way**.[102] The importance of ensuring secure exchange of information emerged as particularly relevant in the context of the COVID-19 pandemic and in relation to the increasing use of communication tools, such as video calls, which often do not ensure high security standards. Secure and interoperable channels of communication were also found to be lacking when considering the PCCCs.[103] In this regard, the limited use of the SIENA system contributes towards risks of unauthorised access to data, leaks, abuses of communication tools and unsecure exchange of sensitive and restricted information.[104]

Moreover, as part of hot pursuits, for instance, officials have reported that national radio communication systems are interoperable only to a limited extent. In practice this can lead to

[100] Transliteration is the process of representing words/names from one language using the alphabet or writing system of another language (multilingual name recognition). The relevant sources considered for this issue are the Schengen evaluation reports: C3, C6, C10, C16, C24, C27, C28, C30.
[101] A fuzzy database is a database which is able to deal with uncertain or incomplete information using fuzzy logic. Fuzzy Logic (FL) is a method of reasoning that resembles human reasoning. The approach of FL imitates the way of decision making in humans that involves all intermediate possibilities between digital values YES and NO. The relevant sources considered for this issue are the Schengen evaluation reports: C3, C6, C9, C15, C17, C19, C24, C27, C29, C30.
[102] Council Document 13083/1/20, 24 November 2020, available at: link. Council Document 8014/1/21, 26 April 2021 (LIMITE). Council Document 10313/20, 4 September 2020 (LIMITE). Schengen Evaluation reports: C5, C15, C30. Technical workshop held on 24 March.
[103] Commission Staff Working Document Accompanying the document Report from the Commission to the Council and the European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanism pursuant to Article 22 of Council Regulation (EU) No 1053/2013 First Multiannual Evaluation Programme (2015-2019) SWD/2020/327 final. Available at: link.
[104] Council Document 5503/21, 28 January 2021. (LIMITE).

situations in which officials from one Member State cross the border to another Member State as part of a hot pursuit, but loose the radio connection to their operations centre. In the worst case scenario, this leads to a higher likelihood of suspects being able to lose police forces.

Structural driver: National and regional information hubs set up by LEAs have different roles, means and capabilities which make their cooperation sub-optimal. LEAs have insufficient knowledge of existing mechanisms and skill gaps

SPOCs/PCCCs do not always play their coordination role and lack resources to face the increasing number of requests

SPOCs do not always play their coordination role and lack resources to face the increasing number of information requests.[105] Member States and SACs are free to decide which law enforcement units and departments are represented within their SPOCs. Hence, although different manuals and national factsheets have been produced in order to facilitate a harmonised approach to the way national SPOCs are organised,[106] there are still significant differences across countries.[107] 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 some confusion when it comes to the cross-border exchange of information, also considering that there is not available information about how the SPOCs are structured in different countries.[108] Thus, when a request for information is addressed to a specific unit, the requesting Member State does not know in advance whether this unit 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 unit. Moreover, SPOCs face a high workload due to the practice of "fishing" and difficulties in the choice of the most appropriate communication channels used to exchange information with SPOCs.[109]

Moreover, the SPOCs – and in some cases also the PCCCs[110] - lack resources to timely and effectively address the increasing number of requests they receive.[111] The increasing amount of information requests has not been accompanied by a proportionate increase of the resources allocated to manage these requests.[112] The lack of sufficient resources allocated to the SPOCs is particularly challenging in cases of urgent requests for information.[113] Pursuant to Article 4 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.[114]

---

[105] Schengen evaluation reports: C8, C9, C18, C21, C25, C28, C31. Interviews: 1 EMPACT Driver. Technical workshop held on 24 March.

[106] Council Document 10492/14, Draft Guidelines for a Single Point of Contact (SPOC) for international law enforcement information exchange; Council Document 12093/19, Draft Council Conclusions on establishing a 'Heads of SPOC'-network – Adoption; Council Document 5825/20 ADD 1 REV 1, Manual on Law Enforcement Information Exchange.

[107] There are even some countries where the SPOC has not been established or has limited functioning. According to their Schengen evaluation reports, C8, C9 and C31 do not to have a SPOC in place, while, in C25, the SPOC is still not operational. Interviews: 1 EMPACT Driver.

[108] Interview with a SPOC representative. Survey: Q 45, 1 representative from a SPOC.

[109] "Fishing" is the practice used in SIENA for which Country A sends a request to Country B with a copy to all Member States). Such requests must be answered, which creates a need for resources that is not proportionate to the added value of the request. Written contribution from a Commission's representative. Interviews: 1 EMPACT Driver and 1 SPOC's representative. Technical workshop held on 24 March.

[110] Council document 14623/17, 27 November 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).

[111] Schengen evaluation reports: C6, C11, C16, C15, C27. ICMPD (2010) Study on the status of information exchange amongst LEAs in the context of existing EU instruments. Available at: link. Survey: Q 42, 1 representative from a specialised investigation unit. Interview: 1 representative from a PCCC.

[112] Comparative analysis of the Schengen evaluation reports.

[113] Schengen evaluation reports: C3, C5, C6, C20, C21. Technical workshop held on 24 March.

[114] 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

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

In some Member States **there is no integration of information included in databases owned by the different law enforcement units**, which form part of the same SPOC and/or the PCCC. The lack of integration of information collected and stored by different LEAs results in a risk of duplications of both uploads and searches of information, hence reducing the overall efficiency of information exchange.[115]

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.

An additional issue hampering a smooth cross-border exchange of information is that **the SPOCs and the PCCs 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,[116] thus hampering cross-border law enforcement cooperation overall.[117] In particular, some stakeholders from SACs pointed to the limited access of the SPOCs to the Europol Information System (EIS) and underlined that this could represent a serious threat to EU security.[118] Indeed, the limited access to the EIS might result in criminals or terrorists entering the country and then moving freely across Europe without any further check. As regards the PCCCs, out of 59 PCCCs active in Europe in 2017, only nine were connected to SIENA.[119] Besides the PCCCs, this consideration also applies to LEAs' regional and local offices that most of the times do not have access to SIENA.[120]

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 and SACs 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 on how to use them.[121]

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

Moreover, currently, **training about cross-border law enforcement cooperation is not held on a regular basis at the 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).[122] In practice, this implies that training for staff involved

response time to requests sent via these platforms hamper cross-border law enforcement cooperation.

[115] Schengen evaluation reports: C3, C18, C19, C20, C21, C25, C23, C29, C30. 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 (November 2020). Survey: Q 29, 34% (n=38) of LEAs respondents pointed out that the lack of coordination between SPOCs and PCCCs hampers cross-border law enforcement cooperation.

[116] Schengen evaluation reports: C23, C3, C4, C6, C8, C9, C10, C11, C19, C12, C13, C16, C17, C18, C15, C20, C24, C25, C27, C28. Survey: Q 44, 71% (n=101) of LEA respondents reported that access to SIENA, SIS/SIRENE, EIS, and Interpol exchange channels and databases differs between countries to a moderate, high degree, or very high degree. Technical workshop held on 24 March 2021.

[117] 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, EIS 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.

[118] Interviews: 1 SAC's representative. 2 SACs' representatives at the Technical workshop held on 24 March.

[119] Council document 14629/17, 27 November 2017 - State of play of the roll-out of SIENA regarding PCCCs - Outcome of questionnaire. (LIMITE).

[120] Schengen evaluation reports: C23, C5, C6, C8, C9, C10, C11, C19, C12, C13, C16, C18, C15, C20, C25, C30, C31. Interviews: 2 EU Agency representatives. Four Member States' representatives at the Technical Workshop held on 24 March. EY, RAND (2020) Evaluation Study on the EU Policy Cycle for organised and serious international crime/EMPACT 2018-2021. (Unpublished).

[121] Schengen evaluation reports: C3, C4, C5, C6, C8, C9, C10, C11, C12, C13, C15, C16, C17, C18, C19, C20, C21, C24, C25, C30, C27, C28, C29, C30, C31. Technical workshop held on 24 March. Survey: Q 30, 1 representative from a SPOC and 2 representatives from specialised investigative units.

[122] Schengen evaluation reports: C4, C6, C9, C16, C17, C18, C19, C24, C31. Survey: Q 59, 58% (n=67) of LEAs

in cross-border cooperation often is 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.[123] Moreover, this training is often voluntary, thus leaving room for heterogeneous skills between police officials, and they are not always addressed at newcomers in the SPOCs and PCCCs.[124]

The choice of channel for information exchange lies with the Member States, leading to a duplication of requests in some cases

The limited training contributes towards some difficulties faced by national law enforcement officials as regards the use of available tools for exchanging information. **The choice of the tool that is used for information exchange is currently left to the Member States and this leads to a risk of duplications of requests, creating additional confusion** due to the number of information systems that can be used.[125] For instance, most countries use both the Secure Information Exchange Network Application (SIENA) (Europol) and I-24/7 (Interpol) and there is not a clear rationale behind the choice of one tool instead of the other.[126] Although the analysis did not find any overlaps or inconsistencies between the relevant EU measures, the availability of a high number of different communication tools does not meet the need to ensure smooth and quick information sharing, particularly when it comes to urgent requests for information.

Language barriers hamper the efficient cross-border exchange of information

Finally, **language barriers were reported by some Member States and SACs** as hampering the cross-border exchange of information.[127] Officials engaged in cross-border cooperation are not always proficient in English and this has a twofold drawback. First, since EU official communication channels 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, fax, etc.). Second, even when official channels are used, information is often reported in a "rusty" English, which is difficult to understand. Thus, officials receiving a request for information often need to take time to translate it.

2.3.2 Core problem 2: The growing intra-EU mobility is not met with an adequate development of tailored joint operations

There is a vital need for cross-border cooperation in relation to day-to-day law enforcement. Key existing instruments for cross-border operational law enforcement cooperation include joint police patrols, joint units, joint offices, and operation points in border areas.[128]

Despite the existence of specific EU measures aimed at regulating their use, **joint patrols are underused.**[129] Besides joint patrols, **also mutual assistance during large-scale events has proved to be limited**. Four main drivers contribute towards an insufficient deployment of joint operations, which would be needed to face the growing intra-EU mobility.

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.

[123] Report from the Commission to the Council and the European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanism pursuant to Article 22 of Council Regulation (EU) No 1053/2013 First Multiannual Evaluation Programme (2015-2019) COM/2020/779 final. Available at: link.

[124] Schengen evaluation reports: C3, C6, C9, C10, C19, C27, C28.

[125] Schengen evaluation reports: C28. Technical workshop held on 24 March 2021. Interviews: 2 SPOCs' representatives. Survey: Q 2 SPOC's representatives and 1 PCCC representative, 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.

[126] 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 Interpol used to a high o very high extent (Interpol: 52%, n=87).

[127] Schengen evaluation reports: C3, C8, C9, C11, C12, C13, C17, C19, C23, C24, C28, C29. Survey: Q 34, 35 LEAs' representatives reported that language barriers are among the main issues they face when sharing information.

[128] Council of the European Union (2020) Enhancing cross-border law enforcement cooperation: Best practices, current challenges and way forward. Brussels: Council of the European Union. Available at link.

[129] Schengen evaluation reports: C10, C12, C18, C20, C29, C30. Technical workshop held on 24 March.

Table 5 - Overview of the drivers and issues behind core problem #2

Key drivers behind Core Problem 2 - The growing intra-EU mobility is not met with an adequate development of tailored joint operations	
Legal driver	There is a limited and at times asymmetric conferral of executive powers of law enforcement officials operating in the respective host States, as well as limited awareness of these powers on the ground
Technical driver	Officials on the ground have limited remote access to relevant law enforcement databases
Structural drivers	National law enforcement authorities have limited financial and human resources to expand the use of joint operations
	Cooperation between law enforcement authorities in different countries, e.g. for the purpose of joint operations notably in border regions, is insufficiently informed by joint threat assessment/risk analysis: • National specialised analytical departments rarely cooperate with similar departments in other countries to design actionable joint cross-border threat assessments/risk analysis • There is limited integration of police and customs information and analysis

Source: Author's own elaboration

Legal driver: There is a limited and at times asymmetric conferral of executive powers of law enforcement officials operating in the respective host States, as well as limited awareness of these powers on the ground

Police officials do not have operational powers in another Member State (unless such possibility is conferred by the host Member State to the seconding Member States' or SACs' officials involved in joint operations), thus foreign officials are in practice often more of an accompanying than an operational colleague.[130] Indeed, pursuant to the Prüm Decisions, officials, specialists and advisers sent by one Member State to another one to prevent criminal offences and maintain public order and security (i.e. mutual assistance) should behave in accordance with the law of the receiving Member State and under the guidance and in the presence of its officials. Similarly, the CISA provides that officials must comply with the law of the Contracting Party in whose territory they are operating and obey the instructions of the competent local authorities.

The Council[131] has pointed out that the **limited executive powers** of police officials operating in the respective host States is **one of the main issues contributing to the limited use of joint patrols**. These restrictions are further exacerbated by the limited awareness of law enforcement officials about the executive powers conferred by different Member States. Notably, officials face the same uncertainties as regards the type of operations and activities that police authorities are entitled to carry out in the territory of another Member State, as well in relation to their executive powers when implementing such operations. Indeed, Member States are left with flexibility when it comes to the deployment of joint operations. Pursuant to the Prüm Decisions, Member States are free to define the scope, subject and conditions of joint operations and to decide whether such operations shall be carried out at all. Moreover, there are no clear EU provisions concerning the types of activities which can be carried out by officials posted abroad. In this regard, and specifically in relation to cross-border surveillance, CISA stipulates only what officials are *not* entitled to do (they are neither authorised to enter into private homes and places not accessible to the public nor arrest the person under surveillance). The lack of clear and harmonised criteria for carrying out joint operations raises some uncertainties for law enforcement officials operating in another territory in relation to the activities they are allowed to implement and how they can implement them.

[130] Article 17 (2) of Council Decision 2008/615. Technical workshop held on 24 March.
[131] Council Document 10313/20, 4 September 2020. Enhancing cross-border law enforcement cooperation: Best practices, current challenges and way forward. (LIMITE). Technical workshop held on 24 March.

Technical driver: Officials on the ground have limited remote access to relevant law enforcement databases

The **access to law enforcement databases through mobile devices is limited.**[132] Information and communication tools currently used at the national level do not ensure that the information collected and stored by police forces is readily accessible by officials on the ground.[133] For example, prior to an international football match, supporters are often subject to screening procedures in order to collect relevant information about potential suspects likely to engage in public disorder actions. However, without direct access to the relevant law enforcement databases, police officials are not in a position to check if the person they are controlling has been responsible for acts of violence and public disorder in the past. It is therefore not possible to filter the "dangerous" supporters and preventing them to access the premises of a specific sport event.[134] Similarly, police officials are often called to patrol access points in a certain city/area, such as train stations, airports and main roads, prior to large mass events. If they could access the relevant databases from these locations, they would be able to quickly check if a person should be stopped.

Structural driver: National law enforcement authorities have limited financial and human resources to expand the use of joint operations

Pursuant to Art. 34 of the Prüm Decisions, each Member State shall bear the costs incurred by its own authorities in the implementation of the Decision.[135] Since available resources at the national level are limited, Member States engage in a relatively low number of joint operations.[136] Member States are reluctant to allocate resources to the deployment of joint operations, since these operations are perceived as too costly. The limited executive powers of foreign police officials contribute towards the perceived limited cost-effectiveness of joint patrols. Besides their limited operational role, the involvement of foreign officials is considered costly also for other reasons. Indeed, for safety reasons, at least two officials with executive powers and entitled to the use of force, are required to take part in a joint patrol.[137] This means that insofar as foreign officials cannot exercise executive powers, at least three officials (two local and one foreign) should form part of the patrol. This composition increases the resources needed and eventually reduces the overall cost-effectiveness of joint patrols compared to national patrols, which require a minimum of two officials. Moreover, in case of joint patrols involving officials from non-neighbouring countries, travel/accommodation costs for joint patrols represent an additional burden for national LEAs, making them reluctant to use this tool.[138]

[132] Schengen evaluation reports: C1, C3, C5, C6, C9, C10, C15, C18, C19, C24, C25, C27, C28, C29, C30, C31. 1 Member State's representative at the Technical workshop held on 24 March. Report from the Commission to the Council and the European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanism pursuant to Article 22 of Council Regulation (EU) No 1053/2013 First Multiannual Evaluation Programme (2015-2019) COM/2020/779 final. Available at: link.

[133] European Confederation of Police (EuroCOP) supporting Commission's initiative to streamline and consolidate existing instruments for cross-border police cooperation (November 2020) and Commission Staff Working Document Accompanying the document Report from the Commission to the Council and the European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanism pursuant to Article 22 of Council Regulation (EU) No 1053/2013 First Multiannual Evaluation Programme (2015-2019) SWD/2020/327 final. Available at: link.

[134] Tait R. (2019) Prague prepares for England fans' long weekend with 'anti-conflict units'. The Guardian. Available at: link.

[135] 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.

[136] Council Document 10062/19, 06 June 2019 - Council conclusions on certain aspects of European preventive policing.

[137] Council Document 10313/20, 8 September 2020. Enhancing cross-border law enforcement cooperation: Best practices, current challenges and way forward - analysis of current legal framework and outcomes of the Presidency questionnaire. (LIMITE).

[138] Council Document 10313/20, 4 September 2020. Enhancing cross border law enforcement cooperation: Best practices, current challenges and way forward. (LIMITE).

Structural driver: Cooperation between law enforcement authorities in different countries, e.g. for the purpose of joint operations notably in border regions, is insufficiently informed by joint threat assessment/risk analysis

National specialised analytical departments rarely cooperate with similar departments in other countries to design actionable joint cross-border threat assessments/risk analysis

Besides the costs referred to above, the limited use of joint patrols can also be linked to the existing limitations in the exchange of information between relevant LEAs. Indeed, there are only few cases of joint threat assessments and risk analysis at the national level, and similarly only few cases of cooperation between countries for the development of cross-border crime analysis/risk assessment analytical products.[139] The limited use of cross-border threat assessment/risk analysis leads to a fragmented and non-exhaustive intelligence picture of cross-border security threats.[140] This, in turn, might result in an underestimation of the actual challenges to public order and safety and eventually to the choice of not implementing joint patrols. As a consequence, the benefits related to the use of joint patrols are perceived as low and largely outweighed by the costs needed to implement them. This contributes to a lack of prioritisation of this tool and to a limited amount of resources allocated for its implementation.

The study identified two main factors which contribute to the limited development of common threat assessments. First, there is **limited cooperation between national specialised analytical departments**.[141] This issue was recently raised also by the Commission,[142] which pointed to the limited use of the Common Integrated Risk Analysis Model (CIRAM) towards the development of effective cross-border threat assessments.[143] Second, even when analytical information is exchanged across countries, it is often fragmented and not comprehensive due to the **limited exchange of information between national law enforcement agencies**, notably between customs and police authorities.[144] In most cases, risk analysis is produced separately by the different types LEAs,[145] and this negatively affects the possibility of planning and performing joint operations.[146]

There is limited integration of police and customs information and analysis

Besides the limited integration of police and customs data and information, threat assessments and risk analyses are usually not disseminated outside the specific law enforcement agency producing them. This further prevents the possibility to develop a relevant and comprehensive national threat picture and affects the ultimate effectiveness of the national response put in place to address the identified threats.[147]

---

[139] Council Document 10313/20, 8 September 2020. Enhancing cross-border law enforcement cooperation: Best practices, current challenges and way forward - analysis of current legal framework and outcomes of the Presidency questionnaire. (LIMITE): CH, CZ, EL, FI, IE, LV, NL. Written contribution from a representative from a national LEA attending the Technical workshop held on 24 March. Survey: Q 55, 4 representatives from specialised analytical departments.

[140] Survey: Q 53, 3 representatives from specialised analytical departments.

[141] Schengen evaluation reports: C1, C3, C6, C9, C11, C15, C18, C19, C24, C28, C31. Survey: Q 49, 62% (n=5) of LEAs' respondents replied that cross-border threat assessment/risk analysis are not shared with the neighbouring country(ies) in view of joint analytical documents. Q 47-48, 55% (n=12) of specialised analytical departments respondents reported to involve stakeholders from other countries for the development of cross-border threat assessments/risk analysis, including specialised analytical department counterparts (25% of total cases, n=10), PCCCs (22% of total cases, n=9), and SPOCs (20% of total cases, n=8). Q 49, 50% (n=12) of specialised analytical departments respondents declared to share threat assessments/risk analysis with the neighbouring country(ies) in view of joint analytical documents.

[142] Report from the Commission to the Council and the European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanism pursuant to Article 22 of Council Regulation (EU) No 1053/2013 First Multiannual Evaluation Programme (2015-2019) COM/2020/779 final. Available at: link.

[143] The CIRAM is a model aimed at providing framework of reference to assist Frontex and Member States in the preparation of risk analyses. It is aimed at disseminating a common understanding of risk analysis and enhancing coherence in the management of the external borders. Available at: link.

[144] Survey: Q 46, 36% (n=19) of respondents from specialised analytical departments reported to undertake cross-border threat assessment/risk analysis with customs, 32% (n=17) with police.

[145] Schengen evaluation reports: C1, C3, C4, C5, C6, C8, C9, C10, C11, C12, C13, C15, C17, C18, C19, C20, C21, C24, C25, C28, C30, C31. Survey: Q 44, only 22% (n=11) of LEAs' respondents reported to undertake threat assessment or risk analysis to plan joint operations/patrols.

[146] Schengen evaluation reports: C1, C3, C4, C5, C6, C8, C9, C10, C11, C12, C13, C15, C17, C18, C19, C20, C21, C24, C25, C28, C30, C31.

[147] Commission Staff Working Document Accompanying the document Report from the Commission to the Council and

2.3.3 Core problem 3: EU and national implementation rules hamper cross-border operational cooperation to fight SOC

Since OCGs do not respect jurisdictional boundaries, close **cooperation between police bodies is key to tackling these threats effectively**. As criminal activities continue to spread across jurisdictions and move and diversify online, joint operational capabilities and a consistent commitment to sharing information, expertise and resources among LEAs from different EU Member States and SACs (as well as actors in the private sector) are increasingly important in effectively tackling (new forms of) organised crime.[148]

Different measures have been established both at the EU and the national levels to increase cooperation and provide an adequate response to the current threats. However, **cross-border operational cooperation against SOC appears to be hampered by difficulties related to the cross-border use of investigative tools**. These difficulties are mainly caused by the current rules provided at the EU, regional and national levels, which are not fully relevant and consistent, and thus result in burdens and operational difficulties.

Table 6 - Overview of the drivers and issues behind core problem #3

Key drivers behind Core Problem 3 - EU and national implementation rules hamper cross-border operational cooperation for SOC	
Legal driver	Rules concerning investigative tools vary between the Member States, notably in relation to: • Urgent need to address: Hot pursuit and surveillance (including interception of communication); • Moderate need to address: Controlled delivery and covert investigations • Low need to address: Use of informants and witness protection

Source: Author's own elaboration

Legal driver: Law enforcement authorities are not able to efficiently use investigative tools across borders and face obstacles caused by differences in national rules

The divergent national implementation rules negatively affect the cross-border use of investigative tools. More specifically, officials conducting cross-border operations may have to observe several sets of rules depending on the Member State they enter during their day.[149] The main challenges relate to the use of cross-border hot-pursuit[150] and surveillance.[151] The need for harmonisation was assessed based on a triangulation of data sources:

- The extent to which there is evident variation and divergent legal processes relevant to use of the tool within European countries;
- The extent to which the tool is used and considered effective in tackling SOC both within and across European countries; and
- The perceived need for harmonisation as identified by stakeholders consulted.

Urgent need to address: Hot pursuit and surveillance

With respect to **hot pursuits**, there are inconsistencies that hamper the efficient use of this tool during cross-border operations.[152] Some Member States and SAC refer directly to CISA as the legal basis for the use of this tool. Even though the use of CISA as the legal basis ensures a

the European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanism pursuant to Article 22 of Council Regulation (EU) No 1053/2013 First Multiannual Evaluation Programme (2015-2019) SWD/2020/327 final. Available at: link.

[148] Europol (2015). *Exploring Tomorrow's organised Crime*. The Hague: Europol.

[149] European Commission (2020) Report from the Commission to the Council and the European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanisms pursuant to Article 22 of Council Regulation (EU) No 1053/2013 – First Multiannual Evaluation Programme (2015-2019). Brussels: European Commission.

[150] Schengen evaluation reports: C1, C4, C6, C10, C11, C15, C18, C20, C25, C31. Interviews: 1 EMPACT Driver. Technical workshop held on 24 March. Survey: Q 59, LEAs respondents reported differences regarding the length of time for which a special investigative tool may be authorised (39%, n=45) and the offences for which an investigative tool may be authorised (52%, n=61) as the main barriers to the effective use of the investigative tools.

[151] Schengen evaluation reports: C1, C3, C4, C6, C8, C12, C19, C21, C23, C24, C27, C29. Interviews: 1 representative from an EU body. Technical workshop held on 24 March.

[152] Schengen evaluation reports: C1, C4, C5, C6, C9, C10, C11, C17, C19, C23, C24, C25, C31.

certain degree of harmonisation, bilateral agreements often add on this basis a number of more specific and operational rules for the implementation of the tool in the different regional contexts. This results in the same tool being regulated differently depending on the regional agreement under which it is applied. Issues mainly relate to differences in the right granted by the national law to foreign officials to arrest/apprehend a suspect. Indeed, the right to arrest during hot pursuit is differently defined across bi-/tri-/multilateral agreements. Some agreements grant foreign officials only the right to apprehend/detain a suspect, while other agreements allow foreign officials also to perform searches and to handcuff a suspect. Finally, differences in territorial and time restrictions represent another barrier for the use of cross-border hot pursuits, with countries setting different restrictions to foreign officials when implementing these tools. Besides differences in bi-/tri-/multilateral, the analysis has identified **issues in relation to the relevance of EU provisions on cross-border hot pursuit**. Notably, since the definition included in Art. 41 CISA only covers land borders, countries having only sea borders cannot use cross-border hot pursuits unless covered in bi-/tri-/multilateral agreements, and also countries with sea borders (but no exclusively) face problems.[153] This leads to an inconsistency between Art. 41 CISA and Art. 20 of the Naples II Convention, which allows customs and all LEAs competent under the Convention to carry out the pursuit also over sea borders. The study also found an issue in terms of the types of authorities allowed to use hot pursuits. Besides the five countries where customs authorities are allowed to use CISA pursuant to Art. 41 (Belgium, France, Germany, Luxembourg, the Netherlands), there are also other Member States and SACs where customs have the power to perform criminal investigations and therefore refer to CISA. In yet other Member States, customs undertake purely administrative controls, preventing them to investigate crimes and, therefore, to use CISA. In the end, the different scope of application of a tool under different instruments leads to uncertainties concerning the proper legal basis.

Concerning **surveillance**, besides differences in terms of the surveillance methods adopted at the national level, there are also differences in the maximum time allowed by different Member States or SACs to carry out surveillance activities. This leads to cases (in countries where this period is comparatively shorter) in which the related timeframe could be insufficient to get evidence about a criminal activity or organisation.[154] Similarly, the different rules applied nationally to the use of audio and technical surveillance, including voice bugging and GPS tracking, and the fact that it is allowed in some, but not all countries hamper its use during cross-border operations.[155] Furthermore, the differences in the types of institutions responsible to oversee the cross-border implementation of investigative tools also create additional obstacles to cooperation. The mapping of country laws on surveillance also revealed data on interception of communication. Due the intrusive nature of the **interception of communication**, the data identified strong procedural safeguards in place at the national level, with law enforcement operatives generally being required to seek authorisation. Several stakeholders identified that varied authorisation processes can hamper the use of this tool during cross-border investigations.[156] Thus, minimum authorisation standards for use, or indeed designated contactable bodies for authorisation, could be considered to balance the efficacy in investigations and procedural safeguards. However, some stakeholders suggested that rather than harmonising law on the operation of surveillance, the focus should instead be on harmonising laws to share information and obtain this from technology providers.[157]

Moderate need to address: Controlled delivery and covert investigations

With respect to **controlled delivery**, there is appetite from stakeholders for harmonisation of existing rules.[158] While overall being considered as a highly effective tool,[159] it also suffers from

[153] Schengen evaluation reports: C1, C6, C15, C18, C20, C25.
[154] Di Nicola, A., Gounev, P., Levi, M., Rubin, J., Vettori, B., Baratto, G., Betgens, M., Bezlov, T., Bressan, S., Constantino, F., Cauduro, A. (2015) Study on paving the way for future policy initiatives in the field of fight against organised crime: the effectiveness of specific criminal law measures targeting organised crime.
[155] Interviews: 1 EMPACT Driver. 1 SAC's representative at the Technical workshop held on 24 March. Survey: Q 97, 54% (n=63) of LEAs' respondents reported that an EU intervention to harmonise the definition of tracking surveillance (e.g. use of GPS/transponders; mobile phones; radio-frequency identification devices (RFID); biometric info technology) would improve cross-border cooperation to a high or very high extent. Workshops held on 24 March and 25 May.
[156] Interviews: 3 EMPACT Drivers; Group interview with EMPACT Support Managers.
[157] Group interview with EMPACT Support Managers.
[158] Technical workshop held on 24 March. Interviews: 1 EMPACT Driver.
[159] Survey: Q 83, 91% (n=110) of LEAs' respondents consider controlled delivery to be effective in cross-border

significant differences in the national authorisation processes that may act as barrier to effective cross-border investigations, particularly with regard to drug trafficking.[160]

Covert operations are permitted in all countries (either anchored in law or procedures) and typically available for a wide range of crime types. Vis-à-vis the other investigative tools, survey participants indicated that it is relatively infrequently used domestically and in cross-border cases, yet it is perceived as having a high effectiveness in both situations. The stakeholders consulted over the course of this study did not regard harmonisation for this tool to be a priority.[161] Yet, there are some differences in crime types and thresholds under which it can be used. The biggest divergence was found between the authorisation processes, which echoes a similar observation made with regard to surveillance, which was assessed as having a higher degree of need for harmonisation. Due to the inherent link of covert operations with surveillance practices, it was therefore assessed to be a **moderate need for harmonisation**, despite its low frequency of use and high perceived effectiveness in law enforcement cooperation.

Low need to address: Use of informants and Witness protection

With respect to **witness protection,** the main differences in national legislation relate to processes of authorisation which are heterogeneous, with a number of different actors and specialised bodies identified across countries. Moreover, most countries specify that in order to offer protection, the witness should be at risk of harm or serious harm.[162] Finally, while some countries require the tool be used in certain criminal cases, specifying crimes such as terrorism and tracking in human beings or firearms[163] or organised crimes,[164] other countries do not restrict the use of witnesses protection to the investigation of specific offences, nor do they set any custodial thresholds.[165] As far as the **use of informants** is concerned, the overall case for harmonisation can be considered as limited. Five countries[166] were found not to use this investigative tool at all, highlighting that there may not be a perceived need in response to their specific crime contexts. Furthermore, the impacts of harmonisation may be hindered because crime and investigative priorities of Member States and SACs reflected in staffing, equipment and financial resources allocated to use of informants, varies between countries.[167] Thus, harmonisation would likely require investment in operational infrastructure in those relevant countries.

investigations to a "high" or "very high" degree.
[160] Schengen evaluation report: C4, C6, C13, C17, C18, C27, C28.
[161] Technical workshop held on 24 March 2021.
[162] National legislation: PL, DE, BE, AT, EE, FR, NL, ES, HR, FI, CZ, ES, FR, IT, RO, SE.
[163] National legislation: NO, FR.
[164] National legislation: PT, FR.
[165] National legislation: AT, CY, CZ, DK, FI, EL, HU, IT, MT, NL, PL, SK, SI, ES, SE, BG, CH
[166] CY, LI, LT, LU, CH.
[167] Group interview with EMPACT Support Managers.

3 THE NEED FOR EU ACTION

3.1 Legal basis

The legal basis for EU action in the field of intra-EU law enforcement cooperation is Title V, Chapter 5 of the Treaty on the Functioning of the European Union (TFEU). Pursuant to Article 87 (TFEU), "the Union shall establish police cooperation involving all the Member States' competent authorities, including police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences". The EU has competence to adopt measures aimed at enhancing and supporting the exchange of information, developing the most relevant skill-set among officials, defining common investigative techniques and, to some extent, to set rules for Member States engaged in joint operations and acting outside their territory.

3.2 The necessity of EU action

EU action is needed to properly address all the three core problems identified. First, Member States and SAC alone would not be able to overcome the actual confusion in relation to the choice of the proper EU legal basis and concerning the most appropriate tool/channel to use for information exchange. Moreover, Member States and SAC alone would not be able to ensure an appropriate and uniform level of knowledge of and capacity to use relevant databases, as well as to overcome current differences among SPOCs ,which hinder the exchange of relevant information across countries. This means that the current differences in the national interpretation and implementation of EU measures would remain and would continue to negatively affect the relevance and efficient sharing of information.[168] Second, Member States and SAC would continue to face uncertainties stemming from different legal systems on the rights given to officials when operating in foreign countries and technical interoperability issues, both relating to IT systems, as well as the frequencies and frequency ranges of radio communication, that would eventually contribute to reducing the appeal of joint operations.[169] Finally, the differences in national rules in relation to investigative tools would remain and Member States and SAC alone would not be in a position to overcome and progressively reduce them. Moreover, an EU intervention would be needed to better match current EU provisions on the cross-border use of investigative tools with law enforcement authorities' need on the ground.[170]

3.3 The added value of EU action

EU intervention could ultimately create added value by contributing towards a common playing field, which could be not achieved by the Member States and SAC alone.[171] Indeed, the study found evidence that current national differences contribute towards making the exchange of information inefficient. Moreover, the cross-border nature of safety and security threats, as well as the challenges related to the increasing cross-border nature of SOC call for an EU intervention of some kind. The EU is expected to be better equipped than individual Member States and SAC to ensure the coherence of the actions taken at the national level, address the legal fragmentation, prevent duplications and uncertainties and eventually ensure an efficient counter-action to cross-border SOC and terrorism.

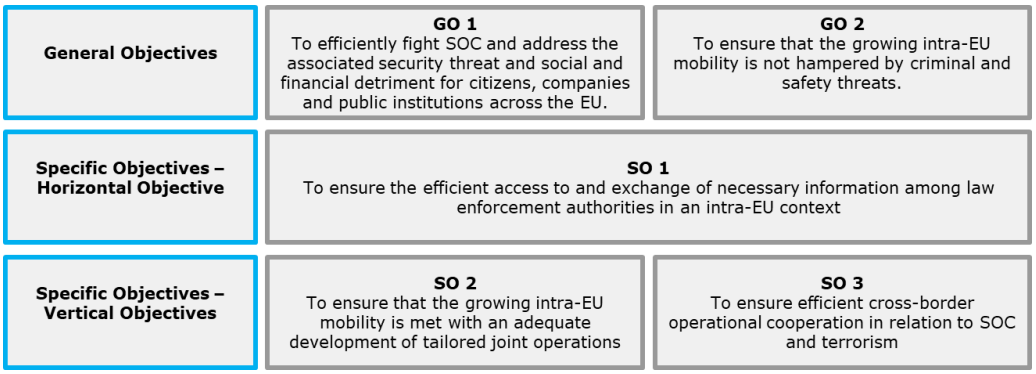
[168] Survey: Q 90, 82% (n=131) of LEAs respondents supported the need for EU intervention in this field reporting a need for EU action from a moderate to a very high extent.
[169] Survey: Q 97, 76% of LEAs (n=64) reporting the need for EU intervention from a moderate to very high extent and 38% (n=32) reporting the same need from a high to very high extent. Q 89, 19% (n=18) of LEAs' representatives would like an EU intervention in the area of international sport/music/cultural events.
[170] Survey: Q 88, 54 (n=83) of LEAs respondents reported a strong need for EU intervention in this field. According to the survey respondents, areas of crimes where the EU intervention is more needed are cybercrime, illegal immigration and terrorism.
[171] Survey Q 92: 2 representatives from NECs, 2 representatives from Specialised investigative units, 1 representatives specialised analytical department, 2 representatives from Public order and safety/NFIP, 1 representative customs authority.

4 POLICY OBJECTIVES

4.1 General and specific objectives

The objectives of the future EU initiative are summarised in the objective tree below, which differentiates between general objectives (GO) and specific objectives (SO).

Figure 6 - Objective tree



Source: Authors' elaboration based on desk research

4.2 Consistency with EU policies and initiatives

The general and specific objectives identified above are consistent with other EU policies in the field of law enforcement cooperation. More specifically, consistency was found with (i) the **EU Security Union Strategy for the period 2020 to 2025,**[172] which points to the need to improve intra-EU operational law enforcement cooperation; (ii) the **Counter-Terrorism Agenda,**[173] which calls for a more effective interoperability of EU information; (iii) the **EU Strategy to tackle organised Crime 2021-2025,**[174] which is focused on boosting law enforcement and judicial cooperation; (iv) **Council Document 13083/1/20,**[175] which calls for the consolidation and improvement of available law enforcement instruments; (v) **Commission Recommendation (EU) 2017/820,**[176] which invites Member States to strengthen cross-border police cooperation; (vi) **Commission Staff Working Document SWD/2020/327 final,**[177] which highlights the need to address the deficiencies and the recurrent issues affecting law enforcement cooperation; (vii) **Council Document 10062/19,**[178] which invites Member States to make more efficient use of the existing legal framework about the deployment of joint operations towards public security; (viii) **Council Document 5503/21**[179] on the use of SIENA as a primary communication channel; and (ix) the **Strategy towards a fully functioning and resilient Schengen area**,[180] which calls for stepping up police cooperation. Notably, the Strategy refers to a forthcoming legislative proposal for an EU Police Cooperation Code, which would formalise and clarify the procedures for information-sharing among Member States and address the need for common standards to allow police officials to cooperate effectively with their peers. Further info supporting the assessment in this section is included in Annex II.

[172] Commission Communication on the EU security union strategy COM/2020/605 final (2020). Available at: link.
[173] European Commission (2020) *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond.* Brussels: European Commission. Available at: link.
[174] European Commission (2020) *A EU Strategy to tackle organised Crime 2021-2025.* Available at: link.
[175] Council Document Nr 13083/1/20, 24 November 2020, Council Conclusions on Internal Security and European Police Partnership. Available at: link.
[176] Commission Recommendation (EU) 2017/820 of 12 May 2017 on proportionate police checks and police cooperation in the Schengen area. Available at: link.
[177] Commission Staff Working Document on the Functioning of the Schengen Evaluation and Monitoring Mechanism pursuant to Article 22 of Council Regulation (EU) No 1053/2013 First Multiannual Evaluation Programme (2015-2019) SWD/2020/327 final. Available at: link.
[178] Council Document 10062/19, 6 June 2019, Council conclusions on certain aspects of European preventive policing. Available at: link.
[179] Council Document 5503/21, 28 January 2021, Council of the EU (2020) Secure communication channel in law enforcement cooperation – SIENA. (LIMITE).
[180] European Commission (2021) Communication from the Commission to the European Parliament and the Council - A strategy towards a fully functioning and resilient Schengen area. COM(2021) 277 final, 2 June, Brussels.

5 OPERATIONAL RECOMMENDATIONS

5.1 Introduction: Approach and types of policy options

Three policy options have been elaborated to address the identified challenges (see the problem assessment in section 2), listed from the least to the most "extensive" option[181]:

- *Policy Option 1:* Baseline Scenario/Status Quo;
- *Policy Optio*n 2: Legal proposal on minimum standards + supporting (soft) measures;
- *Policy Option 3:* Legal proposal aiming for stronger alignment + supporting (soft) measures.

As a first step of Task 6, a **long list of specific legislative and non-legislative elements** (or 'sub-options') was elaborated.[182] Taking the specific objectives and drivers as a starting point, alternative legislative and non-legislative sub-options were identified based on the data collected in the framework of this study, including existing sources, suggestions by stakeholders and good practices identified, as well as proposals from the Study Team. For the most part, the content of the policy options is based on existing measures and good practices in order to ensure that their specific elements have either been tested in national and cross-border contexts or refer to improvements of already existing solutions. However, in some instances, aspects were identified as part of the problem assessment in relation to which none of the sources[183] available to the Team identified a solution, or where additional solutions to those identified in the relevant sources could be considered. Thus, the policy options also contain new solutions that exceed the measures currently available for EU law enforcement cooperation.

As a next step, a **preliminary screening** of the elements included in the long list was performed, reviewing each element/sub-option regarding its (potential) feasibility and effectiveness. Elements, for which a lack of feasibility was found, or which were not considered adequately effective, were discarded for further analysis and inclusion in the policy options (see Annex IV for individual justification).

Those sub-options that passed the preliminary screening were distributed between PO2 and PO3. While the less intrusive sub-options were allocated to PO2, the more intrusive sub-options were included in PO3. Due consideration of the links and interdependencies between certain sub-options was also made when allocating the elements/sub-options to one of the policy options. Hence, in some cases 'clusters' of sub-options were included in the policy options (e.g. in relation to the measures concerning SPOCs and CMS).

The **developed policy options therefore contain the retained legislative and non-legislative elements**, dealing with the problems identified in different ways, while aiming to achieve the policy objectives set out in section 4. Whereas the two policy options developed (in addition to the baseline scenario) both individually address all aspects identified in the problem assessment and the specific objectives, the choice of legislative and non-legislative elements varies slightly between the two policy options. This means that the policy options vary in relation to the extent to which they e.g. aim at harmonising the legal framework governing EU law enforcement cooperation, as well as Member States' national set-ups.[184]

Details on the specific legislative and non-legislative elements each policy option contains is outlined below. Further supporting information, including the intervention logic (which links the policy option elements to the objectives and drivers), is provided in Annex IV[185].

[181] Based on the European Commission's feedback of 10 May and 18 May 2021 regarding the draft policy options, the preliminary sets of policy options provided in the draft interim report and the interim for acceptance have been revised.
[182] The list was structured according to each of the three specific policy objectives and the individual drivers in order to ensure that all objectives, problems and drivers are systematically addressed by the policy options.
[183] Preliminary results of the desk-based analysis, e.g. good practices identified in the Schengen evaluation reports or stemming from bi/tri/multilateral agreements; Discussions with stakeholders (e.g. during the interviews and the technical workshops); and Written feedback, such as the online survey.
[184] Refer to Table 4 in Annex 1 for a list of available relevant EU initiatives and types of cooperation covered by each of them.
[185] This includes: (i) Operational recommendations on action needed at EU level; (ii) A list of policy options identified in

As concerns the **form of the legislative measures** considered, based on the analysis conducted, it appears that both the form of a Directive and the form of a Regulation could be relevant to address the problems identified. Both measures have the potential to harmonise the diverging approaches existing in the Member States that currently are part of the cause of the problem, although to a different degree. This being said, based on an assessment of the political feasibility, it is considered that a policy option in the form of a Regulation can be discarded at this point in time, as it is unlikely to be favoured by the Member States. Hence, **both policy options 2 and 3 would take the form of a Directive** for the purpose of the assessment provided.

Also based on political feasibility considerations, amending the SFD (compared to CISA, Prüm or the Naples II Convention or proposing a new instrument) has been identified as the preferable solution to introduce the legislative elements that address specific objective #1 (information exchange). For all legislative elements referring to operational cooperation (objectives #2 and #3), also amending existing legislation, e.g. Prüm[186], would seem to be advisable. Hence, both policy options (PO2 and PO3) have been set up in the same way and would both involve amendments to the SFD (for information exchange) and Prüm (for operational cooperation).

The reason to consider two legal instruments rather *one* Police Cooperation Code is again the political feasibility of the measures: Whereas measures on information exchange require qualified majority, measures on operational cooperation require unanimity.

While the two options developed in addition to the baseline scenario, which would both imply amending existing legislation, may not seem to be as far-reaching as the new Police Cooperation Code previously communicated by the Commission, they still include some important changes compared to the current situation and have been developed taking due consideration of the problems identified, the objectives developed, as well as proportionality, subsidiarity and political feasibility.

SFD in comparison to CISA, Prüm and the Naples II Convention: High-level overview

With reference to **stakeholders, purpose/scope and criminal offences**, SFD is the wider measure. In particular, the SFD refers to Police, Customs and other Authorities, and to detection, prevention and investigation of a long list of criminal offences. It has to be noted that SFD shall not be applied when dealing with national security issues.

SFD is one of few measures that provides for **languages and channels of communication**, even if only generally speaking.

The SFD covers **information and/or intelligence** but does not impose any obligation on the Member States to gather and store such information for the purpose of sharing it with the competent law enforcement authorities of other Member States. Moreover, Member States shall ensure that conditions not stricter than those applicable at national level for providing and requesting information and intelligence are implemented. Explicit reasons to withhold information or intelligence (SFD, Article 10) are also provided for, and explains when a Member State can refuse to share the requested data. SFD supplies **forms** to request and to provide information or intelligence and establishes deadlines to do so.

Moving to **data protection**, SFD provides for a specification: Information and intelligence may be used by the competent law enforcement authorities of the Member State to which it has been provided solely for the purposes for which it has been supplied in accordance with the SFD or for preventing an immediate and serious threat to public security. From a general point of view, it shall be noted that the Prüm Decision provides for specific indications related to DNA, accuracy, relevance and storage time, technical measures, logging and data subjects' rights. When it comes to data protection, CISA is exhaustive and provides for specific rules in order to identify who is entitled to enter or modify data. All these measures were, however, issued before the GDPR and the Law Enforcement Directive (LED). Therefore, there is a need to align the provisions on data protection described above with the (newer) GDPR and LED instruments.

the stakeholder consultations; (iii) A table on discarded measures, including an individual justification for discarding them (iv) The intervention logic; and (v) An assessment table of the coherence criteria for policy option 2.

[186] Decision 2008/615 contains provisions which are based on the main provisions of the Prüm Treaty 2005 and are designed to improve the exchange of information, whereby Member States grant one another access rights to their automated DNA analysis files, automated dactyloscopy identification systems (fingerprints) (https://ec.europa.eu/anti-fraud/sites/default/files/docs/body/prumtr.pdf) and vehicle registration data. The Decision 2008/615 transpose what is already stated in the previous Treaty. The Treaty also states for air Marshall (article 17), illegal migration (Article 20) which are not analysed by Decision 2008/615.

CISA and the Naples II Convention explicitly regulate **special forms of cooperation** as hot pursuit, cross-border surveillance, controlled delivery, covert investigations, and joint special investigation teams, although only CISA specifies who are the officials referred to and also the criminal offences involved. Otherwise, Naples II identify an effective procedure to request assistance.

Turning to CISA, it provides for specific suggestions to install **specific communication means**, such as telephone, radio and telefax to easily cooperate with other Member States at the boarders. Despite that the suggestion is old-fashioned it is meaningful and should be taken into consideration, although it may be relevant to adapt in view of technological developments.

CISA, in its Article 45, is the only instrument that asks Member States to collect personal data of **persons hosted in hotels, B&B, boats and similar accommodations**.

Both Prüm and CISA provide for liability in similar ways, but the text of Prüm is clearer and provides also for criminal liability.

Lastly, CISA refers to **SIS** (in 2013 updated in SIS II) as primary joint information system to have access to alerts on persons and property for the purposes of border checks and other police and customs checks.

Protecting citizens' personal data and safeguarding fundamental rights were core drivers for the design of the policy options. Each of the policy options aims at maximising the extent to which fundamental rights are safeguarded and balancing to the extent possible any negative effects citizens may face (e.g. concerning increased data collection and information exchange).

In addition, both policy options 2 and 3 would involve replacing the existing data protection provisions in Article 8 of the SFD with a reference to the LED. The impact assessment (see chapter 6) also includes an assessment of data protection and fundamental rights aspects for each of the policy options.

5.2 Description of the policy options

This section provides a description of the three policy options. For the purpose of user-friendliness, the elements of the specific policy options are clustered and presented towards both the specific objectives and problems they aim to address. A more detailed intervention logic that clearly links the four components (i) problems, (ii) drivers, (iii) objectives and (iv) policy options is included in Annex IV.

5.2.1 Policy option 1: The baseline scenario

Table 7 presents the content of the baseline scenario. Under this option, no further policy action is taken than what is already in place or underway.

Table 7 – The baseline scenario

No.	Problem	Elements of the option
Specific objective 1: To ensure the efficient access to and exchange of necessary information among law enforcement authorities in an intra-EU context		
1.1	**Legal barrier**: LEAs face difficulties in interpreting and implementing relevant EU provisions. Moreover, national rules impose obstacles for cross-border information exchange.	*No change to the current policy measures.* The current uncertainties with regard to the applicable legislation and differences between the Member States would remain. There would continue to be unclarity on what data are available in different Member States and deadlines would continue to not be systematically met. Moreover, Member States are 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. The planned changes to SIENA that are currently foreseen by Europol are, however, expected to lead to some clear improvements with regard to the cross-border exchange of information, notably due to its expected doubling of users (further information is provided below, following this table).
1.2	**Technical barrier**: LEAs have outdated IT infrastructure.	*No change to the current policy measures.* 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. The same is valid with regard to the use of secure communication means.

No.	Problem	Elements of the option
1.3	**Structural barrier**: National and regional information hubs set up by LEAs have different roles, means and capabilities, which make their cooperation sub-optimal. LEAs have insufficient knowledge of mechanisms and skill gaps.	*No change to the current policy measures.* The varied competences of the SPOCs across the EU would remain, hampering the efficient exchange of information, notably due to that adequate access to key databases and platforms is not ensured in all SPOCs. 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.
Specific objective 2: To ensure that the growing intra-EU mobility is met with an adequate development of tailored joint operations		
2.1	**Legal barrier:** Law enforcement officials operating in other Member States often have inadequate powers. Moreover, these powers vary between the Member States, which leads to confusion.	*No change to the current policy measures.* Law enforcement officials operating in other Member States than their "own" would continue to face unclarity on their powers on the ground in the hosting Member State and in many cases *de facto* have limited powers to provide efficient support.
2.2	**Technical barrier**: Officials on the ground are not able to efficiently access the information they need to ensure public order and safety.	*No change to the current policy measures.* While some improvements may be made by individual Member States, officials on the ground are expected to continue to not be able to directly access the information they need in relation to international events in the majority of cases, and thus lose valuable time due to the need to obtain the information via a colleague in office, who acts as an intermediary.
2.3	**Structural barrier:** National LEAs have limited financial and human resources to ensure an adequate use of joint operations.	*No change to the current policy measures.* Joint operations are expected to continue to be underused due to a lack of resources in the Member States.
2.4	**Structural barrier:** Cooperation between LEAs in different countries, e.g. for the purpose of joint operations in border regions, is insufficiently informed by joint threat assessment/risk analysis.	*No change to the current policy measures.* The planning of joint operations would continue to suffer from a lack of joint cross-border threat assessments / risk analyses, and information from customs would also in the future be not adequately considered.
Specific objective 3: To ensure efficient cross-border operational cooperation in relation to SOC and terrorism		
3.1	**Legal barrier:** LEAs are not able to efficiently use investigative tools in a cross-border context and face obstacles caused by differences in national rules.	*No change to the current policy measures.* The rules of different Member States concerning key investigative tools are expected to continue to vary, not only causing uncertainties, but operational obstacles to efficiently fight SOC and terrorism, as well as public order and safety.

Source: Author's own elaboration

As indicated above (see legal barrier 1.1) Europol is already making efforts to improve SIENA. These are briefly depicted below. As noted above, the planned changes to SIENA that are currently foreseen by Europol are expected to lead to some improvements with regard to the cross-border exchange of information already in the baseline scenario.

SIENA's development in the baseline scenario

Within the baseline scenario, Europol is striving towards making various improvements in relation to SIENA in order to achieve ensure swift, secure and user-friendly communication and exchange of operational and strategic crime-related information and intelligence between Europol, Member States and Schengen associated countries.

Europol identified major priorities for future developments of SIENA which need to be considered to be part of the baseline scenario. One example is the implementation of the 'Basic Protection Level' (BPL) within SIENA, which aims at establishing a secure channel for non-restricted or classified information that is easier to use and, thus, more accessible to a wider range of stakeholders. In an interview, Europol indicated that the introduction of the BPL is expected to double the number of SIENA users within the next years.[187] In addition, Europol is currently striving towards upgrading SIENA towards a system that enables easier integration with Member States' CMS. Moreover, Europol indicated that development work

[187] Interview conducted on 28.05.2021.

with regard to the user experience is ongoing since 2019, ranging from design improvements to complex functionality developments:

- Design improvements, e.g. landing page redesign, forms fonts and colours, mailbox selection, address book (already implemented), but also development of notifications and search functions, case access, form and message re-design (finalised, pending implementation; and
- Complex functionality developments (to be developed in the future but already 'on the radar') such as possibilities for user customisation by SIENA users, 'smart' translation tools, and mobile functionalities.

During the interview, Europol noted that SIENA messages continue to evolve to rather large message forms, which necessitates streamlining existing forms and facilitating the terminology. Europol pointed out that future developments will be focused on increasing interoperability with both Europol and national systems in order to make SIENA part of the "daily-business" of law enforcement officials. A crucial enabler for this, according to Europol, will be the implementation of follow-up functionalities in case of a hit, regardless of whether the hit was found in a Europol database or not.

Source: Author's own elaboration

If no further action is taken than what is already in place or underway, in the near future LEAs will likely even more than at present face the challenge of keeping pace with criminal groups. LEAs are expected to take advantage of and use new technologies to cope with evolving criminal patterns, e.g. by enhancing systems such as SIENA. At the same time, however, criminals are likely to continue to be quick to exploit the latest social and technological developments such as new end-to-end encrypted communication apps and to devise new *modi operandi* as needed.

5.2.2 Policy option 2: Legal proposal on minimum standards + supporting (soft) measures

The table below presents the elements of policy option 2, which constitutes a legal proposal on minimum standards, e.g. through an amendment of the SFD and Prüm, and that is flanked by supporting (soft) measures.

Table 8 – Legal proposal on minimum standards + supporting (soft) measures

No.	Problem	Elements of the option
Specific objective 1: To ensure the efficient access to and exchange of necessary information among law enforcement authorities in an intra-EU context		
1.1	**Legal barrier**: LEAs face difficulties in interpreting and implementing relevant EU provisions. Moreover, national rules impose obstacles for cross-border information exchange.	• *Clarification of the scope of the SFD*: Clarification of the types of operations to which the SFD applies and definition of the competences LEAs need to have for its application • Establishment of a *common minimum set of data* that has to be made available by all Member States for exchange. The common minimum set could encompass data that is managed by and therefore directly accessible to SPOCs in at least 10 Member States / SAC, thus encompassing the following 10 sets of data: *Wanted/missing persons; Persons suspected of criminal activities (criminal intelligence); Stolen goods; Database of firearms; Photographs (persons); Persons suspected of (a specific) crime; Persons convicted of crime (criminal records); Passports and identity documents; Border controls, border crossings and other border guard matters; Reports (complaints) concerning crimes committed.* • *New provisions ensuring compliance with the deadlines by which data are to be made available to another Member State* (including when a judicial authorisation is required). • New provision, requiring the Member States to set out in the request for information the factual reasons to believe that the relevant information and intelligence is available in another Member State, and explain the purpose for which the information and intelligence is sought in another Member State 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) • *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. Interpol i24/7 should be used in cases where third countries are involved in the exchange of information, and if third countries do not conclude a cooperation

No.	Problem	Elements of the option
		agreement with Europol and do not have access to SIENA. SIENA would need to be monitored 24/7. There would also be an obligation to put Europol in copy in cases concerning information exchange within Europol's mandate. The following non-legislative improvements to SIENA would also be made: - 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) • *Adaptations to the SFD to remove references to "other" cases and also remove the forms for information exchange* (two annexes). • *Adaptations to the SFD to ensure alignment with the Law Enforcement Data Protection Directive (LED),* notably Article 8 on data protection. • *Flanking non-legislative measures*: Training, updated guidance (e.g. on SIENA), 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). Internal Security Fund (ISF) support would be foreseen for the SIENA roll-out.
1.2	**Technical barrier**: LEAs have outdated IT infrastructure.	• *Establishment of common requirements for case management systems (CMS) for the SPOC*: - Clearly define the CMS, including whether according to the national legislation (a) CMS is a database or (b) a workflow system (including the establishment of data retention requirements in line with the General Data Protection Regulation (GDPR), Interpol, SIRENE, etc.) - Provide a list of common requirements for the functionalities of the CMS, e.g.: o Degrees of urgency should be linked with a deadline (e.g. when a deadline draws near, alerts should be triggered). o Selection (in a multiple-choice list by the requesting Member State) and cancellation of the degrees of urgency should be done manually. o One CMS for receiving, sending and dispatching messages (follow up, manage, store and exploit the international exchange of information). Universal message format to be used. o The 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. The same is valid for exporting generated messages. o 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 about persons/objects; per item – per act; author, date and time. This should be done automatically on the basis of the user profile. o Automation of data cross-check, e.g. through improved search tools and the adoption of transliteration and "fuzzy logic" search. o Generation of proper statistics for national analytical needs and as required by EU law (e.g. the Schengen Information System (SIS) Regulation). - 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) - 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. - Availability of technical support. • *Secure communications* (non-legislative measures): Feasibility study on how to improve the secure digital and radio communication between the Member States. Financial support to the work of the EU innovation hub and of the RECG (Radio-communication Expert Group – Sub-group of the LEWP). • *Flanking non-legislative measures*: Training on CMS use.

No.	Problem	Elements of the option
1.3	**Structural barrier**: National and regional information hubs set up by LEAs have different roles, means and capabilities, which make their cooperation sub-optimal. LEAs have insufficient knowledge of mechanisms and skill gaps.	• *Establishment of the SPOC as a "one stop shop" for LEA cooperation through common minimum standards. A SPOC should*[188]: - Be set up through its own national legislative or regulation identity. - 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 having a judicial authority available 24/7 "within" the SPOC). - Have full access to EU and international law enforcement databases (i.e. SIS, Europol databases, Interpol databases and software applications such as EUCARIS). - Be connected to SIENA (for intra-EU cases & Member States), i24/7 (for cases involving third countries), SIS, the SIRENEmail network, and TESTA. - Involve staff in the SPOC who have full access to all relevant national case management systems (including those managed by customs and border guards). - Ensure that all relevant information from the 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 and border guards). - Ensure further coordination between the SPOCs and the PCCCs and other relevant entities, such as the national EMPACT coordinators and the network of EMPACT actors. • *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.
Specific objective 2: To ensure that the growing intra-EU mobility is met with an adequate development of tailored joint operations		
2.1	**Legal barrier:** Law enforcement officials operating in other Member States often have inadequate powers. Moreover, these powers vary between the Member States, which leads to confusion.	• *New provision on the conferral of powers:* The host Member State should confer certain operational powers to officials of seconding Member States that are involved in joint operations. Exceptions may be defined. See, for instance, Council Decision 2008/617/JHA Article 3.2 and 3.3: *Subject to agreement between the Member States concerned, assistance may consist of providing the requesting Member State with equipment and/or expertise and/or of carrying out actions on the territory of that Member State, using weapons if so required. In the case of actions on the territory of the requesting Member State, officials of the assisting special intervention unit shall be authorised to operate in a supporting capacity on the territory of the requesting Member State and take all necessary measures to provide the requested assistance in so far as they (i) operate under the responsibility, authority and direction of the requesting Member State and in accordance with the law of the requesting Member State; and (ii) operate within the limits of their powers under their national law.*

[188] In addition to these measures, it was examined as part of the present study whether the current lack of full computerised access to hotel registers, should the need arise (Article 45 CISA) is an issue that should be addressed. However, relevant evidence that would justify EU action in this regard could not be identified.

No.	Problem	Elements of the option
		This should at minimum enable seconded officials to autonomously perform basic police tasks, such as identity checks, vehicle and body search. This includes the running of identification data in relevant databases. • *Flanking non-legislative measures*: Awareness raising and training.
2.2	**Technical barrier**: Officials on the ground are not able to efficiently access the information they need to ensure public order and safety.	• *New provision on the remote access to relevant law enforcement databases in specific situations:* The Member States are to provide [their own] officials on the ground remote access to specified police databases (or even specified data within them) in relation to specific types of international events (large-scale international football matches, mass tourism and music events, protection of VIPs etc.) via mobile terminals in specific geographical areas, such as major cities or regions where large-scale events take place more frequently. Restrictions on the use of specific types of information by the officials on the ground, including what information may be shared with officials from other countries, would be defined. • *Flanking non-legislative measures*: Awareness raising and training.
2.3	**Structural barrier:** National LEAs have limited financial and human resources to ensure an adequate use of joint operations.	• *Establishment of an appropriate financial instrument* by the Commission (e.g. through the ISF) to contribute to the funding of joint patrols in terms of staff costs; travel costs; accommodation; and expenses. • *Flanking non-legislative measures*: Awareness raising and training.
2.4	**Structural barrier:** Cooperation between LEAs in different countries, e.g. for the purpose of joint operations in border regions, is insufficiently informed by joint threat assessment/risk analysis.	• *New provision on cross-border threat assessment:* The Member States are to cooperate with neighbouring Member States to develop and use cross border threat assessment to better assess the need for joint operations and better inform their planning. • *Flanking non-legislative measures*: - Perform a pilot project to identify approaches to improve the development and use of joint threat assessment and risk analysis; - Development of data collection tools (questionnaire and manual) specifically for customs.
Specific objective 3: To ensure efficient cross-border operational cooperation in relation to SOC and terrorism		
3.1	**Legal barrier:** LEAs are not able to efficiently use investigative tools in a cross-border context and face obstacles caused by differences in national rules.	• *New provisions on surveillance:* - Extend the current EU legal provisions to also cover the use of cross-border surveillance in relation to waterways, sea and air borders - Establish the possibility to start physical surveillance operations on the territory of another Member State - Simplify the legal requirements notably for a surveillance operation transiting by a Member State - Extend the list of offences in relation to which cross-border surveillance is allowed. In addition to the offences included in Articles 40-41 CISA, the extended list would cover the following offences: Extraditable offence (crimes for which the European Arrest Warrant is required); fleeing custody. - Streamline the definitions of "pre-planned" and "urgent" surveillance in the relevant legislative provisions on EU level - Ensure the possibility for technical means of surveillance (e.g. GPS tracker, drone) - Define a common maximum time allowed to carry out cross-border surveillance activities, e.g. specific time as smallest common denominator: 24 hours - Accept and cooperate with the institutions responsible to oversee cross-border implementation of investigative tools in other Member States • *New provisions on hot pursuit:* - Extend the current EU legal provisions to also cover the use of cross-border hot pursuit in relation to waterways, sea and air borders - Extension of offences in relation to which cross-border hot pursuit is allowed. In addition to the offences included in Articles 40-41 CISA, the extended list could

No.	Problem	Elements of the option
		cover the following offences: Extraditable offence (crimes under the European Arrest Warrant); fleeing custody - Permit cross-border hot pursuit continue for at least an hour - Establish common rules for hot pursuit, e.g.: (i) Permit the requesting party the right to continue the hot pursuit if the requested party cannot take over the pursuit in time at a minimum; (ii) Permit hot pursuit beyond extraditable offences if someone avoids police or border checks without any time and territorial restrictions; Permit hot pursuit without any distance limit - Establish minimum standards on the rights and duties of the pursuing officials, including the right to: search a person; put on handcuffs; apprehend; detain; stop cars; perform preliminary arrest, if local authorities do not arrive on time • *Flanking non-legislative measures: Training and joint operation simulation exercises.*

Source: Author's own elaboration

5.2.3 Policy option 3: Legal proposal aiming for stronger alignment + supporting (soft) measures

Table 9 Table 7presents the elements of policy option 3. Many elements that are included in policy option 3 are also included in policy option 2. For the purpose of avoiding duplication, the table only presents elements that represent an addition or a change compared to policy option 2.

Table 9 – Legal proposal aiming for stronger alignment + supporting (soft) measures

No.	Problem	Elements of the option
Specific objective 1: To ensure the efficient access to and exchange of necessary information among law enforcement authorities in an intra-EU context		
1.1	**Legal barrier**: LEAs face difficulties in interpreting and implementing relevant EU provisions. Moreover, national rules impose obstacles for cross-border information exchange.	PO 3 would incorporate all of the measures in PO 2, but go beyond it in the following ways: • Establishment of SIENA as the default channel[189] for information exchange between Member States (excluding those situations where other channels are required by EU law). • Establishment of a common minimum set of data that has to be made available for exchange. The common minimum set could encompass data that is managed other national law enforcement authorities by but still directly accessible to SPOCs in at least 10 Member States / SAC, thus encompassing the following sets of data: *Administrative register on persons (census); Database of prison inmates; Register on enterprises and commercial companies; Information concerning foreign nationals (decisions and permits, measures imposed, etc.); and Passports and identity documents* *Although this dataset also refers to the availability in 10 Member States, it is a different dataset compared to policy option 2. It is expected that the data set under policy option 3 is harder to access than the one under policy option 3 because the data is stored in databases that are managed by other authorities than the SPOC.*
1.2	**Technical barrier**: LEAs have outdated IT infrastructure.	PO 3 would incorporate all of the measures in PO 2, but go beyond it in the following ways: • One CMS to be used by both SPOCs and PCCCs, or, alternatively, a requirement to ensure interoperability between the CMSs of the SPOCs and PCCCs
1.3	**Structural barrier**: National and regional information hubs set up by LEAs have different roles, means and capabilities, which make their	PO 3 would incorporate all of the measures in PO 2, but go beyond the common minimum standards and harmonise the rules on the SPOC in the following ways:

[189] With SIENA being the "default channel" it is meant that SIENA needs to be used mandatorily in relation to all cases, except for cases in which another channel needs to be used (e.g. since they have a clear component to a third country and, thus i24/7 needs to be used). This means that for cases that only have an EU 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.

No.	Problem	Elements of the option
	cooperation sub-optimal. LEAs have insufficient knowledge of mechanisms and skill gaps.	• Instead of "being informed about" (as per PO 2), PO 3 would establish that the SPOC is responsible for all international law enforcement cooperation requests dealt with at national level. • The same minimum requirements for set-up established in PO 2 for the SPOCs should also be applicable to the PCCCs. • Establishment that the communication between the SPOCs should take place in English (unless another common language is used by both SPOCs involved) and that all officials involved in the SPOC would need to have an adequate command of English. • Introduction of shorter intervals between the EU-STNA (e.g. reduction from 4 to 2 years).
Specific objective 2: To ensure that the growing intra-EU mobility is met with an adequate development of tailored joint operations		
2.1	**Legal barrier:** Law enforcement officials operating in other Member States often have inadequate powers. Moreover, these powers vary between the Member States, which leads to confusion.	PO 3 would incorporate all of the measures in PO 2, but go beyond it in the following ways: • The same text on the conferral of powers would be introduced, however, without any exceptions.
2.2	**Technical barrier**: Officials on the ground are not able to efficiently access the information they need to ensure public order and safety.	PO 3 would incorporate all of the measures in PO 2, but go beyond it in the following ways: • No geographical restrictions on the access would be introduced. There would also be less stringent restrictions on the use of the data obtained by the officials on the ground.
2.3	**Structural barrier:** National LEAs have limited financial and human resources to ensure an adequate use of joint operations.	PO 3 would incorporate all of the measures in PO 2, but go beyond it in the following ways: • A higher budget would be allocated within the financial instrument compared to PO 2. In addition to the items funded under PO 2, PO 3 would also foresee additional budget to e.g. train staff on joint operations, and to identify and share best practices. Budget would also be made available for technical means to facilitate training and knowledge sharing on the ground (e.g. a platform or an app that officials can quickly consult)
2.4	**Structural barrier:** Cooperation between LEAs in different countries, e.g. for the purpose of joint operations in border regions, is insufficiently informed by joint threat assessment/risk analysis.	PO 3 would incorporate all of the measures in PO 2, but go beyond it in the following ways: • PO 3 would set out more specific obligations concerning the cooperation related to threat assessments with neighbouring Member States in view of joint operations, e.g. that this needs to be done on an annual basis. • PO 3 would also introduce a new provision, making it compulsory for the Member States to share threat assessment and risk analyses with other LEAs insofar as this does not constitute a security risk for the Member State concerned
Specific objective 3: To ensure efficient cross-border operational cooperation in relation to SOC and terrorism		
3.1	**Legal barrier:** LEAs are not able to efficiently use investigative tools in a cross-border context and face obstacles caused by differences in national rules.	**Surveillance:** • New provision, establishing the possibility to start physical and technical surveillance operations on the territory of another Member State. • New provision, e.g. in the form of minimum standards, concerning the implementation of audio recording, voice bugging and GPS tracking. For example, new provisions establishing audio-surveillance / interception of communications as an investigative tool for all Member States, and defining a common set of rules/criteria for implanting audio-surveillance, covering e.g.: Preventive vs. in reaction to a crime already committed; Suspicious facts vs. suspected case; Scope of the group of persons to be monitored by audio-surveillance (actual suspect vs. contact persons / family members). • Extended definition of offences: In addition to the offences included in Articles 40-41 of CISA, the extended list would cover the following offences: *Murder; Manslaughter; Severe bodily harm; Severe sexual harassment and rape; Arson; Counterfeit currency; Grand theft; Blackmail; Abduction; Hostage taking; Deprivation of liberty; Trafficking in human beings; Drug-*

No.	Problem	Elements of the option
		related crimes; Illegal arms trade; Explosions; Trade with poisonous, nuclear or radioactive substances; Hit and runs after accidents that caused severe injury or death; Terrorism; Sexual exploitation of children; Corruption; Seizure fraud; Money laundering; Cybercrimes; Environmental crimes; Smuggling; Racism and xenophobia; Illegal trade of cultural artefacts; Fraud; Counterfeit products; Forgery of documents; Abduction of means of transport; Sabotage; Being a member of a criminal organisation. The list would be supported by minimum custodial thresholds, which would need to be met before the tool can be used to investigate such offences. • Define a common maximum time allowed to carry out cross-border surveillance activities, e.g. specific time as smallest common denominator: 14 days • New provision, requiring the Member States to accept the involvement of and cooperation with the institutions responsible to oversee cross-border implementation of investigative tools from other Member States. A list of the specific institutions would be made available and kept up to date. **Hot pursuit:** • New provision, permitting cross-border hot pursuit to continue without any time limit (compared to one hour under PO 2) • New provision, introducing common definitions of 'arrest', 'search', 'detain' 'interrogate' etc. **Controlled delivery:** • Common minimum approximation of national rules to facilitate its use in a cross-border context **Covert investigations:** • Common minimum approximation of national rules to facilitate its use in a cross-border context **Interception of communication:** • Common minimum approximation of national rules to facilitate its use in a cross-border context

Source: Author's own elaboration

6 ANALYSIS OF THE IMPACTS OF THE POLICY OPTIONS

6.1 Assessment of the impacts of policy options

6.1.1 Introduction

This section contains the assessment of the impacts of the three policy options described in section 5 in relation to the following **assessment criteria**:

Evaluation of the effects *(Task 8 of the ToR)**:***

- Effectiveness (achievement of the objectives);
- Efficiency (cost-benefit analysis; "value for money"); and
- Coherence and proportionality (internal and external synergies, duplications and inconsistencies, as well as the proportionality of the option in addressing the problems).

Types of impacts *(Task 7 of the ToR)**:***

- Security (achievement of the general objectives including effects on the security of citizens, companies, public authorities and other stakeholders in the EU);
- Economy (financial and economic effects);
- Fundamental rights (assessment of how the option safeguards fundamental rights[190] or any adverse effects);
- Society (cross-border mobility and the use of technology); and
- Environment.

The assessment of the necessity of EU intervention is covered in the section on the EU's right to act (see section 3.2). The issues of subsidiarity and proportionality have been addressed through the screening of the long list of options with regard to their overall feasibility. The findings of this assessment are presented in Annex IV.

The following sub-sections provide assessments of the expected impacts of each of the tree policy options, structured according to the above criteria, starting with effectiveness. For each of the criteria, three separate sub-sections are provided, referring to the specific objectives (see also section 4.1):

- *Specific objective 1:* To ensure the efficient access to and exchange of necessary information among law enforcement authorities in an intra-EU context (referring to 'SO1: Access to and exchange of information');
- *Specific objective 2:* To ensure that the growing intra-EU mobility is met with an adequate development of tailored joint operations (referring to 'SO2: Management of public order and safety); and
- *Specific objective 3:* To ensure efficient cross-border operational cooperation in relation to SOC and terrorism (referring to 'SO3: Fight against SOC and terrorism).

The main findings are summarised in a table at the beginning of each of the sections. Based on the qualitative and quantitative assessments made, the table also includes numeric ratings of the magnitude of the expected impact vis-à-vis the baseline scenario in relation to effectiveness, efficiency, as well as coherence and proportionality.

[190] This assessment refers in particular to the following Articles in the EU Charter of Fundamental Rights: Art. 2 Right to life; Art.3 Right to the integrity of the person; Art. 6 : Right to liberty and security (the extent to which the policy options are expected to increase the security in the EU will, in addition, also be assessed separately); Art. 7 : Respect for private and family life; Art. 8 Protection of personal data; Art. 17 Right to property; and Art. 45 Freedom of movement and of residence. However, some elements of the options also have impacts e.g. related to vulnerable groups, children and elderly.

Whereas the baseline scenario has been, by definition, rated with '0' in relation to each of these three criteria, the other two policy options have been scored on a scale from 1 to 5 in terms of their positive impacts, where 1 represents a very small positive impact and 5 a very large positive impact. In the same vein, -1 represents a very small negative impact and -5 a very large negative impact. A score of "0" means that the option would have the same effect as the baseline scenario.[191]

More elaborate assessments are provided after the summary tables.

Impacts under a Directive vs. under a Regulation

As outlined in section 5.1, both policy options 2 and 3 would take the form of a Directive. With regard to the assessments provided in this chapter, it is crucial to note that it is expected that the implementation of Directives would be a major step forward compared to the baseline scenario. However, the expected impacts would even be exceeded if policy option 2 or 3 would take the form of a Regulation (i.e. aligning the legal framework, processes, and technical approaches to the maximum extent possible), as the Directives would leave further lee-way to the Member States to take individual action than a Regulation.

Annex IV contains detailed information concerning the approach and methodology used to assess the impacts of the policy options in relation to the abovementioned criteria.

6.1.2 Assessment of Policy option 1: Baseline scenario

Table 10 – Baseline scenario: Summary of impacts

Criteria	Rate	Summary of assessment
Evaluation of effects		
Effectiveness	0	*SO 1: Access to and exchange of information* The baseline scenario is expected to, one the one hand, have a small positive impact as regards the achievement of this objective, most importantly since, in relation to facilitating the access to and exchange of information, Europol is expected to make further improvements to SIENA, potentially doubling the number of users. However, this is not expected to be adequate to comprehensively address the current and expected future challenges. The current differences between the national set-ups are expected to continue to exist and hamper the level playing field between Member States and SACs. In view of the expected development of organised crime activities, terrorism and additional challenges in relation to ensuring public order and safety, the already existing and planned measures will not provide an adequate response in the future.
	0	*SO 2: Public order and safety* Intra-EU operational cooperation for public order is expected to remain scarce with only few joint operations taking place in the future, mainly due to the perception of their limited cost-effectiveness, e.g. due to the limited powers of officials who provide support in other Member States and SACs than their own, and the lack of direct access to data of officials on the ground. Moreover, those joint operations that do take place are expected to continue to be inadequately based on common threat assessments / risk analyses to be efficiently implemented.
	0	*SO 3: Fight against SOC and terrorism* Operational cooperation to fight SOC and terrorism is expected to continue to be hampered by the differences between Member States' and SAC's legislation and bi-/tri-multilateral agreements governing the use of investigative tools. For example, no or limited changes are expected in the Member States and SAC, which will imply that they will continue to not consistently cover those types of borders currently not fully covered (waterways, sea and air ways), and the current variations regarding the types of offences covered, the maximum time or distance allowed, technical means of surveillance, the rights and duties of officials involved in hot pursuit etc. are likely to largely remain. This means that an efficient and coordinated response addressing the increasing cross-border challenges linked with SOC and terrorism will not sufficiently take place.
	0	**Overall assessment**

[191] The ratings are based on the triangulation of both qualitative and quantitative data collected throughout the study by means of desk research, interviews, focus groups and an online survey with EU bodies and representatives from the Member States and SAC, two technical workshops, and the Open Public Consultation.

Criteria	Rate	Summary of assessment
Efficiency	0	*SO 1: Access to and exchange of information* In the baseline scenario various measures that can potentially increase the efficiency of law enforcement cooperation in the future will be implemented – most notably through the expected improved access to and exchange of information through Europol's improvements of SIENA. 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. Therefore, it is expected that the efficiency of future law enforcement cooperation will considerably lack behind its potential, thus at least not adequately reducing undue time spent on processes, as well as delays.
	0	*SO 2: Public order and safety* Due to the expected improvements in relation to the access to and exchange of information described above, the management of public order and safety is expected to become slightly more efficient in the baseline scenario. This being said, the number and efficiency of joint operations is not likely to improve as such, since their organisation would not be further supported by the EU level and no changes to the existing national rules e.g. on the conferral of powers would be made. On balance, therefore, no major improvements are expected in relation to the efficiency in the current situation.
	0	*SO 3: Fight against SOC and terrorism* In relation to the fight against SOC and terrorism, the same argumentation applies as in relation the management of public order and safety.
	0	**Overall assessment**
Coherence and proportionality	0	*SO 1: Access to and exchange of information* 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 and the SAC are expected to remain and eventually to increase in the baseline scenario. By definition, the baseline scenario is considered proportionate.
	0	*SO 2: Public order and safety* With regard to the management of public order and safety, the existing bi-/tri-/multilateral agreements are expected to remain in place and the evidenced fragmentation and incoherencies between the Member States and SACs will not be addressed. By definition, the baseline scenario is considered proportionate.
	0	*SO 3: Fight against SOC and terrorism* The lack of further EU measures also implies that no positive impacts on the coherence and proportionality of the existing EU framework is to be expected. By definition, the baseline scenario is considered proportionate.
	0	**Overall assessment**
Types of impacts		
Security	0	The baseline scenario is expected to have a positive impact on EU cross-border law enforcement cooperation. However, the future development of the core problem and its drivers are still expected to facilitate and contribute to the growth (and economic power, see below) of organised crime groups (OCG) in the EU. Therefore, on balance, security is not expected to be adequately ensured in the baseline scenario.
Economy	0	The baseline scenario is not expected to have any positive impact on the economy in the EU.
Fundamental rights	0	In the baseline scenario, it is expected that fundamental rights could be better safeguarded. This does not mean that they are not adequately safeguarded in the baseline scenario, but that there is room for improvement, e.g. as the elements of LED are not included in some of the key legislative instruments currently applicable (as they were introduced prior to LED).
Society	0	The baseline scenario is expected to have limited, but potentially negative impacts, on societal developments such as cross-border mobility.
Environment	0	Cross-border law enforcement cooperation is expected to continue to have a small negative environmental impact.

** The overall assessment refers to the average rating in relation to the SOs*

Source: Author's own elaboration

Effectiveness

It is expected that the baseline scenario will make some minor positive contributions to achieving the objectives. This being said, in view of the expected development of organised crime activities, terrorism and additional challenges in relation to ensuring public order and safety, the already existing and planned measures will not provide an adequate response in the future.

SO1: Access to and exchange of information

The access to and exchange of information is a key means for efficient cooperation between law enforcement authorities in different Member States and SAC. The exchange of information is critical with regard to the following:

- Facilitating the performance of actual investigations by officials at the operational level;
- Obtaining judicial authorisations (information exchanged may be a necessary prerequisite, e.g. for the use of investigative tools); and
- Facilitating the prevention of issues relating to public order and safety, as well as SOC and terrorism.

In this regard, it is important to note the nature of this objective: ensuring more efficient access to and exchange of information will not *per se* lead to more efficient law enforcement cooperation (it is rather a means than an "end"), but through better availability of and access to information, more efficient law enforcement cooperation is more likely. The degree to which positive effects will materialise is, however, dependent on how the information is used.

The access to and exchange of necessary information between law enforcement authorities is expected to remain sub-optimal in the baseline scenario, continuing to cause operational problems in the daily law enforcement operations in intra-EU cross-border situations. In practice, the currently existing different and varying avenues to share information between EU Member States and with EU stakeholders will continue to be used in practice, causing delays and extra work. For example, the practice of 'fishing' is likely to remain, meaning that multiple Member States and SAC may receive the same information request without any clear link to a specific case, thus leading to duplication of work.

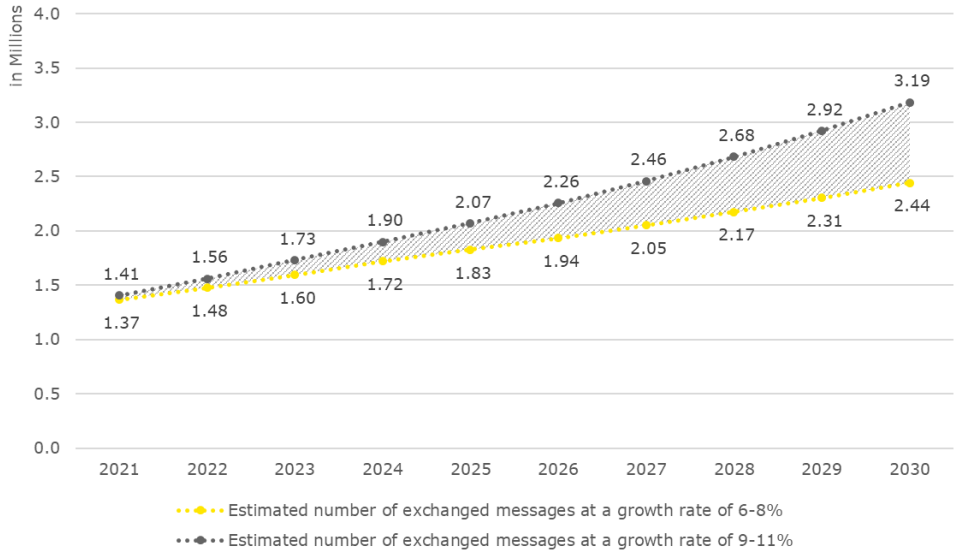
However, as indicated in the previous section on the description of the policy options, Europol is already making efforts to improve SIENA. According to Europol, close to 90,000 new cases were initiated in 2020 via SIENA between Member States/SAC, third countries, and Europol. The majority of these new cases was launched by Member States and SAC. In relation to these cases, more than 1.27 million messages were exchanged via SIENA in 2020 between its 19,000+ users. As part of an interview, France indicated that the number of exchanged messages has increased by 10% per year over the past couple of years. Moreover, Europol indicated that the measures identified in policy option 2 could contribute to increasing the number of messages exchanged on SIENA cases by 50% within the next three years.[192] Based on this, it can be inferred that the number of messages exchanged under the baseline scenario would increase somewhere within this range.

The number of messages sent via SIENA is used as a proxy for the degree to which the EU law enforcement cooperation community is active. The more messages sent via SIENA, the more active the community is. In turn, this activity is expected to result in closer law enforcement cooperation and, in the long run, increased security in the EU.

Based on available information, the expected number of messages exchanged via SIENA in the baseline scenario (policy option 1) has been modelled in the graph below.

[192] Interview conducted on 28.05.2021.

Figure 7 – PO1: Expected development of messages sent via SIENA



Source: Author's elaboration based on available evidence

It can be seen that the number of messages exchanged via SIENA is estimated to increase to 3.19 million messages in 2030 under the assumption of a medium growth rate. If a lower growth rate is assumed, the number of messages is estimated to go up to 2.44 million messages.

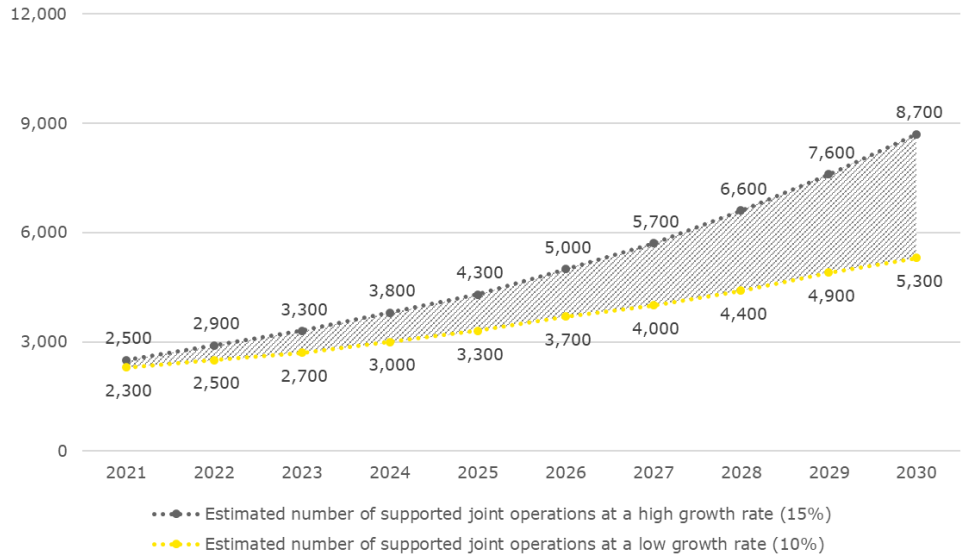
However, this is not expected to be adequate to comprehensively address the current and expected future challenges. The current differences between the national set-ups are expected to continue to exist and hamper the level playing field between Member States and SACs. In view of the expected development of organised crime activities, terrorism and additional challenges in relation to ensuring public order and safety, the already existing and planned measures will not provide an adequate response in the future. In addition to room for improvement with regard to the technicalities of information exchange, differences with regard to the resources allocated to cross-border investigations, as well as the organisational set-up of relevant units, and their operational mandate are in turn expected to continue to exist and hamper the level playing field between Member States.

SO2: Management of public order and safety

Intra-EU operational cooperation for public order is expected to remain relatively scarce with fewer joint operations taking place than relevant to ensure an efficient management of public order and safety. Based on available evidence[193] on the number of joint operations supported by Europol through SIENA between 2010 and 2019 (from 416 in 2010 to 1,874 in 2019; +350%), the following graph depicts the potential development of joint operations in the baseline scenario.

[193] Data and qualitative assessment on the potential development provided by Europol during an interview on 28.05.2021, and as a follow-up.

Figure 8 – PO1: Expected development of joint operations supported by Europol



Source: Author's elaboration based on available evidence

The graph visualises the expected degree to which the EU law enforcement community will increasingly cooperate with each other (based on available data of the historical developments concerning cross-border cases and needs for cooperation). The higher the number, the closer EU law enforcement cooperation. It can be seen that the number of joint operations supported by Europol is expected to increase to up to 8,700 joint operations by 2030 in a scenario with a high growth rate. If a lower growth rate is assumed, the number of joint operations is estimated to go up to 5,300 in the next ten years. While this is an increase in absolute numbers, this is expected to still be inadequate and continue to hamper the effort of law enforcement authorities in the future: More can be done.

The limited powers of officials who provide support in other Member States and SACs than their own are expected to remain, and the lack of direct access to data of officials on the ground is likely to continue to hamper the efficient prevention and response to situations that constitute or involve a threat to public order and safety. Moreover, those joint operations that do take place are expected to continue to be inadequately based on common threat assessments / risk analyses to be efficiently implemented, as Member States are not expected to increasingly share information.

SO3: Fight against SOC and terrorism

The intra-EU cooperation for SOC is also expected to remain (overly) complex and – to some extent - ill-suited to facilitate effective and efficient transnational investigations and operations. For example, it is expected that the Member States and SAC will continue to not consistently cover those types of borders currently not fully covered (waterways, sea and air ways), and the current variations regarding the types of offences covered, the maximum time or distance allowed, technical means of surveillance, the rights and duties of officials involved in hot pursuit etc. are likely to largely remain. As a consequence, the challenges related to the cross-border use of investigative tools to fight SOC are expected to not be effectively addressed. It can be expected that, while the overall EU framework will remain intact, the Member States and SACs will continue to use different approaches to defining (the use of) investigative tools according to bi-/tri-/multilateral agreements and/or national legislation to fight SOC. This is expected to continue to hamper the effective and efficient cooperation in cross-border criminal operations at the operational level. Ultimately, this means that an efficient and coordinated response addressing the increasing cross-border challenges linked with SOC and terrorism will not sufficiently take place.

Efficiency

While some elements of the baseline scenario are expected to make a small positive contribution to improving the efficiency of cross-border law enforcement cooperation, overall, the baseline scenario would not provide an adequate response from an efficiency perspective.

SO1: Access to and exchange of information

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.

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 SACs 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 two to four weeks in almost half of the cases in which delays occurred. Even longer delays were reported to be experienced in the largest part of the rest of the cases. Such delays are clearly hampering the efficient implementation of law enforcement operations in intra-EU cross-border cases. However, the baseline scenario also contains various measures that could potentially increase the efficiency of EU law enforcement cooperation in the future. As reported above in relation to the effectiveness criterion, most notably, Europol's envisaged improvements to SIENA could potentially contribute to speeding up the technical processes and have a significant impact on the number of users.

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 Euro.

The assumptions above are also presented in the following table.

Table 11 – Estimation of costs for SIENA and CMS

Member State package estimate[194]			
CMS for 10 MS	10 x 150.000	1,5 million Euro	***Total***: 2,5 million EUR (one-time investment needed)
SIENA integration in CMS for 20 MS	20 x 50.000	1 million Euro	
EUROPOL package (incl. improved infrastructure, etc.)			
Total: 1.7 million EUR per year (yearly investment needed). This value is expected to increase, in case SIENA would become the default channel for communication, since this would require e.g. more hardware.			

Source: Data provided by Europol

[194] The information provided should be used carefully. It should be understood as "in case a CMS is needed for 10 MS, 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.

Moreover, whereas today, the time it takes to receive feedback on a case that is marked as 'not urgent' in SIENA may be up to one week, it will be possible in the baseline scenario to reduce this 'waiting' time to only a few seconds through the introduction of automated hit/no hit functionalities. Moreover, from a purely technical perspective, it is already possible to exchange information instantaneously between countries, as well as between EU bodies and countries on a more or less automated basis.

However, at this stage, the potential efficiency gains from SIENA improvements are considered to be rather *technical possibilities* than actual commitment for implementation. The reason for this is that whereas there is a lot of potential for improvement concerning SIENA from a technical perspective, Member States' political and financial commitment to implement these potential improvements is expected to remain a barrier for more efficient EU law enforcement cooperation according to Europol.

Moreover, there are instances in which cases are currently not being dealt with as efficiently as possible, since channels such as SIENA are not permanently monitored within SPOCs and judicial authorities necessary to obtain specific permits for investigation are not always present. The limited interoperability between different large-scale IT systems (e.g. due to vast differences between various 'inhouse solutions' used in the EU), as well as the limited functionalities of the CMS in various Member States are also expected to remain and continue to hamper cross-border information exchange in the future. More specifically, these challenges are expected to continue to cause undue waiting time and delays in the future, ultimately implying that law enforcement operations may fail in instances where they could have been successful, would information exchange have been more efficient.

Overall, however, it also needs to be considered that – in the absence of further going intervention from the EU in the baseline scenario – formal and informal processes that have been established over the past years are expected to remain intact. This means that stakeholders are expected to continue to use processes that have proven themselves to in many cases work well in practice. 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. These practices may, of course, not in all cases be the most efficient ones from an outsider's and a systematic perspective. However, informal practices are a considerable part of law enforcement cooperation today and have been an important means so far. This being said, in view of the development of organised crime activities and terrorism, notably due to more sophisticated and evolving *modus operandi*, as well as additional challenges in relation to public order and safety, such traditional ways of working may no longer prove adequate in the future. More specifically, while they may work well between countries where frequent contacts and cooperation are established, other countries, with whom cooperation is currently only rarely taking place, may suffer from poor collaboration (means). In particular in view of the evolution of cybercrime, which is not bound by physical borders, in the baseline scenario it would not be adequately ensured that not only criminals, but also LEAs, are sufficiently exploiting the benefits of technological and other developments.

SO2: Management of public order and safety

Due to improvements in relation to the access to and exchange of information, the management of public order and safety is expected to become slightly more efficient in the baseline scenario. One of these improvements is a three-year project by one Member States to enhance joint operations, including a digital platform to optimise administrative and operational management with a budget of 1.4 billion EUR.[195] At the same time, however, the existing fragmentation, diverging informal practices, as well as the lack of political and budgetary commitment are expected to continue to hamper more efficient cross-border law enforcement cooperation in terms of joint operations etc. The number and efficiency of joint operations is not likely to improve as such, since their organisation would not be further supported by the EU level and no changes to the existing national rules e.g. on the conferral of powers would be made. On balance, therefore, no major improvements are expected in relation to the efficiency in the current

[195] Interview conducted on 07.06.2021

situation. On the contrary, the insufficient use of joint operations is likely to have a negative impact from an efficiency perspective.

SO3: Fight against SOC and terrorism

In relation to the fight against SOC and terrorism, the same argumentation applies as in relation the management of public order and safety.

Coherence and proportionality

The measures in place both at the EU and national levels are expected to continue to contribute to the fragmentation of the legal landscape governing EU law enforcement cooperation. By definition, the baseline scenario is considered proportionate as it gives Member States considerable leeway in terms of following their own approaches based on national legislation, as well as bi-/tri-/multilateral agreements.

SO1: Access to and exchange of information

As regards the access to and exchange of information, the identified uncertainties and inefficiencies in the intra-EU law enforcement cooperation are expected to remain and eventually to increase (e.g. due to inconsistent implementation, application and practical use in the Member States, as well as lack of political and financial commitment) in the baseline scenario.

SO2: Management of public order and safety

With regard to the management of public order and safety, bi-/tri-/multilateral agreements are expected to largely remain in place, continuing the existing fragmentation between Member States. The lack of further planned EU measures also implies that no impacts on the current incoherencies relating to the existing EU framework are to be expected. The same argumentation applies in relation to the coherence between the EU and national levels. Thus, the baseline scenario gives Member States considerable leeway which, in turn, causes increased fragmentation and uncertainty for law enforcement cooperation.

SO3: Fight against SOC and terrorism

In relation to the fight against SOC and terrorism, the same argumentation applies as in relation the management of public order and safety.

Security

Some aspects of the baseline scenario are expected to have small positive impacts on the achievement of the general objectives, i.e. ensuring security in the EU for citizens, businesses, and public authorities. This being said, as noted under the effectiveness criterion, on balance, security is not expected to be adequately ensured in the baseline scenario. The reasons are depicted below.

SO1: Access to and exchange of information

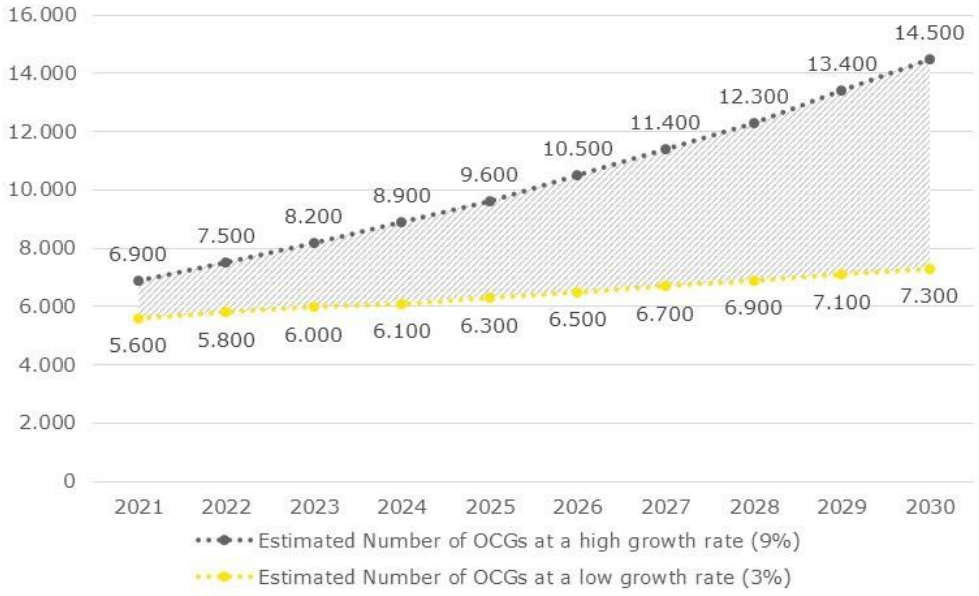
The improved access to and exchange of information is expected to have a positive impact on EU cross-border law enforcement cooperation. However, the future development of the core problem and its drivers are still expected to facilitate and contribute to the growth (and economic power, see below) of organised crime groups (OCG) in the EU.

As pointed out in the problem assessment section, this is also reflected in the EU SOCTA 2021[196], which identifies high-risk criminal networks (including corruption, money laundering and use of firearms) as the most important crime priority for the immediate future – even before cybercrime. The number of OCGs operating across-borders in the EU has increased from roughly

[196] Council of the European Union (2021): EU crime priorities for the period 2022-2025: Policy advisory document (PAD). Document nr. 7232/21. 24 March 2021.

3,600[197] in 2013 to more than 5,000[198] in 2017 according to Europol. This corresponds to an average increase of 9% per year. Based on this growth rate, the number of OCGs operating across borders in the EU today (2021) could be as high as 7,000 and could even double until 2030.[199] Even in a scenario with a lower growth rate of 3% per year, the number of OCGs operating across borders in the EU could grow up to more than 7,000 in 2030.

Figure 9 – PO1: Expected development of the number of organised crime groups

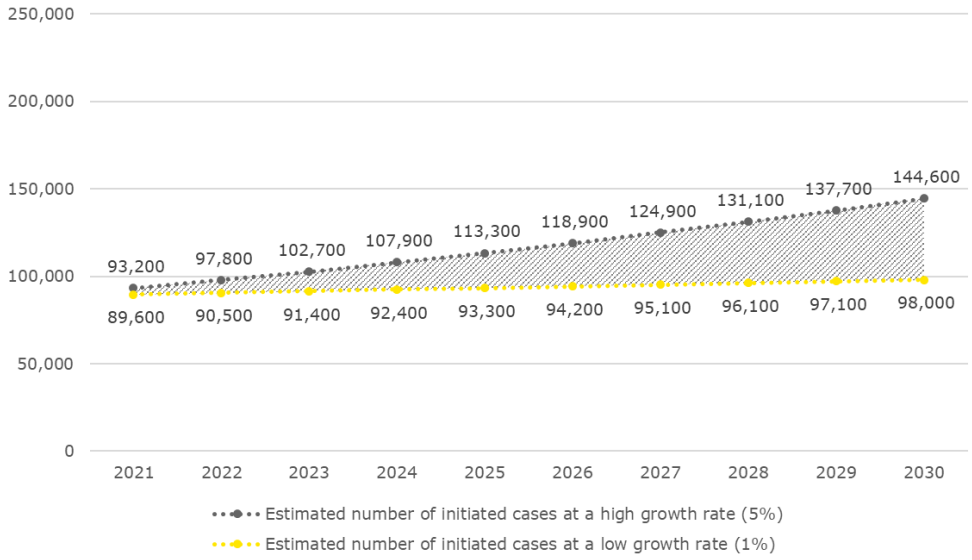


Source: Author's elaboration based on available evidence

In addition to the growing number of organised crime groups active in the EU, there is also evidence that Europol has been increasingly active over the past couple of years. Whereas in 2016, 46,437 cases were initiated, the number increased to 88,748 in 2020.[200] Based on this evidence, and corresponding to the expected development of the number of organised crime groups active in the EU above, the number of cases initiated in SIENA could increase over the next years in the way modelled in the graph below.

[197] Europol (2017), Serious and organised Crime Threat Assessment (SOCTA): Crime in the age of technology.
[198] Ibid.
[199] This estimate is based on the assumption that the number of organised crime groups can increase with a constant growth rate and that no consolidation and saturation effects, e.g. due to competition between Organized Crime Groups or the size of criminal markets affect the overall development of the number. Thus, this estimate needs to be treated with caution and the actual number of organised crime groups operating in the EU is likely to be (significantly) lower than this estimate.
[200] Europol (2020): SIENA Annual Report 2020.

Figure 10 – PO1: Expected development of the number of initiated cases in SIENA



Source: Author's elaboration based on available evidence

It can be seen that the number of initiated cases in SIENA can go up to 144,600 in 2030 if a high growth rate is assumed. If a rather low growth rate is assumed, the number of initiated cases in SIENA is estimated to still increase to 98,000 in the next ten years. However, reliable data is largely missing. Therefore, the estimates need to be treated very carefully.

The increasing number of organised crime groups active in the EU is expected to have a negative impact on citizens and businesses (in particular SMEs), as well as public authorities and other stakeholder groups. Most notably, in the baseline scenario, the number of incidents in which citizens or businesses fall victim to SOC is expected to increase in the future. In addition, the likelihood in particular of specific vulnerable groups of citizens to fall victim to SOC is expected to increase, including children, elderly, and persons with disabilities. Moreover, negative impacts are expected on persons who do not possess sufficient digital literacy to cope with the risk of cybercrime. Businesses, especially SMEs, are expected to be negatively affected largely from the expected increase in cybercrime that is expected to go along with the rise of organised crime groups active in the EU.

SO2: Management of public order and safety

With specific regard to the management of public order and safety, security concerns are expected to be more prominent in the baseline scenario than today. After the COVID-19 pandemic, more persons are expected to travel across borders and mass gatherings are expected to take place again on a more frequent basis, posing additional challenges to public order and safety. This means that room for improvement is expected to not only continue to exist, but become more important with regard to the management of public order and safety.

SO3: Fight against SOC and terrorism

In relation to the fight against SOC and terrorism, the same argumentation applies as in relation the management of public order and safety.

Economy

The baseline scenario is not expected to have any positive impact on the economy in the EU.

SO1: Access to and exchange of information

The baseline scenario can be expected to create minor positive economic impacts on markets related to IT-related products and services used for information exchange. In addition, the continuous need to procure related hard- and software is also expected to have positive impacts on the labour market and the demand for specialised expert staff.

SO2: Management of public order and safety

Neither positive nor negative economic impacts are expected in relation to the management of public order and safety in the baseline scenario.

SO3: Fight against SOC and terrorism

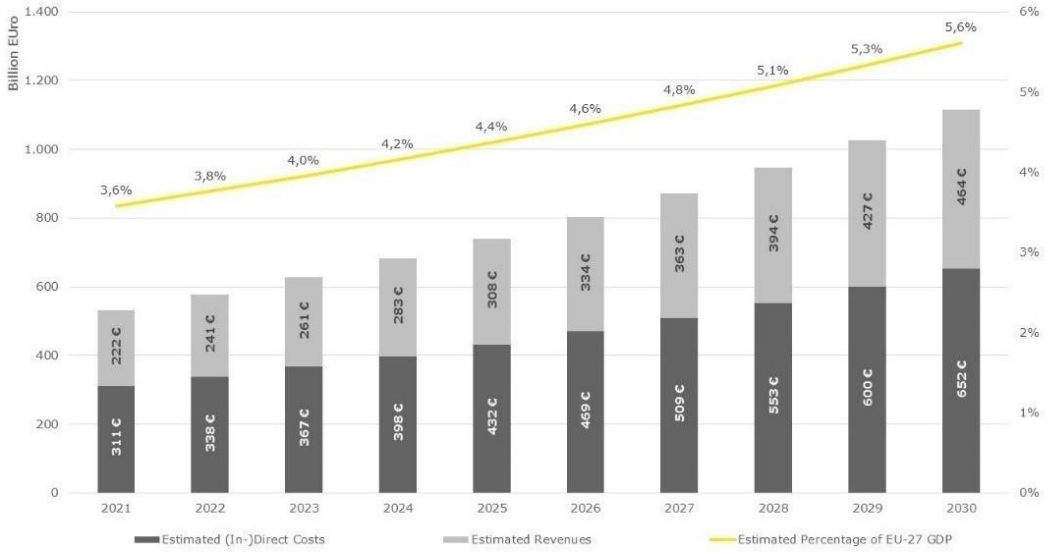
Organised crime groups are expected to exploit the increasing cross-border mobility and new technologies (see also societal impacts below) in order to realise criminal proceeds and to cause increasing harm for EU governments, businesses and citizens.

Different stakeholders are expected to continue to be affected by SOC to varying degrees and in different fashion. From an economic perspective, whereas citizens may e.g. fall victim to cash and online payment fraud, businesses – and in particular SMEs – might, for instance, be negatively affected through extortion (e.g. by means of digital ransomware), as well as the hacking of their IT systems. As a consequence, the ability of businesses to produce and service their customers may be severely impaired, leading to an overall loss of turnover and profit. This is also expected to have negative impacts on citizens' job security. The economic consequences of SOC for governments are profound: SOC severely hampers the ability of governments to collect and allocate taxes, as well as public funding – thus jeopardising the purpose and functioning of public authorities.

Available quantitative evidence concerning the problem today shows that the annual overall economic damage from OCG – i.e. the annual (in-) direct costs from their activities[201] plus the criminal proceeds[202] – could have been as high as 450 billion EUR in 2019 (around 3.2% of the EU27 GDP).

Assuming that this overall economic damage will also increase – similar to the number of OCG (see above) – at an annual rate of 9%, the overall economic damage could grow to close to 1.1 trillion EUR in 2030. This corresponds to 5.6% of the EU27 GDP.

Figure 11 – PO1: Expected development of economic caused by SOC



Source: Author's elaboration based on available evidence

The rough estimates provided above are only indicative and need to be treated with great caution as there are also sources according to which the economic impact of organised crime in the EU can be expected to be smaller. A 2020 European Parliament briefing paper[203], for instance, cites estimates from a 2016 European Parliamentary Research Service study[204], according to which

[201] Levi, M., M. Innes, P. Reuter & R. Gundur. 2013. The Economic, Financial & Social Impacts of organised Crime in the EU. As of 8 December 2020: link.
[202] RAND Europe & EY for the EC (2021) Mapping the risk of serious and organised crime infiltrating legitimate businesses
[203] European Parliamentary Research Service (2020): Understanding the EU response to organised crime. See: link.
[204] European Parliamentary Research Service (2016): organised Crime and Corruption. Cost of Non-Europe Report. See: link.

the economic loss from organised crime was estimated to be between 218 and 282 billion EUR annually, with criminal proceeds totalling around 110 billion EUR per year. According to the report, this corresponded to between 0.7 % and 1.28 % of the EU's annual GDP.

Fundamental rights

The following analysis concerns *possible risks* relating to fundamental rights based on the analysis of current practices. No detailed information or factual evidence concerning the extent to which these risks actually materialise in the Member States has been collected within the framework of this study in relation to the aspects indicated below.

In the baseline scenario, it is expected that the current practices within cross-border law enforcement cooperation could continue to have a negative impact on authorities' ability to safeguard fundamental rights. This may, for instance, refer to the following Articles in the EU Charter of Fundamental Rights that relate to security aspects (see also the assessment of security provided above):

- Art. 2: Right to life;
- Art. 3: Right to the integrity of the person;
- Art. 6: Right to liberty and security;
- Art. 17: Right to property; and
- Art. 45: Freedom of movement and of residence.

Moreover, due to the outdated provisions on data protection and privacy within the SFD, there is also room for improvement in relation to the following fundamental rights:

- Art. 7: Respect for private and family life;
- Art. 8: Protection of personal data.

Safeguarding fundamental rights is expected to continue to be a key priority for law enforcement officials in the future.

SO1: Access to and exchange of information

There are various aspects concerning the access to and exchange of information in relation to which safeguarding fundamental rights could be improved in the baseline scenario. There is, for instance, a risk that existing law enforcement databases are subject to inherent, unconscious biases and stereotypes (e.g. ethnicity, gender, sexual orientation, culture and religion, citizenship, (dis-) ability etc.). Thus, the exchange of information within the framework of the currently applicable legislative instruments is expected to continue to exacerbate this risk.

Moreover, 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 is expected to have a negative impact on the extent to which law enforcement authorities are able to safeguard citizens' fundamental rights.

In a similar vein, the use of different information channels in addition to SIENA does not ensure as efficiently as possible law enforcement processes. Thus, citizens face undue processing time in case they are wrongfully subject to a criminal investigation.

On the flipside, this also means that in case criminals are rightfully suspected but law enforcement processes take undue time, citizens may be negatively affected in the baseline scenario as criminals may have considerable leeway to commit further crimes – thus negatively impacting e.g. on citizens' right to liberty and security, right to life and right to property.

Moreover, there are situations in which officials "fish" for information via various channels and from various Member States and SAC regarding a case. This is expected to potentially compromise (undue) suspects' fundamental rights. The same is valid in relation to existing forms and the lack of an automated display of a hit/no hit indication: Both are expected to prolong law enforcement cooperation processes and, therefore, put an undue burden on citizens and their fundamental rights.

In the baseline scenario, more often than not, case management is distributed across several platforms and layers. The complexity of available CMS is, in turn, be an enabler of officials to access and exchange information they should, under given circumstances, not be able to access and exchange. Therefore, the current landscape of Member States' CMS is expected to pose a risk for safeguarding fundamental rights. Actual examples of such instances have, however, not been identified in the framework of this assignment.

Finally, 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 citizens' right to privacy, liberty and security.

SO2: Management of public order and safety

As concerns the management of public order, critical issues exist in case citizens are wrongfully detained without law enforcement authorities having adequate possibilities to appropriately and swiftly check relevant databases for pre-existing information (e.g. if the apprehended person actually is the person that officials had been looking for). Thus, the lack of remote access to relevant law enforcement databases in specific situations is expected to continue to be a risk for safeguarding citizens' fundamental rights.

SO3: Fight against SOC and terrorism

The existence of only relatively narrow provisions concerning specific investigative tools (e.g. surveillance) can be expected to continue to hamper fundamental rights of victims of SOC, in particular children and other vulnerable persons who are more at risk than others to be subject to trafficking in human beings, slavery and forced labour.

Society

The baseline scenario is expected to have limited, but potentially negative impacts on societal developments such as cross-border mobility. The take-up of modern technology by citizens, businesses and public authorities, e.g. in relation to secure online services (communication, banking, shopping etc.) which could potentially be exploited by organised crime groups, is not expected to be affected.

SO1: Access to and exchange of information

While there is great potential for LEAs to become more efficient in addressing intra-EU cross-border cases than they are today by making use of relevant technological developments, such as a "law enforcement cooperation app" for information exchange, direct remote access to databases across all countries etc., there is low feasibility for a common adoption of such tools with or without EU action due to political feasibility and subsidiarity considerations. Hence, the positive effects that are possible in the baseline scenario are expected to not fully materialise. Instead, OCGs are more likely to use technological possibilities, becoming more challenging to catch, in particular in cross-border contexts.

SO2: Management of public order and safety

Two of the major drivers and enabling factors of SOC, as well as situations that are critical to manage from a public order perspective are cross-border mobility of criminals and citizens, as well as the use of technology.

After a COVID-19-induced dip, cross-border mobility within the EU and Schengen areas is expected to become even more frequent than before – at least in the long-run and in relation to tourism both for leisure and for attending (mass) events. While both the number of citizens within the EU and Schengen area, as well as the share of persons that have relatives and/or friends in other countries than their home country are increasing, backlog and catch-up effects can be expected to spur cross-border mobility after the COVID-19-pandemic has settled. This is expected to continue to pose challenges for the fight against SOC and the management of public order and safety in the baseline scenario.

Driven through the pandemic, the shift of both personal and professional aspects of life towards the digital world is expected to continue to increase. The increasing use of, for instance, online communication tools, digital shopping and banking services, as well as tools for digital identification are expected to continue to set the stage for perpetrators to commit further cyber and financial crimes in the baseline scenario.

SO3: Fight against SOC and terrorism

In relation to the fight against SOC and terrorism, the same argumentation applies as in relation to the management of public order and safety.

Environment

Cross-border law enforcement cooperation is expected to continue to have a small negative environmental impact.

SO1: Access to and exchange of information

The negative environmental impact mainly stems from the use of electricity in relation to computers and servers used for information exchange and case management, as well as mobile phones and in relation to light etc. in law enforcement authorities' offices. Moreover, these offices are expected to continue to have a negative effect due to heating.

SO2: Management of public order and safety

On the more operational side, a negative impact from CO2 emissions will remain in the future, e.g. stemming from physically moving staff between locations, e.g. for joint operations, or in relation to hot pursuits. Overall, however, the environmental footprint of law enforcement activities that specifically concern cross-border cooperation is considered negligible in the baseline scenario.

SO3: Fight against SOC and terrorism

In relation to the fight against SOC and terrorism, the same argumentation applies as in relation the management of public order and safety.

Effects of the policy option 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.[205]

Table 12 – PO 1: Impacts on different types of stakeholders

			SO 1: Access to and exchange of information	SO 2: Operational cooperation for public order and safety	SO 3: Operational cooperation to fight SOC and terrorism
Public authorities	Law Enforcement Authorities	SPOCs			
		PCCCs			
		Other			
	Judicial Authorities				
	Data Protection Authorities				
NGOs					
Citizens / Businesses					

Source: Author's own elaboration

[205] 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.

6.1.3 Assessment of Policy option 2: Legal proposal on minimum standards + supporting (soft) measures

Table 13 – Policy option 2: Summary of impacts

Criteria	Rate	Summary of assessment
Evaluation of effects		
Effectiveness	4	<u>*SO 1: Access to and exchange of information*</u> Policy option 2 is expected to achieve this policy objective to a large extent. Notably, it is expected to facilitate to a large extent the swift exchange of a (minimum) standard set of data via one main channel and, thus in turn contribute to the ability to more effectively fight SOC and manage public order. Moreover, it 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. Ultimately, this option will make sure that Member States and SACs have a notable increased security and awareness of the types of data they can access and within what time they will be able to obtain the data.
	4	<u>*SO 2: Public order and safety*</u> The policy option is expected to have a moderate positive effect on cross-border operational cooperation for public order and safety. The benefits will mainly be due to: • More clarity on and increased powers of officials who provide support in other Member States and SACs than their own, meaning that they will be able to take on a more operational role than what is currently often the case. This will have a direct impact on the cost-effectiveness of involving officials from other Member States/SAC; they will no longer be reduced to spectators or be able to provide very limited support, but there will be more potential for giving them important operational tasks. • Increased possibilities for direct/remote access to data of officials on the ground that are involved in ensuring public order and safety concerning specific events in specific locations. This will reduce the time taken to access data and will significantly increase the possibilities to rapidly identify whether certain data are available or not. • An increased number of joint operations, due to the possibility to obtain financial support for costs that are not incurred for operations within the own Member State/SAC. • Moreover, those joint operations that do take place are expected to be more efficient based on common threat assessments / risk analyses.
	3	<u>*SO 3: Fight against SOC and terrorism*</u> Policy option 2 is expected to have a moderate positive effect on the fight against SOC and terrorism. Those types of borders currently not fully covered (waterways, sea and air ways) will be commonly addressed in all Member States and SAC, meaning that efficient responses are not hampered by the types of borders that are crossed by criminals. Moreover, a common definition of the types of offences covered, the maximum time or distance allowed, technical means of surveillance, the rights and duties of officials involved in hot pursuit etc. will significantly facilitate the use of investigative tools in cross-border situations. This means that an efficient and coordinated response addressing the increasing cross-border challenges linked with SOC and terrorism can take place to a higher degree than what is currently possible.
	3.7	**Overall assessment**

Criteria	Rate	Summary of assessment
Efficiency	4	*SO 1: Access to and exchange of information* It is expected that this policy option will contribute to increasing the efficiency of EU law enforcement cooperation to a large extent. The measures foreseen under this policy option are expected to contribute to reducing the undue time officials need to devote to cross-border law enforcement cooperation. PO 2 can therefore be considered to have a large positive impact on efficiency. Most notably, the access to and exchange of information is expected to be become swifter through establishing SIENA as the preferred channel for information exchange, introducing common data requirements and deadlines, as well as minimum standards for CMS. As a consequence, law enforcement officials are expected to be able to spend more time on 'solving' cross-border cases rather than 'administrating' them. This way, in turn, efficiency gains are expected to contribute positively to the efficiency of the policy option, as well as overall security impacts. There will, however, be a need for some investments as part of this policy option. This includes the need for IT-and staff-related investments at both the EU and national levels. Moreover, there will be an increased need for training of officials through the introduction of this policy option.
	3	*SO 2: Public order and safety* Overall, this policy option is expected to lead to more efficiency in relation to ensuring public order and safety. As noted under effectiveness, more clarity on and increased powers of officials who provide support in other Member States and SACs than their own will have a positive impact on the cost-effectiveness of involving officials from other Member States/SAC; they will be able to provide more comprehensive support than under the baseline scenario (including potentially more important operational tasks). Providing officials on the ground with increased possibilities for direct/remote access to data in the framework of specific events in specific locations will require some IT investments. On the other hand, through the direct (remote) access to the relevant data the time taken to access data will be reduced, as well as staff costs, as no intermediary based in an office will be necessary to involve, and will significantly increase the possibilities to rapidly identify whether certain data are available or not. The expected increase in the number of joint operations under policy option 2 is expected to necessitate increased budgetary spending from the Member States, but will also be supported by the EU, which will provide financial support for certain costs in relation to joint operations. Those joint operations that do take place are expected to be more efficient based on common threat assessments / risk analyses.
	4	*SO 3: Fight against SOC and terrorism* Increased use of technology-supported investigative tools will enable law enforcement officials to conduct their investigations quicker and at less operational costs. It is, however, expected that Member States would need to invest in such technology, as well as in relation to respective training for officials.
	3.7	**Overall assessment**
Coherence and proportionality	4	*SO 1: Access to and exchange of information* The policy option is expected to have a large positive impact on increasing the coherence of the legislative framework at both the EU and national levels governing cross-border law enforcement cooperation. The measures are considered proportionate.
	4	*SO 2: Public order and safety* The coherence with bi-/tri-/multilateral agreements and national legislation varies, depending on the respective measures enshrined in this option. However, the overall direction and intention of measures under this option appear to be coherent with those of many agreements, as well as most national legislation. A lack of coherence in this context is mainly justified by differences in operational details, rather than diverging overall objectives. The measures are considered proportionate.
	4	*SO 3: Fight against SOC and terrorism* The focus of this option on the establishment of minimum standards and minimum common requirements as well as the streamlining of existing approaches has a positive impact on its coherence with existing measures on all levels analysed. The measures are considered proportionate.
	4.0	**Overall assessment**

Criteria	Rate	Summary of assessment
Types of impacts		
Security	3	The measures foreseen under this policy option are expected to have moderate positive impacts on ensuring security in the EU for citizens, businesses, and public authorities. By increasing and improving the information base, the measures foreseen under this option in relation to access to and exchange of information can be considered an enabler for the implementation of joint operations, as well as the use of investigative tools. However, information and intelligence collected through joint operations for public order and safety, as well as through the use of investigative tools may – once exchanged with other Member States – inform other, non-related investigations and procedures within respective jurisdictions (both in relation to cross-border and domestic situations).
Economy	2	Policy option 2 is expected to have a small positive impact on the economy. Naturally, organised crime groups are also still expected to cause economic harm for citizens, businesses (in particular SMEs), and governments under this policy option – however, to a slightly lesser extent than in the baseline scenario.
Fundamental rights	3	Policy option 2 is expected to improve EU safeguards for fundamental rights in the EU and SAC to a moderate extent, including the freedom of movement and of residence. In addition, the measures are aimed at improving citizens security in the EU and, thus, are expected to contribute to ensuring the personal liberty and security. The measures foreseen under policy option 2 are expected to be fully coherent with the GDPR, as well as the Data Protection Law Enforcement Directive – thus appropriately protecting citizens' personal data whenever and wherever it is used for the purpose of law enforcement cooperation.
Society	1	The measures foreseen under this policy option are expected to increase the security for citizens and businesses in the EU to a moderate extent. This is in turn expected to have a positive impact on cross-border mobility of citizens and businesses, including in relation to personal travel for tourism. No impact is expected on the uptake of technology by citizens and businesses.
Environment	1	Policy option 2 is expected to have an overall very small to negligible environmental impact.

** The overall assessment refers to the average rating in relation to the SOs*

Source: Author's own elaboration

Effectiveness

Overall, in terms of **effectiveness**, policy option 2 is expected to achieve the policy objectives (see section 4.1) to a large extent.

SO1: Access to and exchange of information

Policy option 2 contains a comprehensive set of measures that aim at facilitating the **access to and exchange of necessary information** among law enforcement authorities in an intra-EU context.

Positive impacts are, for example, expected to stem from the combination of the following measures that aim to address current **legislative barriers**:

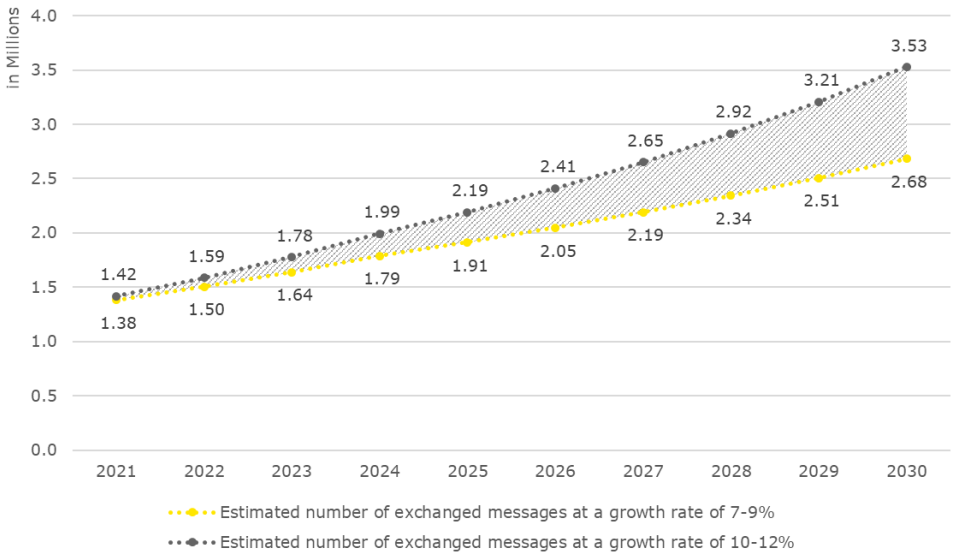
- **Access to data in other Member States**: The establishment of requirements concerning (i) a common minimum set of data that all Member States and SAC need to provide in combination with (ii) an explanation of the factual reasons for the information request, and (iv) ensuring the compliance with the deadlines by which the data are to be made available will make sure that Member States have a notable increased security in relation to the types of data they can access and within what time. In addition, information concerning additional data that are available in each Member State will be provided online (through a non-legislative flanking measure), which will have additional positive effects, and also contribute to addressing the current problem that Member States and SAC do not know which data they may be able to obtain from other countries.
- **Communication channel to be used**: The establishment of SIENA as the preferred channel of communication for intra-EU cases (unless other EU information channels have

to be used) and the foreseen extension of the functionalities of SIENA (going beyond those changes already planned by Europol) will mean that information exchanges will be more efficiently handled via one common channel for information exchanges in relevant cases.

These measures will thus enable the Member States and SAC to identify, as well as swiftly request and receive the most crucial information their counterparts in other countries can be expected have for their investigation or operation via the appropriate channel. Since the measures are expected to increase the clarity of what can reasonably be expected from other countries in specific cases, the policy option is expected to significantly increase the extent to which authorities can effectively fight SOC and manage situations that are critical for public order and safety due to prompter access to the information they need. It has to be noted, however, that under this policy option, the use of SIENA as the preferred channel would only apply to information exchanges with other Member States and SAC (intra-EU exchanges). Where third countries are involved in the information exchange, i24/7 is rather to be used in order to avoid that both i24/7 and SIENA are used in parallel.

Similar to the baseline scenario, the expected number of messages exchanged via SIENA provides an important indicator for efficient information exchange, and can also be used as an important statistical source of information in case Europol is informed about the exchanges, as is foreseen under this option. The expected effects under policy option 2 have been modelled in the graph below.

Figure 12 – PO2: Expected development of messages sent via SIENA



Source: Author's elaboration based on available evidence

It can be seen that the number of messages exchanged via SIENA is estimated to increase to 3.53 million messages in 2030 under the assumption of a high growth rate. If a lower growth rate is assumed, the number of messages is estimated to go up to 2.68 million messages. This is an increase of 240,000 to 340,000 messages sent in 2030 compared to the baseline scenario (+10%).

The foreseen extensions of the functionalities of SIENA under this policy option seamlessly add on to the efforts Europol is currently making to develop SIENA further (see the description of the baseline scenario in section 5). However, Europol also pointed out that there are vast differences between the 15 identified SIENA user groups: Some may use SIENA only twice a month whereas others may use it multiple times daily. Therefore, Europol emphasised that in order to maximise the positive impact of SIENA a 'one size fits all' approach should be avoided. Instead, account needs to be taken of differing user demands and capabilities in order to realise the potential SIENA has for effective law enforcement cooperation. This means that, in order to increase SIENA's contribution to the effectiveness of law enforcement cooperation, the system needs to be as tailor-made as possible to individual users without jeopardising its large scale application.

In a similar vein, the representatives of an EU Member State indicated in an interview that, although they use SIENA already very frequently as their most important information exchange channel, their law enforcement authorities would greatly benefit from even more Member States and SAC using SIENA as the preferred channel.[206] In addition, stakeholders have also emphasised that knowing in advance what types of data can, at the minimum, be expected from other countries' counterparts is a key enabler for national procedures since information gaps can effectively be filled – and criminals eventually be caught quicker. This was confirmed by the participants of the 2nd technical workshop, held in May 2021. A large majority of the participants indicated in breakout session 1 that the package of measures centred around information exchange would have a positive or very positive impact.

According to the Schengen evaluation reports, however, only a handful of countries would be affected in practice if SIENA was established as the preferred channel for intra-EU information exchange (see Annex IV, five countries indicated they would prefer SIENA. Four countries indicated that i24/7 is their preferred communication channel. 17 countries declared that they are indifferent with regard to the choice of channel. 5 countries did not provide information). It can be inferred that the evidence gathered points to differences between established practices in the field and the processes foreseen 'on paper' – therefore, there is a need to clarify which channel should be used under which circumstances. This also corresponds to evidence derived from the Schengen evaluation reports that indicates that close to half of the countries use the forms contained in the SFD to a limited extent.

Additional supporting evidence is provided in Annex IV.

At the more **technical level**, the positive impacts of this policy options on the effectiveness of law enforcement cooperation are expected to stem from:

- The definition of common requirements for functionalities of the CMS;
- The establishment of the need for an accreditation of the CMS; and
- The establishment of quality control mechanisms within the CMS.

Interviewees from Member States and SACs, as well as participants to the 2nd technical workshop in May 2021 pointed out that there are currently vast differences between countries with regard to the level of development of their CMS. While some countries do not seem to work with a modern CMS in relation to cross-border law enforcement cooperation, other countries have large-scale IT systems in place that are seamlessly interoperable and integrated with SIENA. Thus, the measures identified above are expected to contribute to level the playing field in terms of technical progress of law enforcement cooperation between countries and, thus, facilitate the access to and exchange of information. This is expected to contribute to an increasingly effective law enforcement cooperation in the future in terms of fighting SOC, as well as managing public order and safety: Data can be exchanged in a more structured and sifter way, the case management is more streamlined and efficient, there is more clarity concerning what can be expected from other Member States.

This was largely confirmed by Member State during the 2nd technical workshop in which the large majority of participants of breakout session 1 indicated that the envisaged measures centred around national CMS for SPOCs would have a (very) positive impact on cross-border law enforcement cooperation.

In one interview, the representatives of a Member State pointed out that existing CMS are typically based on inhouse solutions and, consequently, not necessarily tailored to the needs of cross-border law enforcement cooperation.[207] According to them, any EU solution would have to find a common ground between existing systems and, to the extent possible, build 'on top' in order to maximise the extent to which the systems used in practice can be used seamlessly. The interviewees also pointed to the financial costs that the introduction of common minimum requirements for functionalities, accreditation and quality control of Member States' CMS may have (see the section concerning efficiency below).

[206] Interview conducted on 27.05.2021.
[207] Interview conducted on 19.05.2021.

Additional supporting evidence is provided in Annex IV.

The information contained in the Schengen evaluation reports shows that countries' interpretation of what a SPOC is and what its duties are differ from each other. For instance, 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. SPOCs also vary in their types of authorities involved in the SPOC. For instance, in C20, the International Relations Unit serves as a SPOC. This unit is under the umbrella of the Deputy Commissioner for Administration and Security and encompasses three units (Europol, SIRENE, and Interpol). The C17 SPOC is divided into two sub-units. Whereas one sub-unit is the national coordination centre on a 24/7 basis, the other sub-unit is responsible for international police cooperation on a 24/7 basis. In C5, the SPOC hosts the Interpol National Central Bureau, the National Unit of Europol, the National SIRENE bureau, the contact point for Prüm and the SFD, the contact point for the Police Working Group on Terrorism, and the liaison officials' network.[208]

While this indicator does not constitute adequate evidence for a need for EU action on its own merit (other indicators, such as a lack of access to all relevant databases are more important in this regard), it provides an indication that, at the **structural level**, there is great potential for impacts to be realised through the measures aimed at establishing minimum requirements under policy option 2. More specifically, positive impacts of policy option 2 in terms of access to and exchange of information are expected to stem from establishing the SPOC as a "one stop shop" for LEA cooperation in all Member States and SAC. More specifically:

- 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 of the SPOCs have a negative impact on the speed with which information can be exchanged. Here it is important to note that policy option 2 would not involve the EU prescribing that certain new access rights are given to specific law enforcement officials in the Member States and SAC; it would merely imply that officials who *already have* those relevant access rights (as provided for by the Member States and SAC) are involved in the SPOC.
- The requirement to have a judicial authority available 24/7 "within" the SPOC (this person would not necessarily need to be physically present within the SPOC) 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 met also in these cases. At present, deadlines are almost always exceeded where 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 better informed future action. It will, however, also mean that the SPOC will have better possibilities to assist with information exchanges if needed and be able to draw on the vast expertise and experience of cross-border cooperation of those involved in the SPOC.

As part of the 2nd technical workshop the majority of representatives in breakout session 1 on information exchange confirmed that the set of measures that is foreseen under policy option 2 is expected to have a very positive impact on intra-EU law enforcement cooperation – in particular the requirements to have access to a judicial authority 24/7, as well as to ensure access to EU and international law enforcement databases.

In addition, interviewees from several Member States and SAC confirmed the need to adequately reflect the practical importance of SPOCs (and PCCCs) within countries' national set-ups.[209] The foreseen measures are expected to increase trust between national authorities in the ability to effectively deal with urgent cases in a timely manner and to provide adequate feedback so that ongoing investigations and operations are not stalled. It was pointed out that through the introduction of the foreseen measures, officials are required and enabled to be even more informed and responsive than today – thus contributing to ensuring that SOC is fought and

[208] Schengen evaluation reports: C5, C17, C20.
[209] Interviews conducted on 19./27./28.05.2021.

public order managed more effectively across borders. More specifically, whereas in some Member States only indirect access to border guards' or customs databases is available, the implementation of direct access would greatly facilitate the practical cooperation.

Overall, this is expected to lead to time savings and reduced waiting time in the operational procedures, as well as reduced incidences of delay. One interviewee estimated that, for instance, in a non-urgent information request, the introduction of the foreseen measures could cut the waiting time for feedback from around 5 working days to mere seconds.[210] In turn, this is expected to speed up processes in the requesting country and, thus, contributes to more effective law enforcement overall.

This being said, there are some limitations to the measures foreseen in this option, as they would only be applicable to SPOCs and not to PCCCs.

Additional supporting evidence is provided in Annex IV.

One of the crucial enablers that was pointed out by stakeholders is – in order to maximise the positive impact of the foreseen measures – the establishment of appropriate training.

SO2: Management of public order and safety

In addition to measures relating to specific objective 1, policy option 2 also contains measures that are aimed at ensuring that the growing intra-EU mobility is met with an adequate development of tailored joint operations (specific objective 2).

As concerns tailored joint operations, the measures foreseen under policy option 2 (see Table 8) are expected to contribute to a moderate extent to improved quality and effectiveness of operational cooperation for public order and safety.

Both the introduction of new provisions on the conferral of powers, as well as on the remote access to relevant law enforcement databases in specific situations were welcomed by the participants of breakout session 2 during the 2nd technical workshop. The (large) majority of participants indicated that this would have a (very) positive impact on law enforcement cooperation. The same is valid in relation to measures fostering the joint development and cross-border sharing of risk analyses and threat assessments.

With specific regard to the mobile/remote access to databases, the evidence contained in the Schengen evaluation reports shows that 10 countries have full, 6 countries have limited, and 14 countries have no mobile access to law enforcement databases. Thus, any legislative changes in this regard could at least be expected to affect 20 countries.

The feedback received also shows that there is considerable appetite by the countries for EU Commission funding of joint operations in order to facilitate the political negotiations for necessary budget allocations.

The participants pointed out that one of the main impacts of the policy option is expected to be increased awareness of officials at different levels of joint operations – both in border regions, as well as between countries that do not share a border directly. Moreover, it was emphasised that joint operations are expected to benefit from the more comprehensive information available for the operational planning.

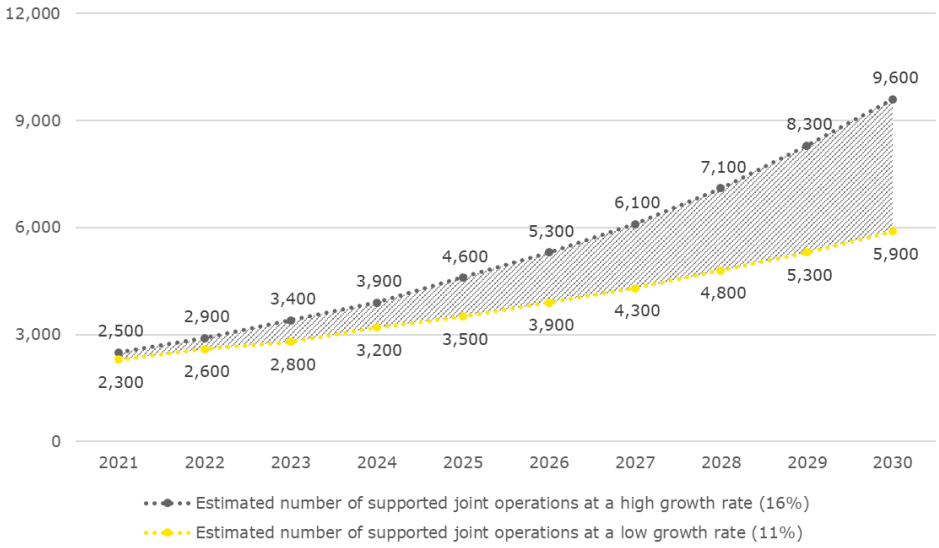
However, workshop participants did not indicate that this would 'automatically' also lead to an increased frequency of joint operations in the future. In fact, it was pointed out that, in order for more joint operations to take place in an even smoother manner, even more effective and user-oriented training measures at different levels are imperative.

Based on the information provided by Europol[211] (see also the explanation in relation to the baseline scenario), the following graph depicts the potential development of joint operations due to the measures foreseen under policy option 2.

[210] This does, however, not mean that the time needed to solve cross-border cases would be reduced from several days to a few seconds. In practice, law enforcement officials do not just 'wait' for information from their counterparts in other countries – instead, they act on different parallel investigation streams simultaneously. However, since the feedback on a specific enquiry would be obtained quicker, the overall speed of the investigation process is expected in to increase.

[211] Data and qualitative assessment on the potential development provided by Europol during an interview on

Figure 13 – PO2: Expected development of joint operations supported by Europol



Source: Author's elaboration based on available evidence

It can be seen that the number of joint operations supported by Europol is expected to increase to up to 9,600 joint operations by 2030 in a scenario with a high growth rate. If a lower growth rate is assumed, the number of joint operations is estimated to go up to 5,900 in the next ten years. This is an increase of 600 to 900 joint operations in 2030 compared to the baseline scenario (+10%).

SO3: Fight against SOC and terrorism

The measures foreseen under policy option 2 that are aimed at ensuring efficient cross-border **operational cooperation in relation to SOC and terrorism are expected to achieve this objective to a moderate extent.**

The participants of the 2nd technical workshop indicated during breakout session 3 that in particular concerning surveillance and hot pursuit the foreseen measures are expected to have (very) positive impact in terms of improving the ability to fight against SOC and terrorism. In addition, the participants confirmed that the measures are expected to increase the overall clarity of the applicable legislation.

Interviewees from one Member State pointed out that ensuring streamlined possibilities to use technical means of surveillance in other countries could increase the frequency of cross-border surveillance by up to 30% over the next couple of years.[212] This increased application of cross-border surveillance is expected to increase the extent to which perpetrators of SOC can effectively be detected and arrested in cross-border cases.

Moreover, this is also expected to contribute positively to the efficiency of cross-border surveillance (see the section below).

As regards hot pursuits, the interviewees indicated that establishing stable and secure means of radio communication are a crucial enabler for operational success. It was pointed out that in up to 25% of cross-border cases, officials in a hot pursuit lose the radio communication signal between them and their counterparts in the mission control. This can potentially have severe negative effects on the ability of officials to pursue perpetrators. Given that cross-border hot pursuits take place rather frequently and on short notice (e.g. once per week), the reduction of problems in relation to radio communication is a crucial enabler for the effectiveness and success of cross-border cooperation to fight SOC and terrorism. In this regard, the LEWP's work in relation to the European fleet map could be an integral step forward.

According to the information contained in the Schengen evaluation reports, the measures foreseen under policy option 2 are expected to have different impacts on different clusters of

28.05.2021, and as a follow-up.
[212] Interview conducted on 27.05.2021.

countries. Whereas, for instance, only a few countries would be affected by legislative changes in relation to distance limits for surveillance, the majority of countries would be affected by legislative changes concerning the surveillance techniques specified in national law. Similar is valid in relation to hot pursuits and controlled delivery.

Additional supporting evidence is provided in Annex IV.

Efficiency

It is expected that policy option 2 will contribute to increasing the efficiency of EU law enforcement cooperation to a large extent.

SO1: Access to and exchange of information

Already in the baseline scenario, efficiency gains can be expected through the steady improvements of SIENA. However, these will potentially be counteracted by the lack of or limited political and financial commitment at the national level to implement technical developments. Under policy option 2, however, the measures foreseen legally mandate the implementation of measures which, in turn, is expected to serve as a catalyst for improved efficiency of law enforcement cooperation.

Establishing a common minimum set of data that has to be made available for exchange, as well as establishing SIENA as the preferred 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.[213]

The costs associated with SIENA under policy option 2

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

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 50,000 EUR take into account 30,000 to 40,000 EUR 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.

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

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.

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.[214] The data stems from Poland and is provided in the following table.

Table 14 – 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 4.38 million EUR were

[214] 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

allocated.[215] In addition, there is IT-related budget allocated in each of the 16 federal states. In Bavaria, for instance, around 2.15 million EUR were devoted to the procurement and rental of hard- and software in 2020.[216] A very rough estimate of the overall IT-budget allocated to the German police forces (both federal and state levels) could, therefore, be between 28 and 39 million Euro.[217] 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 5,6 to 7.8 million EUR – 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 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 100,000 Euro.

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.

[215] 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
[216] 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
[217] The budget of the state levels could e.g. range between 1.5 and 2.15 million Euro.

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.

Table 15 – 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
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: Author's own elaboration

SO2: Management of public order and safety

With particular regard to the efficiency of measures in relation to **public order and safety**, the expected increase in number of joint operations under policy option 2 is expected to necessitate increased budgetary spending from the Member States. During the first technical workshop, for instance, the typical costs for joint patrols were illustrated by representatives of two countries:

- France indicated that in 2019, 93 French officials were sent to Croatia in relation to a multi-day joint patrol. For each person, at least 650 EUR (without salary) were accounted for in relation to the costs of deployment (daily allowance, insurance), as well as the costs of transport to and from the hosting country. Thus, the costs for this single illustrative example were at least 60,450 EUR on the French side. In addition to this, Croatia as the host country had to pay the costs of accommodation, food, fuel within their territory, as well as appropriate health care.
- France is also working on an electronic platform project that would cost 1,400,000 EUR in a four-year time frame. This platform should allow for real-time communication for enhanced cooperation. The platform should be accessible via computers and mobile phones. Mobile access would be needed so that agents on the ground can access the platform easily. To set up a mobile app linked to that platform would cost 100,000 Euro. The Dutch representative indicated that, in terms of costs for such a technical solution, the Dutch government had earmarked between 700,000 and 800,000 Euro.
- Czechia illustrated that a typical joint patrol may necessitate costs on the side of the hosted country of around 94,500 EUR for 40 officials and four drivers over a timeframe of eight weeks. In addition, the representative indicated that over the summer, joint patrols are less expensive for the hosted countries (618 EUR per person for one month).

France illustrated that 235 foreign officials were hosted in 2019, totalling at least 145,230 Euro.

Given that the number of joint operations is expected to increase (see also Figure 13 concerning the expected development of joint operations supported by Europol), significant investments are expected in relation to operational cooperation for public order and safety under policy option 2.

There are various additional (non-) legislative measures at EU and national 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.

Table 16 – Estimates for addition costs at EU-level related to information exchange

Measure	Cost estimate in Euro
EU level	
Establishment of an appropriate financial instrument by the Commission (e.g. through the ISF) to contribute to the funding of joint patrols in terms of staff costs; travel costs; accommodation; and expenses.	5.0 - 7.5 million
Perform a pilot project to identify approaches to improve the development and use of joint threat assessment and risk analysis.	750,000 – 1,000,000
Development of data collection tools (questionnaire and manual) specifically for customs.	25,000 – 50,000
Awareness raising and training.	500,000 – 750,000
National level	
Implementation of remote access to relevant law enforcement databases in specific situations.	3.0 - 4.5 million
Cooperation with neighbouring Member States to develop and use cross border threat assessment to better assess the need for joint operations and better inform their planning.	25,000 – 50,000 per Member State

Source: Author's own elaboration

SO3: Fight against SOC and terrorism

As concerns the fight against SOC, the representatives of Slovenia indicated during an interview[218] that the increased use of technology-supported investigative tools will enable law enforcement officials to conduct their investigations quicker and at less costs. For instance, cross-border surveillance operations could potentially be conducted at 20% less costs if, instead of additional staff, modern technology such as GPS trackers and drones were used to a larger extent. The policy option is not expected to lead to any major additional implementation costs as such. On balance, the efficiency of this policy option would thus be high.

Additional supporting evidence is provided in Annex IV.

Coherence and proportionality

The policy option is expected to have a large positive impact on increasing the coherence of the legislative framework at both the EU and national levels governing cross-border law enforcement cooperation. The measures foreseen are considered proportionate in view of the efforts required by Member States to develop further existing national legislation, as well as bi-/tri-/multilateral agreements.

In comparison with **horizontal EU objectives**, policy option 2 is assessed to be coherent. The streamlining, clarification and expansion of measures aiming to ensure an efficient information exchange between Member States, an adequate development of tailored joint operations as well

[218] Interview conducted on 28.05.2020.

as efficient cross-border operational cooperation in relation to SOC and terrorism support the EU's overall objectives, notably:

- To promote peace and the well-being of EU citizens;
- To offer EU citizens freedom, security and justice; and
- To build and support a trustful cooperation between Member States.

Same as for the horizontal EU objectives, policy option 2 is considered coherent with **existing binding and non-binding EU measures**. This assessment is based on the fact that most of the measures proposed under this policy option represent a streamlining of already existing legislative measures or a transmission of non-binding EU measures into legislative ones. Based on the data collection and the analysis of EU legal measures in this study (see Annex II) policy option 2 would not cause conflicts with existing EU measures but rather represents a supplement to and/or manifestation of existing approaches.

SO1: Access to and exchange of information

Besides this coherence from a legal perspective at the EU level, specific measures of the option, such as the establishment of SIENA as the preferred channel of communication, are likely to produce a high adaption pressure for Member States. This is due to the numerous communication channels currently used and practical preferences that were developed in the past. While there is an overall coherence between policy option 2 and relevant EU measures, these measures are partly not coherent with operational procedures and preferences of law enforcement officials in the Member States.

Depending on whether a specific national legislation or agreement covers measures and their definition (e.g. competences of a SPOC, requirements of a CMS, minimum standard of data to be exchanged, etc.), the assessment of coherence between this policy option and national law/bi-/tri-/multilateral agreements differs.

- The challenge of a diverse landscape of (inter-) national rules and measures is particularly obvious in the area of investigative tools, such as surveillance and hot pursuit. Numerous bi-/tri-/multilateral agreements include specific definitions and rules of application for both tools, leading to different assessments of coherence for each agreement. The same line of argumentation applies for national legislation.
- As in the paragraph above, there is no conflict between the overall direction of the policy option and national law/bi-/tri-/ multilateral agreements. However, the fact that the measures proposed would imply a need to change specific details on both levels should be taken into account when assessing the option's coherence.

SO2: Management of public order and safety

Regarding the coherence with bi-/tri-/multilateral agreements, some of the measures proposed under policy option 2 are likely to cause conflicts as well as an increased need for adaption, both for the agreements themselves and operational structures and processes within the Member States covered by the agreement. The same argumentation applies for national legislation, which under the current EU legislation in the area of cross-border law enforcement cooperation is often the primary legal basis for action.

SO3: Fight against SOC and terrorism

The measures are expected to contribute to the coherence with horizontal EU objectives, existing binding and non-binding EU measures, bi-/tri-/multilateral agreements between Member States and SAC, as well as with national legislation.[219]

[219] The assessment provided in this section refers to the external coherence of policy option 2. The criteria of internal coherence of the option itself was already carefully considered at the development stage of the option. Therefore, policy option 2 is considered as internally coherent. A further analysis of the internal coherence is not included in this section.

Security

The measures foreseen under this policy option are expected to have moderate positive impacts on ensuring security in the EU for citizens, businesses, and public authorities.

SO1: Access to and exchange of information

The security-related impacts related to the measures foreseen concerning each of the three specific objectives can hardly be separated from each other and are expected to rather have a combined or cumulative effect than as stand-alone measures.

By increasing and improving the information base, the access to and exchange of information can be considered an enabler for the implementation of joint operations, as well as the use of investigative tools.

However, information and intelligence collected through joint operations for public order and safety, as well as through the use of investigative tools may – once exchanged with other Member States – inform other law enforcement procedures. Therefore, the measures foreseen under this policy option in relation to public order and SOC can also be expected to be an enabler and catalyst for the access to and exchange of information.

Overall, the combination of the foreseen measures in relation to all three specific objectives is expected to be the main driver behind increased security in the EU.

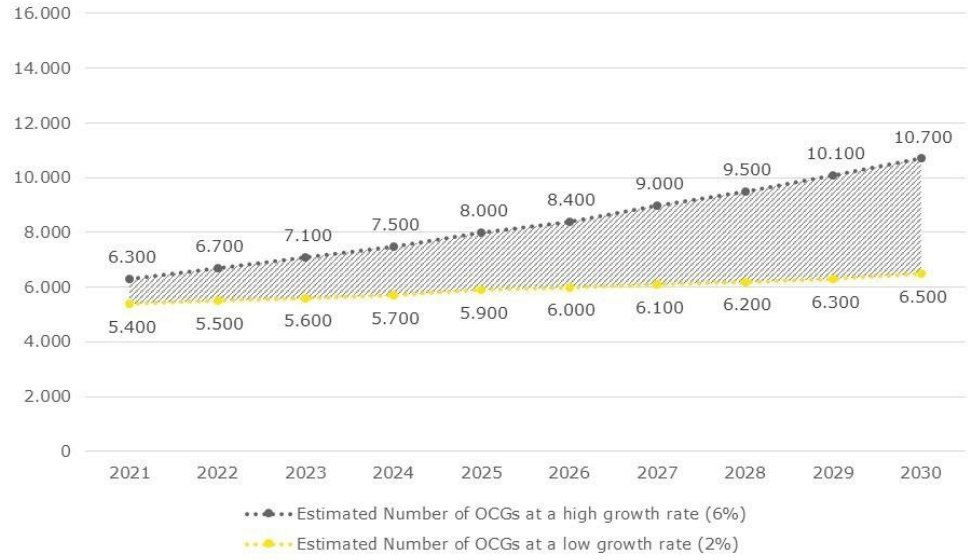
Therefore, the data presented hereunder is also a function of the measures implemented in relation to the other specific objectives.

Similar to the development of the core problem under the baseline scenario, the number of organised crime groups active in the EU is expected to increase under this policy option. The increase in the number of organised crime groups is expected to be less pronounced under policy option 2 than in the baseline scenario due to more efficient law enforcement cooperation. This means that citizens, businesses (in particular SMEs), and governments continue to face increasing security threats from SOC. However, both the number of incidents, as well as the likelihood of falling victim to SOC (in particular for vulnerable groups of persons and SMEs) is expected to be smaller compared to the baseline scenario.

Reliable figures are, of course, challenging to estimate due to the hidden nature of SOC, as well as the general lack of available quantitative evidence. It can, however, be expected that the range in which the number can be expected to develop is lower compared to the baseline scenario.

The following figure depicts the potential development of the number of organised crime groups until 2030. Similar to the baseline scenario, historic data provided by Europol has been used. However, the growth is expected to be smaller (i.e. 2% to 6% instead of 3% to 9%).

Figure 14 – PO2: Expected development of the number of organised crime groups

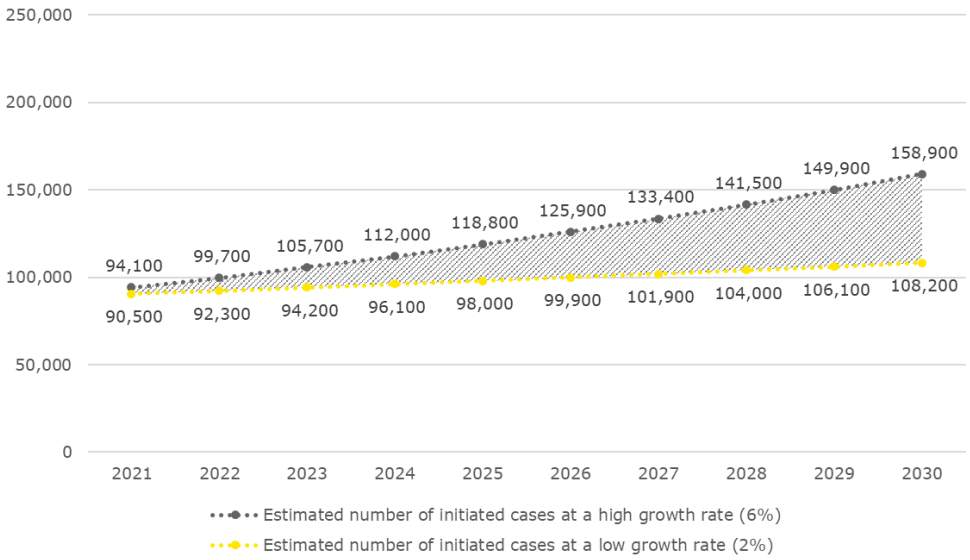


Source: Author's elaboration based on available evidence

As can be seen, the number of organised crime groups is expected to range roughly between 6,500 and 11,000. These estimates, however, need to be treated with great caution, in particular, as the preventive effect of law enforcement cooperation is generally perceived as being limited.

Similar to the baseline scenario, the number of cases initiated is expected to increase under policy option 2 over the next years. The quantitative increase is expected to be stronger than in the baseline scenario, despite the slightly more limited increase in organised crime groups. The graph below depicts the potential development

Figure 15 – PO2: Expected development of the number of initiated cases in SIENA



Source: Author's elaboration based on available evidence

It can be seen that the number of initiated cases in SIENA can go up to 158,900 in 2030 if a high growth rate is assumed. If a rather low growth rate is assumed, the number of initiated cases in SIENA is estimated to go up to 108,200 in the next ten years.

However, reliable data is largely missing. Therefore, the estimates need to be treated very carefully.

SO2: Management of public order and safety

The measures foreseen under this policy option are expected to contribute to increase security from a public order and safety management perspective. While the number of critical mass gatherings and other relevant incidents are expected to increase in similar fashion as under the baseline scenario, the necessary precautions law enforcement officials can take and the operational responses they can find are expected to be more effective in the future.

For instance, enabling officials remote access to specified police databases (or even specified data within them) in relation to specific types of international events (large-scale international football matches, mass tourism and music events, protection of VIPs etc.) via mobile terminals in specific geographical areas could enhance the extent to which crowds are being securely managed from an operational perspective.

Overall, however, the same argumentation applies as in relation the access to and exchange for information applies: The combination of measures foreseen under this policy option covering all three specific objectives is the main driver behind increased security in the EU.

SO3: Fight against SOC and terrorism

In relation to the fight against SOC and terrorism, the same argumentation applies as in relation the access to and exchange for information, as well as the management of public order and safety: The combination of measures is the main driver behind increased security in the EU.

Economy

Policy option 2 is expected to have a small positive impact on the economy. Naturally, organised crime groups are also expected to cause economic harm for citizens, businesses (in particular SMEs), and governments under this policy option – however to a slightly lesser extent than in the baseline scenario.

SO1: Access to and exchange of information

The introduction of the measures foreseen under this policy option may have positive effects on markets related to IT-related products and services – for instance due to Member States' need to procure related hard- and software, as well as their need for specific expert staff.

SO2: Management of public order and safety

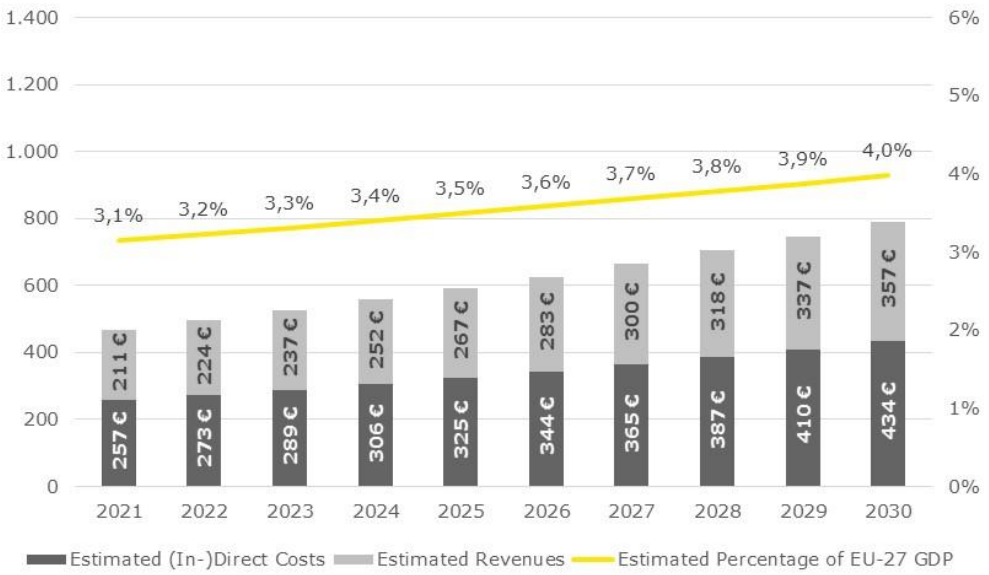
Cross-border mobility, in particular for touristic purposes after the Covid19-pandemic, is expected to increase. A crucial enabler for this development is the effective and efficient management of public order and safety. Therefore, it can be expected that the measures foreseen under this policy option will have a positive economic impact, e.g. in terms of increased GDP in tourism-related industries. However, reliable figures are not available.

Moreover, it is not clear to what extent the measures foreseen are the root causes of increased mobility or if not some – or all – cross-border travel would occur to the same extent if the measures were not introduced.

SO3: Fight against SOC and terrorism

Based on the approach used to quantify the damage outlined in relation to the baseline scenario, it can be estimated that organised crime groups may cause damage of up to 4.0% in 2030 under this policy option. This means it can be expected that the overall annual economic damage from organised crime groups could grow to roughly 800 million EUR in 2030 (i.e. around 300 million EUR less than in the baseline scenario; -27%).

Figure 16 – PO2: Expected development of economic damage caused by SOC



Source: Author's elaboration based on available evidence

As pointed out before, it is imperative to treat these estimates with great care: They should be considered to be at the upper boundary. This means that the actual future economic damage from organised crime groups is very likely to be lower than the numbers reported above. More reliable data is, however, missing.

Fundamental rights

Effective and efficient law enforcement cooperation is a crucial prerequisite to ensuring a common area of freedom, security and justice without internal borders. Yet, new measures in relation to law enforcement cooperation may have implications for fundamental rights of citizens, including for instance the protection of data and privacy when sharing information across border. Thus, there is a fine line to draw between the importance of effective and efficient law enforcement cooperation and safeguarding fundamental rights.

Moreover, there are various degrees to which fundamental rights can be affected, e.g. ranging from the interference of a measure with fundamental rights, to a violation or an infringement. In case a measures interferes with fundamental rights political and legal decisions need to be taken based on the importance of particular impacts of the measures on fundamental rights. However, the measures may not violate or infringe fundamental rights.

The measures foreseen under policy option 2 are expected to be fully coherent with the GDPR, as well as the Data Protection Law Enforcement Directive – thus appropriately protecting citizens' personal data whenever and wherever it is used for the purpose of law enforcement cooperation.

Overall, policy option 2 is expected to improve EU safeguards for fundamental rights in the EU and SAC to a moderate extent, including the freedom of movement and of residence. In addition, the measures are aimed at improving citizens' security in the EU and, thus, are expected to contribute to ensuring the personal liberty and security.

SO1: Access to and exchange of information

The measures foreseen under this policy option are expected to reduce the likelihood for persons to both fall victim to SOC, as well as to be apprehended based on incorrect information, miscues, and misfortune.

There is, however, still a risk that existing law enforcement databases are subject to inherent, unconscious biases and stereotypes (e.g. ethnicity, gender, sexual orientation, culture and

religion, citizenship, (dis-) ability etc.). It is, therefore, crucial for maintaining the potential positive impact of improved access to and exchange of information to critically review the stored information and – most importantly – the information transmitted between countries in order not to (re-) produce discriminatory prejudices in the cross-border context.

More specifically, it should be noted that various elements foreseen under this policy option may have different impacts on fundamental rights, as outlined in the following.

Legal barriers

Whereas adaptations to the SFD to ensure alignment with the Law Enforcement Data Protection Directive, notably Article 8 on data protection, are expected to positively impact safeguarding citizens' fundamental rights, the establishment of a common minimum set of data that has to be made available by all Member States for exchange may potentially have a negative impact on fundamental rights.

The collection and exchange of data in the context of cross-border law enforcement needs for a precise and explicit legal ground and operational justification. Thus, the measures foreseen under policy option 2 need to practically useful and lawful in order to minimise the impact on fundamental rights from a data protection perspective. Moreover, the policy option's measures should be aligned with various principles for which the implementation is ensure through appropriate legal and technical safeguards:

- Purpose limitation, i.e. the principle of collecting (and exchanging) only information that strictly necessary and relevant for the purpose of cross-border law enforcement; and
- Data minimisation, i.e. the principle of keeping the information collected and exchanged as definite as possible in order to be able to ensure an appropriate data quality (accuracy, completeness, and recentness).

Moreover, access to the data collected and exchanged should be given only to officials that ultimately need access in order to perform their duties. Therefore, the implementation of policy option 2 needs to be closely aligned with the current reform processes concerning the mandate, role and operational competencies of Europol.

Moreover, Member States may view some information to be exchanged as privileged / classified – and therefore as a risk to the security of their citizens. This is also expected to hamper the political feasibility of the policy option.

In contrast, however, 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 safeguarding fundamental rights for citizens. The swifter exchange of information is expected to contribute to more efficient law enforcement processes. This means that eventual suspects who are being wrongfully accused of certain crimes are expected to be cleared faster of any charges than under the baseline scenario. This is expected to improve safeguarding, for instance, of citizens' right to liberty and security, respect for private and family life, and freedom of movement and of residence. In a similar vein, of course, the swifter exchange of information is expected to improve citizens' liberty, safety, and freedom of movement from persons rightfully suspected to commit further crimes.

In a similar vein, the provision of 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 expected to contribute to potentially clear citizens from wrongful charges in a swifter fashion.

Moreover, the clear establishment of SIENA as the preferred information channel to be used, as well as the requirement for Member States to set out the factual reasons to believe that the relevant information and intelligence is available in another Member State is expected to have a positive impact by minimising the opportunities for officials to "fish" for specific information that could compromise suspects' fundamental rights. Thus, both measures are regarded as a means to provide officials with information they are eligible to obtain without providing further resources than necessary under specific circumstances.

The same is valid for the establishment of new, simpler and more user-friendly forms, as well as introduction of an automated display of a hit/no hit indication. Since it is expected to be clearer under policy option 2 (compared to the baseline scenario) which information can be queried from other Member States and the link to the specific Member State need to be set out, the risk of officials wrongfully obtaining unsolicited information that may compromise suspects' fundamental rights is expected to decrease.

Adaptations to the SFD to remove references to "other" cases are 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 being safeguarded (either wrongfully suspected citizens being cleared of charges quicker or citizens' being safeguarded more swiftly from rightfully suspected criminals committing further crimes).

Technical barriers

At the technical level, there are potential risks as concerns fundamental rights being safeguarded in relation to Member States' CMS that are used for cross-border exchanges of information by SPOCs. Policy option 2 aims to address existing risks by introducing common requirements for the functionalities of the CMS 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 compared to the baseline scenario.

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 undue, unsolicited information is expected to be more limited than in the baseline scenario.

At the same time, however, the automation of data cross-checks, e.g. through improved search tools and the adoption of transliteration and "fuzzy logic" search, is expected to potentially have a negative impact on fundamental rights – depending on the quality of the underlying algorithms and their practical uses by officials. For instance, through the implementation of a "fuzzy logic" search, citizens who would under the baseline scenario not become suspects in relation to a specific case could wrongfully be accused of crimes if they are being (wrongly) identified by the "fuzzy logic" algorithm. This is also a critical issue with regard to safeguarding the privacy of citizens' information. Accompanying safeguards, such as a manual control following the use of algorithms, would need to be foreseen.

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 safeguarding 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. However, within the framework of this study, no data has been collected on security breaches and there is no evidence of concrete problems for the time being.

In a similar vein, respective training with regard to the use of Member States' CMS is expected to have a positive impact on law enforcement authorities' ability to safeguard fundamental rights.

Structural barriers

At the structural level, policy option 2 foresees 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 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 stakeholders as an excessive measure in view of providing law enforcement authorities with only the necessary access to information. In the same vein, involving staff in the SPOC who have full access to all relevant national case management systems could be seen as critical from a fundamental rights perspective.

This is also expected to hamper the political feasibility of policy option 2.

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 law enforcement authorities' ability to safeguard citizens' fundamental rights.

SO2: Management of public order and safety

With specific regard to the management of public order, the freedom of assembly and of association is not expected to be infringed through the introduction of policy option 2. More specifically, the improved access to and exchange of information enables law enforcement authorities to take 'better' decisions based on a more comprehensive and sounder information base. Thus, for instance, potential operations to dismantle political mass gatherings are expected to be much more targeted, tailored, and likely justified in the future.

However, the introduction of a new provision on the conferral of powers could potentially be regarded as critical by stakeholders. Although foreign officials would, of course, continue to work under the guidance of officials of the host Member State, in citizens may have the perception that foreign officials are not legitimate law enforcement authorities – thus compromising safeguarding fundamental rights in the view of citizens.

At the same time, however, establishing a new provision on the remote access to relevant law enforcement databases in specific situations could have a positive impact on safeguarding fundamental rights – in case the access is guaranteed to be secure from a technical perspective and personal data is protected accordingly. As already lined out above in relation to the access to and exchange of information, officials being able to swiftly access information can contribute to even quicker clear citizens from undue charges within specific critical situations, thus, ensuring citizens' right to liberty and security, respect for private and family life, and freedom of movement and of residence. IN addition, of course, swifter access of information can also contribute to safeguarding citizens' fundamental rights by saving citizens from rightfully suspected citizens committing further crimes.

From a macro-perspective, establishing a new provision on cross-border threat assessment could, on the one hand, contribute to safeguarding fundamental rights. Citizens are expected to be more secure in case threat assessments and intelligence are being developed jointly and / or shared with other Member States for both preventative and reactive purposes. However, on the other hand, there could also be potential negative impacts on fundamental rights, notably with regard to the confidentiality of (classified) information.

SO3: Fight against SOC and terrorism

Some of the most common forms of SOC are trafficking in human beings, slavery and forced labour. Therefore, the policy option is expected to positively impact on ensuring that the prohibition of such criminal acts maintained – in particular with a view to the fundamental rights of children.

However, at the same time, establishing new provisions on surveillance (e.g. to also cover the use of cross-border surveillance in relation to waterways, sea and air borders, to start physical surveillance operations on the territory of another Member State, and to extend the list of offences in relation to which cross-border surveillance is allowed) might be regarded by stakeholders as excessive and increase the risk for confidentiality breaches by law enforcement authorities.

This could also hamper the political feasibility of the policy option.

Society

The measures foreseen under this policy option are expected to increase the security for citizens and businesses in the EU to a moderate extent. This is expected to have a positive impact on cross-border mobility of citizens and businesses, including in relation to personal travel for tourism. No impact is expected on the uptake of technology by citizens and businesses.

SO1: Access to and exchange of information

Neither positive nor negative direct societal impacts are expected in relation to the access to and exchange of information.

SO2: Management of public order and safety

Due to increased security within the Member States and SAC, it can be expected that cross-border mobility will increase in the future – in particular in relation to personal travel after the COVID-19 pandemic. The impact is, however, expected to be very small. Persons who want to travel for tourism, who want to attend mass sports events, concerts or other large gatherings in another country are expected to still do so even if the measures foreseen under policy option 2 would not be introduced. In terms of cross-border mobility for professional purposes, it remains to be seen to what extent and for how long the remote communication tools widely used during the pandemic will continue to be used also afterwards. In any case, the impact of policy option 2 in terms of increased cross-border mobility, both in relation to travel for personal and professional purposes, is expected to be very small to negligible.

The measures foreseen under this policy option are not expected to have an impact on the uptake and use of technology by citizens and businesses in relation to non-criminal purposes.

SO3: Fight against SOC and terrorism

In relation to the fight against SOC and terrorism, the same argumentation applies as in relation the management of public order and safety.

Environment

Policy option 2 is expected to have an overall environmental impact that is considered very small to negligible within the framework of this study.

SO1: Access to and exchange of information

The measures foreseen under this policy option are expected to have a slightly negative environmental impact. This is due to increased electricity needs of computers and servers in relation to the access to and exchange of information. In addition, there may also be additional need for office space, related electricity and heating.

SO2: Management of public order and safety

The need for the physical re-location of staff for the purpose of joint operations (e.g. by bus or plane) is expected to have a negative environmental impact with regard to CO_2 emissions.

SO3: Fight against SOC and terrorism

CO_2 emissions may also slightly increase due to the increased use of investigative tools such as hot pursuits (at least when not using electric cars) or officials travelling across borders for surveillance purposes (e.g. by car or plane). Overall, however, the environmental impact is considered negligible within the framework of this study.

Effects of the policy option 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.[220]

Table 17 – PO 2: Impacts on different types of stakeholders

			SO 1: Access to and exchange of information	SO 2: Operational cooperation for public order and safety	SO 3: Operational cooperation to fight SOC and terrorism
Public authorities	Law Enforcement Authorities	SPOCs			
		PCCCs			
		Other			
	Judicial Authorities				
	Data Protection Authorities				
NGOs					
Citizens / Businesses					

Source: Author's own elaboration

The table shows that public authorities are expected to be affected quite positively through the introduction of the elements relating to each of the specific objectives – in particular SPOCs. Moreover, citizens and businesses are also expected to be affected in a positive manner.

6.1.4 Assessment of Policy option 3: Legal proposal aiming for stronger alignment + supporting (soft) measures

Table 18 – Policy option 3: Summary of impacts

Criteria	Rate	Summary of assessment
Evaluation of effects		
Effectiveness	4	<u>*SO 1: Access to and exchange of information*</u> The additional/more extensive measures in policy option 3 compared to policy option 2 expected to further enhance positive impacts on the access to and exchange of information. Respective measures cover the establishment of a common minimum set of data that Member States and SAC need to collect in relation to cross-border cases, which goes beyond the set of data foreseen in policy option 2 ; and the establishment of SIENA as the default (rather than the preferred) channel of communication. On a more technical and structural level, the following additional measures are added under policy option 3: • The establishment of one CMS to be used by both SPOCs and PCCCs, or, alternatively, a requirement to ensure interoperability between the CMSs of the SPOCs and PCCCs; • Instead of "being informed about" (policy option 2), policy option 3 would establish that the SPOC is responsible for all international law enforcement cooperation requests at national level; • The same minimum requirements established for the SPOCs should also be applicable to the PCCCs. The measures above are expected to further facilitate the access to and exchange of information, i.e. by supporting the harmonisation of workflows and organisational structures to an even larger extent than policy option 2.

[220] 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.

Criteria	Rate	Summary of assessment
	4	*SO 2: Public order and safety* The measures foreseen are expected to enlarge the impacts already expected to be triggered by policy option 2. The largest positive impact be expected from two measures: • A higher budget would be allocated within the financial instrument. In addition to the items funded under policy option 2, policy option 3 would also foresee additional budget to e.g. train staff on joint operations and identify and share best practices. Budget would also be made available for technical means to facilitate training and knowledge sharing on the ground; • New provision, making it compulsory for the Member States to share threat assessment and risk analyses with other LEAs insofar as this does not constitute a security risk for the Member State concerned. Especially the importance of user-oriented training for more joint operations to take place in an even smoother manner training was highlighted by participants.
	4	*SO 3: Fight against SOC and terrorism* The measures under PO3 aimed at ensuring efficient cross-border operational cooperation in relation to SOC and terrorism are expected to achieve the objectives to a large extent. As for policy option 2, the measures are expected to support an efficient and coordinated response addressing the increasing cross-border challenges linked to SOC and terrorism. The differences between the respective measures under policy options 2 and 3 are limited and stem from different scopes of application or clearer definitions of specific investigative tools, leaving Member States with a bit less leeway for action (policy option 3). However, these discrepancies are not expected to have a visible impact on the effectiveness.
	4.0	**Overall assessment**
Efficiency	3	*SO 1: Access to and exchange of information* The positive impact of option 3 on efficiency regarding information exchanged can be assessed as moderate. The assessment is specifically based on the fact that the (limited number of extended/additional) measures foreseen in relation to information exchange under option 3 are considered to be more 'intrusive', thus leaving less leeway for Member States to adapt legislative and functional requirements towards their own priorities and needs. This reduced leeway and increased adjustment pressure are expected to cause relatively high implementation costs for Member States, i.e. IT-development and roll-out. The following measures were added/adapted compared to policy option 2: • Establishing SIENA as the default channel for information exchange (instead of only the preferred one); • Requiring SPOCs and PCCCs to use one CMS or to make their large-scale IT systems interoperable with each other; and • Making SPOCs responsible for all international law enforcement cooperation requests dealt with at national level.
	3	*SO 2: Public order and safety* The policy option contains measures in relation to the management of public order and safety that may be most effective from a pure law enforcement cooperation perspective, such as the conferral of certain operational powers to foreign officials without any exceptions or the compulsory for Member States to share threat assessment and risk analyses with other LEAs insofar as this does not constitute a security risk for the Member State concerned. However, Member States may find these measures to be too far reaching from a political perspective. This is expected to hamper the implementation from an efficiency point of view.
	2	*SO 3: Fight against SOC and terrorism* In relation to the fight against SOC and terrorism, the same argumentation applies as in relation the management of public order and safety.
	2.7	**Overall assessment**

Criteria	Rate	Summary of assessment
Coherence and proportionality	3	*SO 1: Access to and exchange of information* The policy option is expected to have a small positive impact on increasing the coherence of the legislative framework at both the EU and national levels governing cross-border law enforcement cooperation. The formulation of measures under policy option 3 represents an extension of issues covered under option 2 as well as an increased degree of legal obligation. This leaves Member States with less leeway for its implementation. Policy option 3 is therefore considered to cause a higher number of conflicts with existing measures, specifically with bi- and multilateral agreements as well as national legislation. The measures are still considered proportionate.
	2	*SO 2: Public order and safety* As concerns the management of public order and safety, the measures proposed under policy option 3 are considered coherent with existing measures, albeit to a low extent. This overall assessment is based on the finding that most additional measures proposed under this option would rather broaden the scope of application of existing EU measures as well as their degree of legal obligation towards the Member States than affecting the core of these measures as such. However, the "conferral of certain operational powers to foreign officials without any exceptions" justifies the lower extent of coherence for policy option 3. The measures are still considered proportionate. However, adaptation efforts by Member States are expected to be higher than under policy option 2.
	1	*SO 3: Fight against SOC and terrorism* The measures proposed under policy option 3 are expected to be coherent with existing measures, albeit to a very low extent. This overall assessment is based on the fact that the formulation of measures under policy option 3 represents an extension of issues covered under option 2 as well as an increased degree of legal obligation. This leaves Member States with less leeway for their implementation and an increase adaption pressure and potentially causes conflicts with national rules as well as with provisions in bi/tri/multilateral agreements. The measures are still considered proportionate. However, adaptation efforts by Member States are expected to be higher than under policy option 2.
	2.0	**Overall assessment**
Types of impacts		
Security	4	The measures foreseen under policy option 3 are expected to have large positive impacts on the achievement of the general objectives, i.e. ensuring security in the EU for citizens, businesses, and public authorities.
Economy	3	Policy option 3 is expected to have a moderate positive impact on the economy. Also under policy option 3 organised crime groups are expected to continue to cause economic damage for citizens, businesses (in particular SMEs), and governments. However, somewhat less pronounced than in the baseline scenario.
Fundamental rights	2	The assessment of the impacts for policy option 3 in relation to these criteria is similar to the impacts outlined in relation to policy option 2 (see section 6.1.3). With specific regard to fundamental rights, however, the extension of the common minimum set of data required to be collected by Member States to passport and identity document data is expected to potentially have, in some cases, negative impacts on e.g. vulnerable persons.
Society	1	
Environment	1	

** The overall assessment refers to the average rating in relation to the SOs.*

Source: Author's own elaboration

Effectiveness

Similar to policy option 2, policy option 3 is expected to achieve the policy objectives to a large extent. Since policy option 3 mostly incorporates all the measures in policy option 2 (but in some cases goes beyond the measures included in option 2), the following analysis of the effectiveness of this option is exclusively focussed on additional and diverging points.

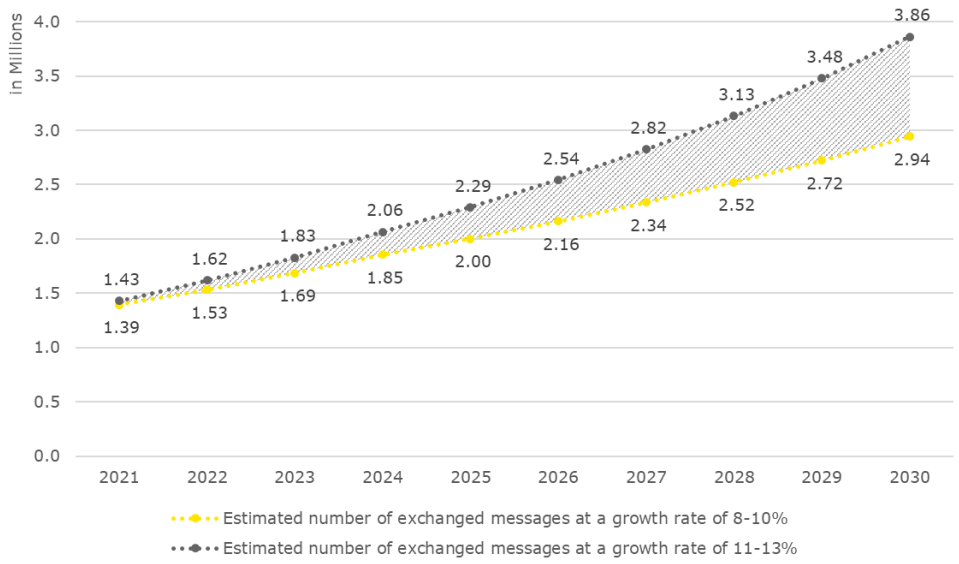
SO1: Access to and exchange of information

In addition to the points described in section 6.1.3. on the assessment of policy option 2, the most important impacts on the specific objective aiming at facilitating the **access to and exchange of necessary information** are expected to stem from two different measures:

- The establishment of a common minimum set of data that Member States and SAC need to collect in relation to cross-border cases, which goes beyond the set of data foreseen in policy option 2[221]; and
- The establishment of SIENA as the default (rather than the preferred) channel of communication.

The definition of SIENA as the default channel instead of a preferred channel (policy option 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 (see figure below).

Figure 17 – PO3: Expected development of messages sent via SIENA



Source: Author's elaboration based on available evidence

The number of messages exchanged via SIENA is estimated to increase to 3.86 million messages in 2030 under the assumption of a high growth rate. If a lower growth rate is assumed, the number of messages is estimated to go up to 2.94 million messages.

At the more **technical and structural level**, the positive impacts of policy option 3 on the effectiveness of law enforcement cooperation are expected to stem from the following additional measures:

- The establishment of one CMS to be used by both SPOCs and PCCCs, or, alternatively, a requirement to ensure interoperability between the CMSs of the SPOCs and PCCCs;
- Instead of "being informed about" (policy option 2), policy option 3 would establish that the SPOC is responsible for all international law enforcement cooperation requests at national level;
- The same minimum requirements established for the SPOCs should also be applicable to the PCCCs.

All three points above are expected to further enhance the positive impacts on the access to and exchange of information between Member States by supporting the harmonisation of workflows and organisational structures to an even larger extent than PO2.

SO2: Management of public order and safety

As for policy option 2, the measures concerning **tailored joint operations** foreseen under policy option 3 are expected to contribute to a large extent to improved quality and effectiveness of operational cooperation for public order and safety. On this specific point, the assessment of the

[221] See Table 9: Administrative register on persons (census); Database of prison inmates; Register on enterprises and commercial companies; Information concerning foreign nationals (decisions and permits, measures imposed, etc.); and Passports and identity documents.

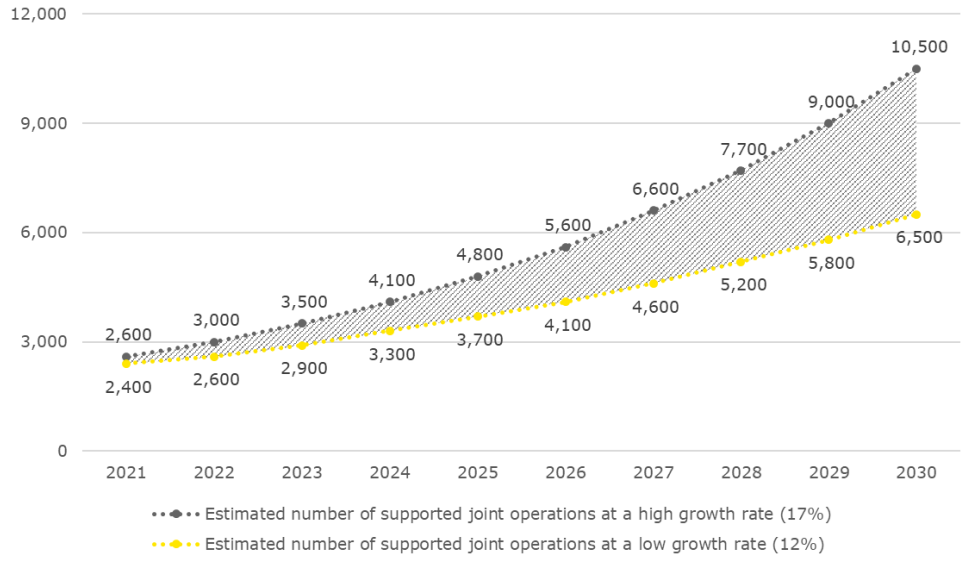
efficiency for policy options 2 and policy option 3 only shows a minimal deviation, if any at all. Most measures for both options under the respective specific objective are almost congruent, with some extension of the scope and/or degree of legal obligation (e.g. measure 2.1 "[…] same text on the conferral of powers […] without any exceptions").

The largest positive impact of policy option 3 on tailored operations can be expected from two measures:

- A higher budget would be allocated within the financial instrument. In addition to the items funded under policy option 2, policy option 3 would also foresee additional budget to e.g. train staff on joint operations and identify and share best practices. Budget would also be made available for technical means to facilitate training and knowledge sharing on the ground;
- New provision, making it compulsory for the Member States to share threat assessment and risk analyses with other LEAs insofar as this does not constitute a security risk for the Member State concerned.

Especially the importance of user-oriented training for more joint operations to take place in an even smoother manner training was highlighted by participants of the 2nd technical workshop. The two measures above are expected to further enhance the positive impacts on joint operations already triggered by the respective measures included under policy option 2. They would therefore, presumably, imply an increased number of joint operations supported by Europol (see figure below).

Figure 18 – PO3: Expected development of joint operations supported by Europol



Source: Author's elaboration based on available evidence

The number of joint operations supported by Europol is expected to increase to up to 10,500 joint operations by 2030 in a scenario with a high growth rate. If a lower growth rate is assumed, the number of joint operations is estimated to go up to 6,500 in the next ten years. Compared to policy option 2, this is an increase of 600 to 1,100 in 2030 (i.e. +10%).

SO3: Fight against SOC and terrorism

As for policy option 2, the measures under policy option 3 aimed at **ensuring efficient cross-border operational cooperation in relation to SOC and terrorism** are expected to achieve this objective to a large extent. This assessment is based on the same line of argumentation as for policy option 2 in section 6.1.3. The differences between the respective measures under policy options 2 and 3 are limited and stem from different scopes of application or clearer definitions, leaving Member States with a bit less leeway for action. However, these discrepancies are not expected to have a visible impact on the criterion of effectiveness.

The maximum time allowed to carry out cross-border surveillance activities under policy option 3 is 14 days (not 24 hours as under policy option 2). Thus, policy option 3 can be expected to enable more effective surveillance (higher quality, more detailed info) than policy option 2.

Efficiency

Policy option 3 is expected to contribute to increasing the efficiency of EU law enforcement cooperation to a moderate extent.

SO1: Access to and exchange of information

Whereas, for the most part, similar arguments apply as in relation to policy option 2, policy option 3 is considered to be more 'intrusive', while leaving less leeway for Member States to adapt legislative and functional requirements towards their own priorities and needs. Most notably, this concerns:

- Establishing SIENA as the default channel for information exchange (instead of only the preferred one);
- Requiring SPOCs and PCCCs to use one CMS or to make their large-scale IT systems interoperable with each other; and
- Making SPOCs *responsible* for all international law enforcement cooperation requests dealt with at national level.

In relation to SIENA 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 if 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 i24/7 should rather have been used. At the same time, however, Europol indicated that SIENA should become the default channel for information exchange in the EU as it is expected that through the introduction of new functionalities, the take-up and practical use of SIENA will strongly increase over the next years.

As concerns IT systems, it is expected that, in addition to the measures foreseen under policy option 2, Member States would need to spend even more additional budget on IT-related developments, training and staff in order to satisfy the requirements foreseen under this policy option – in particular making large-scale IT systems at least interoperable with each other.

In particular the interoperable alignment of SPOCs' and PCCCs' large-scale IT-systems is expected to require increased investment and budgetary spending (including for technical developments, implementation and maintenance). During the 2nd technical workshop, one Member State pointed out challenges with regard to the political and technical feasibility of this measure.

Moreover, requiring the SPOCs to be responsible rather than 'only' informed about international cases is expected to create considerable need for change and adaptation of national legislation, structures, processes, and administrative burden.

At the same time, however, the additional benefits from these measures compared to what can be achieved under policy option 2 are considered limited.

In addition, policy option 3 contains soft measures that aim at improving the effectiveness of law enforcement cooperation but, at the same time, may counteract its efficiency (e.g. the requirement that communication between SPOCs should take place in English).

SO2: Management of public order and safety

As concerns the management of public order and safety, as well as the fight against SOC and terrorism, policy option 3 is considered to be most effective from a pure law enforcement cooperation perspective – however, jeopardising the political feasibility of the policy option as such.

For instance, not granting Member States exceptions with regard to the conferral of power to officials from other countries, as well as setting common minimum requirements for national rules to facilitate the interception of communication in a cross-border context may be seen by Member States too far reaching in the political process.

However, with e.g. even higher funding for joint operations foreseen, policy option 3 does also contain measures that could facilitate political negotiations in the long run.

SO3: Fight against SOC and terrorism

Due to the coverage of additional investigative tools (i.e. controlled delivery and interception of communication), it is expected that policy option 3 will contribute to the efficiency of EU law enforcement cooperation to a large extent. It is expected that the foreseen measures – in particular the use of modern surveillance technology – will facilitate quicker and swifter cross-border investigations, thus reducing the need for time- and staff-intensive operations.

In contrast to policy option 2, the maximum time allowed to carry out cross-border surveillance activities under policy option 3 is 14 days (not 24 hours). This means, on the one hand, that surveillance activities can be more effective. On the other hand, however, they are also expected to become more costly and time consuming.

At the same time, however, the policy option's efficiency may be hampered by an eventual lack of political and financial commitment to cross-border cooperation overall, as well as the need for increased training of officials.

Coherence and proportionality

The policy option is expected to have a small positive impact on increasing the coherence of the legislative framework at both the EU and national levels governing cross-border law enforcement cooperation. The measures foreseen are still considered proportionate. However, it is expected that Member States would have to make considerable efforts to develop further existing national legislation, as well as bi-/tri-/multilateral agreements – in particular with regard to the management of public order and safety, as well as the fight against SOC and terrorism. This assessment follows the same line of argumentation used in relation to policy option 2 concerning the criterion of coherence and proportionality.

Since policy option 3 mostly incorporates all the measures in policy option 2, the following analysis of the coherence of this option is exclusively focussed on additional and diverging points.

SO1: Access to and exchange of information

Compared to the second policy option, policy option 3 aims for a stronger alignment of existing binding and non-binding measures, both on EU as well as Member State level. The formulation of specific measures proposed (e.g. degree of legal obligation or number of issues covered) therefore provides Member States with less leeway for their implementation on national level. This applies to measures under all three specific objectives and can for example be illustrated by measure no. 1.1.: Instead of establishing SIENA as the "preferred" channel of information exchange (option 2), the respective measure under policy option 3 proposes the establishment of SIENA as "default" channel of communication. This change in wording represents an extension of the likely impact of the measure and is therefore considered to cause a higher number of conflicts with existing measures in bi- and multilateral agreements and national legislation. The same argumentation applies for measures in which the list of requirements, criteria or common standards was extended for policy option 3 (see for example measure 1.3).

SO2: Management of public order and safety

As concerns the management of public order and safety, the measures proposed under policy option 3 are considered coherent with existing measures, albeit to a low extent.

This overall assessment is based on the finding that most additional measures proposed under this option would rather broaden the scope of application of existing EU measures as well as their degree of legal obligation towards the Member States than affecting the core of these

measures as such. A new provision to cooperate with neighbouring MS to develop and use cross-border threat assessment serves as an illustrative example for this assessment.

However, the measure "Conferral of certain operational powers to foreign officials without any exceptions" justifies the lower extent of coherence for policy option 3 compared to option 2. Member States often clearly define the executive powers of foreign officers in their national law and show great differences in this regard. A new provision on the conferral of powers might therefore cause conflicts with national law, depending on the exact scope of rights and duties of foreign officials currently enshrined on national level. The same line of argumentation applies for bi/tri/multilateral agreements.

SO3: Fight against SOC and terrorism

As concerns the fight against SOC and terrorism, the measures proposed under policy option 3 are expected to be coherent with existing measures, albeit to a very low extent.

This overall assessment is based on the fact that the formulation of measures under policy option 3 represents an extension of issues covered under option 2 as well as an increased degree of legal obligation. This leaves Member States with less leeway for their implementation and an increase adaption pressure. Policy option 3 is therefore considered to cause a higher number of conflicts with existing measures at the national level. The more specific extension of the list of offences for which certain investigative tools can be applied as well as the clearer definition of rights and duties of foreign officials serve as examples for such measures and their expected impacts.

Depending on the current rules in the Member States, the coherence between policy options 3 and national law varies significantly between Member States. The same line of argumentation applies for bi/tri/multilateral agreements. In general, there is a fundamental lack of coherence between the measures proposed and the national law/agreements regarding the primary legislative basis for the use of investigative tools such as hot pursuit and surveillance.

Security

The measures foreseen under policy option 3 are expected to have large positive impacts on the achievement of the general objectives, i.e. ensuring security in the EU for citizens, businesses, and public authorities.

SO1: Access to and exchange of information

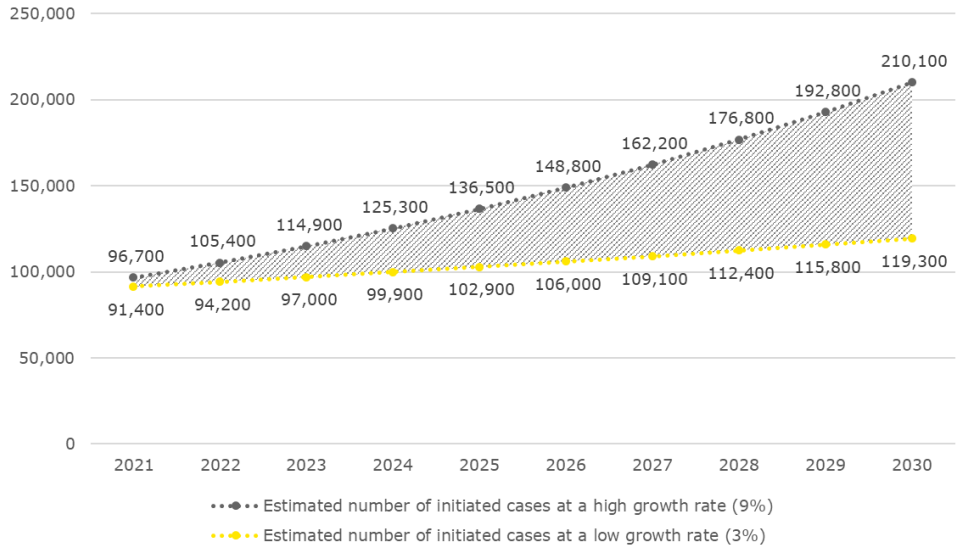
Again, as already pointed out in relation to policy option 2, the combination of the foreseen measures in relation to all three specific objectives is expected to be main driver behind increased security in the EU.

Therefore, the data presented hereunder is also a function of the measures implemented in relation to the other specific objectives.

Similar to the development under the baseline scenario, the number of organised crime groups active in the EU is expected to increase under this policy option. However, less pronounced. With reliable numbers missing, it is expected that the effect of policy option 3 on the number of organised crime groups active in the EU would be of similar magnitude as the effect of policy option 2.

Similar to policy option 2, the number of cases initiated is expected to increase under policy option 3 over the next years. However, the development is expected to be more pronounced. The graph below depicts the potential development.

Figure 19 – PO3: Expected development of the number of initiated cases in SIENA



Source: Author's elaboration based on available evidence

It can be seen that the number of initiated cases in SIENA can go up to 210,100 in 2030 if a high growth rate is assumed. If a lower growth rate is assumed, the number of initiated cases in SIENA is estimated to go up to 119,300 in the next ten years.

However, reliable data is largely missing. Therefore, the estimates need to be treated very carefully.

SO2: Management of public order and safety

Similar to policy option 2, this policy option is also expected to have a positive impact on the management of public order and safety. The impact is expected to be more pronounced than under policy option 2 as the measures foreseen hereunder are considered to be stricter and, thus, leave les leeway for diverging approaches between Member States.

SO3: Fight against SOC and terrorism

In relation to the fight against SOC and terrorism, the same argumentation applies as in relation the access to and exchange for information, as well as the management of public order and safety: The combination of measures is the main driver behind increased security in the EU.

Economy

Policy option 3 is expected to have a moderate positive impact on the economy. Also under policy option 3 organised crime groups are expected to continue to cause economic damage for citizens, businesses (in particular SMEs), and governments. However, somewhat less pronounced than in the baseline scenario.

SO1: Access to and exchange of information

Similar to policy option 2, the measures foreseen under policy option 3 may have positive effects on markets related to IT-related products and services. Due to the need to also integrate PCCCs CMS with SPOCs, further investments may be necessary.

SO2: Management of public order and safety

Similar to policy option 2, cross-border mobility, in particular for touristic purposes after the COVID-19 pandemic, is expected to increase. Therefore, the effective and efficient management of public order and safety is crucial for tourism-related economic impacts to materialise.

With no reliable data available, however, it is not clear to what extent the measures foreseen are the root causes of increased mobility or if not some – or all – cross-border travel would occur to the same extent if the measures were not introduced.

SO3: Fight against SOC and terrorism

With reliable figures largely missing, the economic damage caused by organised crime groups under policy option 3 is expected to be of similar magnitude as under policy option 2.

Fundamental rights, Society, and Environment

The assessment of the impacts for policy option 3 in relation to these criteria is similar to the impacts outlined in relation to policy option 2 (see section 6.1.3).

With specific regard to fundamental rights, however, the extension of the common minimum set of data required to be collected by Member States to passport and identity document data is expected to potentially have negative impacts on the protection of citizens' data, as well as – ensuing – other fundamental rights such as the right to liberty and safety. In addition, there may, in some cases, be negative impacts on vulnerable persons such as homeless persons and refugees (who often do not possess appropriate identity documentation).

Effects of the policy option 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.[222]

Table 19 – PO 3: Impacts on different types of stakeholders

			SO 1: Access to and exchange of information	SO 2: Operational cooperation for public order and safety	SO 3: Operational cooperation to fight SOC and terrorism
Public authorities	Law Enforcement Authorities	SPOCs			
		PCCCs			
		Other			
	Judicial Authorities				
	Data Protection Authorities				
NGOs					
Citizens / Businesses					

Source: Author's own elaboration

As concerns PO3, the table shows that public authorities are expected to be affected even more positive than under PO2. This is also expected to be valid for citizens and businesses.

6.2 Political feasibility of the policy options

Throughout different stages of the study, 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 open 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

[222] 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.

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 in chapters 6.1 and 6.3 has 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 foreseen 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.

Table 20 – Stakeholders' high-level support for the policy options

Stakeholders in the Member States / Topics	Public authorities					NGOs & civil society
	Law Enforcement Authorities			Judicial Authority	Data Protect. Authority	
	SPOCs	PCCCs	Other			
Overarching topics						
Access to and exchange of information						
Operational cooperation for public order and safety						
Operational cooperation to fight SOC and terrorism						
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						
Alignment of threat assessments / risk analyses						
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: Author's own elaboration

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.

6.3 Ranking and comparison of the impacts of policy options

In order to rank and compare the policy options' performance vis-à-vis the baseline scenario, a Multi-Criteria-Analysis (MCA) has been applied in full alignment with the European Commission's *Better Regulation Guidelines* (see Tool #63). Annex IV provides further details regarding the MCA approach used. The MCA is a tool for the qualitative analysis and comparison of a complex set of alternatives concerning the extent to which various measures achieve their objectives, are efficient, coherent etc. It is based on qualitative ratings and rankings with quantitative data supporting the assessment.

Transparency in Multi-Criteria-Analyses (MCA)

The MCA is a qualitative tool, and thus always subject to scrutiny concerning the implicit and explicit judgments made during the assessment process. Therefore, it is crucial for the application of the MCA to be transparent about the data used and the sources, as well as how specific data has fed into and shaped the analysis.

The MCA has been carried out in three steps:

- Step 1: Set-up of the framework of criteria, as well as an assessment grid;
- Step 2: Establishment of an outranking matrix; and
- Step 3: Assessment through a permutation matrix.

The steps are elaborated further below.

6.3.1 Step 1: Set-up of the framework of criteria, as well as an assessment grid

The following three criteria have been used for the MCA in line with the assessments made in section 6. The number in brackets depicts the relative weight of each criterion for the MCA. The higher the number, the more weight the criterion has:

Evaluation of effects

- Effectiveness (Weight 4);
- Efficiency (Weight 3);
- Coherence and proportionality (Weight 2).

Types of impacts

- Security (Weight 3);
- Economy (Weight 1);
- Fundamental rights (Weight 4);
- Society (Weight 1);
- Environment (Weight 1).

The respective weightings indicate the relative importance of the criteria vis-à-vis each other. In the above list, for instance, the weightings show that the effectiveness of the policy option is deemed twice as importance as its coherence for the MCA.

The criteria in relation to the evaluation of the effects have been rated in relation to each of the specific objectives whereas the types of impacts have been rated in relation to each of the policy options as a whole. The following table provides an overview of the numeric ratings that have been used in the tables below.

Table 21 – Overview of ratings in relation to specific objectives

Criteria	Specific objective	BS (PO1)	PO2	PO3
Evaluation of effects				
Effectiveness	1 – Information exchange	0	4	4
	2 – Public order	0	4	4
	3 – SOC & terrorism	0	3	4
Efficiency	1 – Information exchange	0	4	3
	2 – Public order	0	3	3
	3 – SOC & terrorism	0	4	2
Coherence and proportionality	1 – Information exchange	0	4	3
	2 – Public order	0	4	2
	3 – SOC & terrorism	0	4	1
Types of impacts				
Security		0	3	4
Economy		0	2	3

Criteria	Specific objective	BS (PO1)	PO2	PO3
Fundamental rights		0	3	2
Society		0	1	1
Environment		0	1	1

Source: Author's own elaboration

The following table translates these ratings into aggregate values for the MCA's assessment grid.

Table 22 – MCA Assessment grid

Criteria	Direction	Weight	Rating		
			BS (PO 1)	PO2	PO3
Evaluation of effects					
Effectiveness	+	4	0	3.7	4.0
Efficiency	+	3	0	3.7	2.7
Coherence & prop.	+	2	0	4.0	2.0
Types of impacts					
Security	+	3	0	3	4
Economy	+	1	0	2	3
Fundamental rights	+	4	0	3	2
Society	+	1	0	1	1
Environment	+	1	0	1	1

Source: Author's own elaboration

6.3.2 Step 2: Establishment of an outranking matrix

In step 2, based on the assessment grid, an outranking matrix has been developed. In this matrix, the sums of the weights for all criteria in relation to which a given policy option performs better than other policy options are indicated. Based on Table 23, the outranking matrix looks the following way:

Table 23 – MCA Outranking matrix

Policy	BS (PO1)	PO2	PO3
BS	0	0	0
PO2	19	0	9
PO3	19	8	0

Source: Author's own elaboration

The outranking matrix shows that both policy options 2 and 3 are expected to be similarly favourable compared to the baseline scenario (both have received the same score of 19). However, it also shows that policy option 2 has received a higher score compared to policy option 3 (9) than vice versa (8). Therefore, when compared with each other, PO2 is considered more favourable than PO3.

6.3.3 Step 3: Assessment through a permutation matrix

In step 3, the outranking matrix was transformed to a policy permutation matrix in which pairings and the coefficients from the outranking matrix of step 2 were summed up. The permutation matrix provides a clear overview of which policy option is most favourable, second-most favourable, least favourable etc., as well the relative 'favourability' of different combinations of policy options. Since there are three policy options, there are six possible permutations. Their rankings are provided in the table below.

Table 24 – MCA Permutation matrix

#	Permutation			Policy Pairing			Coefficients *					Score	Rank
#1	BS	PO2	PO3	BS PO2	BS PO3	PO2 PO3	0	+	0	+	9	9	5
#2	BS	PO3	PO2	BS PO3	BS PO2	PO3 PO2	0	+	0	+	8	8	6
#3	PO2	BS	PO3	PO2 BS	PO2 PO3	BS PO3	19	+	9	+	0	28	3
#4	PO2	PO3	BS	PO2 PO3	PO2 BS	PO3 BS	9	+	19	+	19	47	1
#5	PO3	PO2	BS	PO3 PO2	PO3 BS	PO2 BS	8	+	19	+	19	46	2
#6	PO3	BS	PO2	PO3 BS	PO3 PO2	BS PO2	19	+	8	+	0	27	4

*Source: Author's own elaboration; * see Table 23*

The permutation table shows that permutation #4 is most advantageous. This means that, based on the assessment, policy option 2 should be implemented. If this is not possible, e.g. due to political reasons, the Commission could aim at implementing policy option 3. In case this should also not be possible, the Commission should remain with the baseline scenario. The scores are interesting: Permutations #4 and #5 almost have the same score. This means that, from a pure MCA perspective, there is only marginal difference between the Commission initiating the policymaking process on the grounds of policy options 2 and 3.

6.4 Elaboration of the preferred policy option

Based on the assessments provided in section 6, as well as the outcomes of the MCA in section 6.3, policy option 2 is most favourable, i.e. a legal proposal on minimum standards that is flanked by supporting (soft) measures.

However, stakeholders have repeatedly pointed out that there are limitations to this option as some measures relating to the access to and exchange of information would only be applicable to SPOCs and not to PCCCs:

- *Technical aspects:* The requirements foreseen for national CMS only apply to SPOCs under policy option 2, whereas the would be extended to PCCCs under policy option 3 (or alternatively that full interoperability between both IT-systems would need to be ensured)
- *Structural aspects:* Policy option 2 includes various minimum requirements for SPOCs (including the requirement to operate 24/7 and having a judicial authority available 24/7 "within" the SPOC). Under policy option 3, these requirements would also apply to PCCCs.

The limited alignment of SPOCs and PCCCs under policy option 2 is expected to create inefficiencies between different law enforcement authorities through the establishment of diverging practices in institutions that should, ideally, be streamlined.

Therefore, the actually preferred policy option would be policy option 2, insofar amended that the measures foreseen in relation to SPOCs would also apply to PCCCs.

A summary of the intervention logic of the preferred option is provided in the table below. The more detailed intervention logic is provided in Annex IV.

Table 25 – Intervention logic of the preferred policy option

No.	Problem	Drivers / Causes	Operational objectives	Elements of the preferred policy option
Specific objective 1: To ensure the efficient access to and exchange of necessary information among law enforcement authorities in an intra-EU context				
1.1	**Legal barrier**: Difficulties in interpreting and implementing provisions on access to and exchange of information	• Unclear EU measures • No exchange of common minimum data sets • Delays in the judicial authorization process • Distinction of information is unclear and complex • Swedish Framework Decision is not aligned with the Law Enforcement Data Protection Directive	Clarity on information available and exchange based on certain regulations	• *Clarification of the scope of operations and competencies* • *Exchange of a common minimum set of data including e.g. wanted/ missing person, persons suspected in criminal activities, etc.* • *Compliance with certain provisions* • *SIENA as the main information channel* • Improvements in the form and functionality of SIENA • *Removal of the reference "other" cases in the SFD* • *Alignment of SFD with the Law Enforcement Data Protection Directive* • *Flanking non-legislative measures*
1.2	**Technical barrier**: Outdated IT infrastructure	• Missing information management tools • Difficulties due to rudimentary search tools • Usage of unsecure communication means	Efficient monitoring and access to and exchange of data	• *Establishment of common requirements for case management systems (CMS)*: - Clear definitions for the CMS. Establishment of common requirements: Degrees of urgency; Manual selection and cancellation of the degrees of urgency; Usage of one CMS; Ability to import and export incoming messages; Clear identification of the case and its components; Automation of data cross-check; Generation of proper statistics - Accreditation of CMS - Quality control through certain requirements and structures - Availability of technical support • *Improvement of digital & radio communication (supporting the EU innovation hub, RECG)* • *Flanking non-legislative measures*
1.3	**Structural barrier**: Difficulties in cooperation due to different national and regional systems and mechanisms and insufficient knowledge about it	• Insufficient coordination and resources of SPOCs/PCCCs • No common structure of the SPOCs/PCCCs information management system • No direct and user-friendly access to relevant databases and platforms • Variations in access and use of databases between Member sates • Limitations of training availability • Limited awareness and knowledge of databases • Decision for information exchange lies with the Member States • Language barriers	Ensuring information exchange between Member states and making sure officials have skills and knowledge to perform duties	• *Establishment of the SPOC as a "one stop shop" for LEA cooperation through common minimum standards. A SPOC should*: - Be set up through its own national legislative or regulation identity - Be sufficiently informed about cooperation requests - Have full access to EU and international law enforcement databases - Be connected to SIENA, i24/7, SIS, SIRENEmail network, and TESTA - Involve staff in the SPOC who have full access to national CMSs - Ensure integration of relevant information from PCCCs in the SPOC info system - Have arrangements to get access to relevant databases - Have full computerized access to hotel registers - Ensure further coordination • *Establishment of new provisions:* - Provision on appropriate English skills - Provision on mandatory training for specific roles • *Establishment of flanking soft measures in the form of training measures:* - Establishment of an awareness raising and training campaign - CEPOL to provide training material on common aspects for Member States - CEPOL to provide voluntary induction training on cross-border law enforcement - Expansion of the existing CEPOL practice - Performance of a regular review of the training content provided by CEPOL

No.	Problem	Drivers / Causes	Operational objectives	Elements of the preferred policy option
Specific objective 2: To ensure that the growing intra-EU mobility is met with an adequate development of tailored joint operations				
2.1	**Legal barrier:** Confusion due to differences in power between the member states	Limited and asymmetric execution power in host states and lack of knowledge on the ground	Clarity on power to get adequate support in other countries	• *New provision on the conferral of powers:* The host MS should confer certain operational powers to officers of seconding MS. Exceptions may be defined • This should enable seconded officers to autonomously perform basic police tasks • *Flanking non-legislative measures*
2.2	**Technical barrier**: Insufficient access to specific information for officers on the ground	Limited access to databases at international events	Ensure prompt access to required data	• *New provision on the remote access to relevant law enforcement databases at specific types of international events* • *Flanking non-legislative measures*:
2.3	**Structural barrier:** Limited resources to ensure an adequate use of joint operations	Challenges covering costs for joint operations including: • Additional costs; • Travel costs; • Accommodation; • Expenses.	Ensuring availability of resources to benefit from joint operations	• *Establishment of an appropriate financial instrument by the Commission* • *Flanking non-legislative measures*
2.4	**Structural barrier:** Insufficient information by joint threat assessment/ risk analysis	• No cooperation between analytical departments in different countries • Limited integration of police and customs information and analysis	Ensuring parties are adequately informed and all information is considered at joint operations	• *New provision on cross-border threat assessment* • *Flanking non-legislative measures*: - Improve the development and use of joint threat assessment and risk analysis - Development of data collection tools
Specific objective 3 : To ensure efficient cross-border operational cooperation in relation to SOC and terrorism				
3.1	**Legal driver:** Inability to efficiently use investigative tools and facing obstacles caused by differences	Rules vary between the Member State: • *Urgent need to address*: Hot pursuit and surveillance, controlled delivery • *Moderate need to address*:, Interception of communication, Use of informants, Witness protection and Covert investigations	Ensuring ability to use investigative tools in an efficient way in intra-EU cross-border cases	• *New provisions on surveillance:* Extend the current EU legal provisions; Establish the possibility to start physical surveillance operations on the territory of another Member State; Simplify the legal requirements; Extend the list of offences in relation to which cross-border surveillance is allowed; Streamline the definitions of "pre-planned" and "urgent" surveillance in the relevant legislative provisions on EU level; Ensure the possibility for technical means of surveillance; Define a common maximum time allowed to carry out cross-border surveillance (e.g. 24 hours); Accept and cooperate with the institutions responsible to oversee cross-border implementation of investigative tools • *New provisions on hot pursuit:* Extend the current EU legal provisions; Extension of offences in relation to which cross-border hot pursuit is allowed; Permit cross-border hot pursuit continue for at least an hour; Establish common rules for hot pursuit; Establish minimum standards on the rights and duties of the pursuing officers • *Flanking non-legislative measures*

Source: Author's own elaboration

In view of the types of problems identified as part of this study, as well as their magnitude and likely future development, the preferred policy option is considered in line with the subsidiarity and proportionality principles. Any measures that were not considered in conformity with these have been discarded throughout the study process. A more detailed analysis of the necessity of EU action, as well as its added value is provided in sections 3.2 and 3.3.

The assessments and MCA have shown that the preferred policy option is expected to have a large positive impact in terms of effectiveness, efficiency, as well as coherence and proportionality. The table below summarises the main advantages and disadvantages of the policy option in this regard in view of the specific objectives for policy intervention.

Table 26 – Main advantages and disadvantages of the preferred policy option

Main advantages	Main disadvantages
Specific objective 1: To ensure the efficient access to and exchange of necessary information among law enforcement authorities in an intra-EU context	
• Expected to facilitate to a large extent the swift exchange of a (minimum) standard set of data via one main channel and, thus in turn contribute to the ability to more effectively fight SOC and manage public order. • 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. • 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. • There are various elements that are expected to have a slightly negative impact on LEAs' ability to safeguard fundamental rights
Specific objective 2: To ensure that the growing intra-EU mobility is met with an adequate development of tailored joint operations	
• Increases clarity on and increased powers of officials who provide support in other Member States and SACs than their own, meaning that they will be able to take on a more operational role than what is currently often the case. This will have a direct impact on the cost-effectiveness of involving officials from other Member States/SAC. • Increased possibilities for direct/remote access to data of officials on the ground that are involved in ensuring public order and safety concerning specific events in specific locations. This will reduce the time taken to access data and will significantly increase the possibilities to rapidly identify whether certain data are available or not. • Contribute to reducing the undue time officials need to devote to cross-border law enforcement cooperation. Law enforcement officials are expected to be able to spend more time on 'solving' cross-border cases rather than 'administrating' them. • Similar to the above, option is expected to contribute in a largely positive way to safeguarding fundamental rights.	• Necessitates increased budgetary spending from the Member States, but will also be supported by the EU, which will provide financial support for certain costs in relation to joint operations. • Again, there are various elements that are expected to have a slightly negative impact on LEAs' ability to safeguard fundamental rights
Specific objective 3: To ensure efficient cross-border operational cooperation in relation to SOC and terrorism	
• Significantly facilitates the use of investigative tools in cross-border situations. This means that an efficient and coordinated response addressing the increasing cross-border challenges linked with SOC and terrorism can take place to a higher degree than what is currently possible. • The assessment of the impacts on fundamental rights is similar to the above.	• In terms of substance, the assessment of the impacts on fundamental rights is similar to the above. • However, the actual impact is expected to be more far reaching than under PO2.

Source: Author's own elaboration

Overall, it is expected that the preferred policy option will have a large impact on the efficiency of EU cross-border law enforcement cooperation. However, reliable quantitative data on costs are largely missing. With the scale and intensity expected to increase in the future, the overall macro-level, EU-wide costs associated with law enforcement cooperation can naturally also be expected to increase. This being said, at the micro-level, it is expected that the preferred policy option will contribute to reducing 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 foreseen under the preferred policy option.

Table 27 – Main types of costs expected to be reduced / increased with preferred policy option

Main types of costs increased	Main types of costs decreased
Specific objective 1: 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) *Member State level:* • Necessitates investments at MS level, including for IT- and staff-related investments. • Increased budgetary spending by MS on officers' training	*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) • Less time needed for case management • Fewer resources needed for case management, i.e. more resources spent on „solving cases"
Specific objective 2: To ensure that the growing intra-EU mobility is met with an adequate development of tailored joint operations	
EU level: • EU funding (e.g. through the Internal Security Fund) and financial support • Costs in relation to awareness raising and training (incl. by CEPOL) *Member State level:* • Increased budgetary spending on cross-border operations, e.g. Staff; Travel; Accommodation; Expenses. • Increased budgetary spending on officers' training.	*EU level:* • n/a *Member State level:* • Costs in relation to the development and implementation of data collection tools • Costs for the development of risk analyses shared with other Member States
Specific objective 3: To ensure efficient cross-border operational cooperation in relation to SOC and terrorism	
EU level: • EU funding (e.g. through Internal Security Fund) and financial support • Costs in relation to awareness raising and training (incl. by CEPOL) *Member State level:* • Necessitates investments in modern technology concerning investigative tools, as well as in relation to respective training for officials. • Increased budgetary spending on officers' training.	*EU level:* • n/a *Member State level:* • Technology-supported investigative tools will enable law enforcement officials to conduct their investigations quicker and at less costs.

Source: Author's own elaboration

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.

It is of critical importance to carefully take account of these success factors with a particular view to safeguarding fundamental rights.

In addition to these success factors, the implementation of the preferred policy option should be closely monitored in order to ensure that expectations are being met adequately. The following set of high-level indicators should be regarded as a basis upon which a more detailed monitoring framework should be developed in the future:

Table 28 – Main indicators for the monitoring of the preferred policy option

	Implementation ("outputs")	Application ("results & impacts")
SO1: Access to and exchange of information	• Number of messages sent / received • 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[223] • Level of awareness and knowledge among officials • Degree of smoothness of law enforcement cooperation
SO2: Management of public order and safety	• Number of joint operations • Number of officials sent across borders • Number of remote requests for access to databases • Share of outflow and usage of funds • Degree of application of data collection tools • Capital / operational expenditures, e.g. in relation to IT and training	In addition to SO1: • Number of basic police tasks, such as identity checks, vehicle and body search by seconded officials • Clarity of risk and threat landscape in the EU
SO3: Fight against SOC and terrorism	• Number of instances in which different investigative tools have been implemented • Degree to which modern technology is applied in cross-border situations • Capital / operational expenditures, e.g. in relation to IT and training	In addition to SO1: • Number of instances in which foreign officials have performed basic police tasks across borders • Average duration and geographical reach of the use of investigative tools

Source: Author's own elaboration

The responsibility for the collection of the relevant monitoring data should be in the hands of national authorities. In particular the SPOCs are expected to be well placed to perform such activities in line with national legislation as the competent authority. Relevant data could e.g. be gathered from national statistical offices and, more specifically, from the law enforcement authorities at different national levels to which the legislative proposal governing the preferred policy option applies. In terms of frequency, data should be gathered by competent authorities at least on a biannual basis.

Subsequently, the monitoring data gathered should be used to inform an evaluation of the implementation of the preferred policy option, e.g. five years after its entry into force and / or the deadline for transposition of the legal instrument.

[223] Depending on the type of case, this could mean e.g. apprehensions and arrests.

In line with the Commission's *Better Regulation Guidelines*, notably tool #47[224], the minimum criteria against which the implementation of the preferred policy option should be evaluated are:

- ***Relevance***, e.g.: To what extent is the intervention still relevant? To what extent have the (original) objectives proven to have been appropriate for the intervention in question? How well do the (original) objectives of the intervention (still) correspond to the needs within the EU?
- ***Effectiveness***, e.g.: What have been the (quantitative and qualitative) effects of the intervention? To what extent do the observed effects link to the intervention? To what extent can these changes/effects be credited to the intervention?
- ***Efficiency***, e.g.: To what extent has the intervention been cost effective? To what extent are the costs of the intervention justified, given the changes/effects it has achieved?
- ***Coherence***, e.g.: To what extent is this intervention coherent with other interventions which have similar objectives?
- ***EU added value***, e.g. What is the additional value resulting from the EU intervention(s), compared to what could reasonably have been expected from Member States acting at national and/or regional levels?

The Commission's legal proposal relating to the preferred policy option needs to incorporate the necessary monitoring and evaluation clauses.

Political feasibility

It can be noted that the political feasibility of new measures in the area of law enforcement cooperation is general challenging, but in particular a legislative proposal in relation to objectives #2 and #3 concerning operational cooperation may be met with insufficient political support. In such case, the Commission could e.g. take the approach of addressing objective #1 concerning information exchange through a new proposal amending the SFD, supported by a Communication and / or Recommendation concerning the foreseen measures in relation to objectives #2 and #3, thus *encouraging* the Member States to take the proposed action instead of proposing an amendment to e.g. Prüm. The *types* of effects and impacts that would result from a Communication or Recommendation would be the same as those that have been outlined above in section 6 for policy option 2. However, the *extent/magnitude* of the impacts would be dependent on the willingness of the Member States to take up the proposed measures. Overall, it can be expected that while the types of effects would be the same as those described above in section 6, their extent / magnitude would be lower.

[224] See: https://ec.europa.eu/info/sites/default/files/file_import/better-regulation-toolbox-47_en_0.pdf

GETTING IN TOUCH WITH THE EU

In person
All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at:
https://europa.eu/european-union/contact_en

On the phone or by email
Europe Direct is a service that answers your questions about the European Union. You can contact this service:
- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696, or
- by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online
Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications
You can download or order free and priced EU publications from: https://op.europa.eu/en/publications.
Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents
For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU
The official portal for European data (https://data.europa.eu/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

DR-01-21-413-EN-N

Publications Office
of the European Union

doi: 10.2837/179127
ISBN 978-92-76-43474-0