



Brussels, 8.12.2021
SWD(2021) 377 final

COMMISSION STAFF WORKING DOCUMENT
EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT REPORT

Accompanying the document

Proposal for a Directive of the European Parliament and the Council
on information exchange between law enforcement authorities of Member States,
repealing Council Framework Decision 2006/960/JHA

{COM(2021) 782 final} - {SEC(2021) 420 final} - {SWD(2021) 374 final}

Executive Summary Sheet

Impact assessment on a proposal to modernise existing intra-EU law enforcement cooperation by creating an EU police cooperation code on information exchange and communication

A. Need for action

Why? What is the problem being addressed?

Security and cross-border crime (including tax crimes) are, by definition, an international issue. As mentioned in the 2020 EU Security Union Strategy, Europe faces a **security landscape in flux**, with evolving and increasingly complex security threats. These threats spread across borders and manifest themselves in organised crime groups that engage in a wide range of criminal activities. Even a seemingly local crime may have links to other offences committed across Europe by the same perpetrators. Furthermore, the **growing intra-EU mobility** creates additional challenges for the prevention and fight against all forms of criminal threats.

The rapidly **evolving criminal landscape and the increased mobility of people** suggests that cross-border cooperation between law enforcement authorities in the EU will be crucial to tackle criminal offences, and allow EU citizens to safely enjoy their rights of free movement in the future.

However, there are still borders and obstacles for data exchange between law enforcement, which leads to blind spots and loopholes for numerous criminals and terrorists that act in more than one Member State. Given the cross-border nature of fighting crime and enhancing security, Member States must rely on one another to close the information gap.

Law enforcement authorities in the EU cooperate and exchange information, notably based on the Framework Decision (2006/960/JHA) on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU (Swedish Framework Decision – SFD), but there are important shortcomings.

Law enforcement authorities **do not effectively nor efficiently exchange information** with their partners in other Member States because of **three legal, structural and technical problems**.

- 1) **Rules at national level impede the effective and efficient flow of information.** Indeed, the 2006 Swedish Framework Decision is not fully implemented preventing law enforcement authorities from other Member States from receiving such information in an effective and efficient way;
- 2) **Structures at national level are not always set up and equipped in a sufficiently efficient and effective manner.** Indeed, Member States do not always have the necessary structures in place to receive information requests from other Member States, channel them to the right authorities at national level, and provide the requested information accordingly;
- 3) **The free choice of communication channel(s) between Member States causes recurrent duplication of requests.** Indeed, Member States' law enforcement authorities use a variety of different channels to send information request to other Member States and respond to them, which hampers effective and efficient exchange of information.

These three problems are interlinked. All three issues raise important policy choices that require a detailed assessment of the problem drivers, the related objectives, available policy options and their impact.

What is this initiative expected to achieve?

This initiative is expected to fundamentally support the Member States in fulfilling their commitment to law enforcement cooperation. It responds to pressing operational needs and calls from the Council to consider *"consolidating the EU legal framework to further strengthen cross-border law enforcement cooperation, to support the development of smooth and swift information exchange and further development of relevant structures and platforms"*.

The initiative seeks to achieve the following **objectives**:

- 1) **Objective I:** To facilitate **equivalent access for law enforcement authorities** to information held in another Member State (similar to the access granted to information within a Member State), while complying with fundamental rights and data protection requirements;
- 2) **Objective II:** To ensure that all Member States have an effective functioning **Single Point of Contact**

(SPOC), including when a **judicial authorisation** is required to provide the data upon request of another Member State, and ensuring its effective cooperation with **Police and Customs Cooperation Centres (PCCCs)**;

- 3) **Objective III**: To establish a **mandatory default communication channel** for law enforcement information exchange between Member States (where relevant).

What is the value added of action at the EU level?

EU action is expected to bring benefit for the entire EU with a ripple effect on Schengen Associated Countries, by reinforcing the overall security and trust among the Member States. In doing so, it is expected to support the Schengen core principle (an area without controls at internal borders).

Common **EU level rules, minimum standards and requirements** will highly enhance information flow, in line with **high-level data security** and **data protection** standards.

Additionally, common standards allow for certain level of automation in information exchange workflows thereby releasing law enforcement officers from certain labour-intensive/time-consuming manual activities.

B. Solutions

What legislative and non-legislative policy options have been considered? Is there a preferred choice or not? Why?

A number of legislative policy options have been considered. Following a pre-selection, some options were quickly discarded. The other **policy options have been assessed in full detail**:

- 1) Policy option addressing **objective I**: (*'facilitate the equivalent access to information'*)
 - **policy option 1.1**: Legal proposal updating the 2006 Swedish Framework Decision (SFD) to ensure its alignment with the 2016 Law Enforcement Data Protection Directive + flanking soft measures (training, Commission guidance);
 - **policy option 1.2**: Option 1.1 + simplification in the use of the SFD + improve clarity on the national data sets available for possible exchange;
 - **policy option 1.3**: Option 1.2 + provisions ensuring compliance with deadline requirements by which data is to be made available to another Member State (including when a judicial authorisation is required).
- 2) Policy options addressing **objective II**: (*'ensure that all Member States have an effective functioning Single Point of Contact (SPOC), including when a judicial authorisation is required to provide the data upon request of another Member State, and ensuring its effective cooperation with Police and Customs Cooperation Centres (PCCCs)'*)
 - **policy option 2.1**: Continue with Council non-binding guidelines on national Single Points of Contact + flanking soft measures (training, financial support, guidance);
 - **policy option 2.2**: *Approximation of minimum standards* on the composition of the Single Points of Contact (including the mandatory presence of a judicial authority), its functions, staffing and IT systems, and in its cooperation with regional structures such as Police and Customs Cooperation Centres + flanking soft measures (training, financial support, guidance);
 - **policy option 2.3**: *harmonisation* of rules on the composition of the Single Points of Contact (including the mandatory presence of a judicial authority), its functions, staffing and IT systems, and its cooperation with regional structures such as Police and Customs Cooperation Centres + flanking soft measures (training, financial support, guidance).
- 3) Policy options addressing **objective III**: (*'establish a mandatory default communication channel for law enforcement information exchange between Member States (where relevant)'*)
 - **policy option 3.1**: Continue with Council non-binding guidelines and Recommendations to put Europol in copy when using SIENA¹ in cases within Europol¹ mandate + flanking soft measures

¹ Europol's "Secure Information Exchange Network Application".

(training, financial support);

- **policy option 3.2:** Obligation to use the same communication channel for the same purpose (making of Europol SIENA the preferred channel where relevant) + obligation to put Europol in copy when using SIENA in cases within Europol's mandate + Flanking soft measures (as in option 3.1);
- **policy option 3.3:** obligation to use SIENA by default for all bilateral information exchange (unless otherwise regulated by EU law) + obligation to put Europol in copy when in cases within Europol's mandate, both after the end of a transition period and with Internal Security Fund support for the SIENA roll-out + flanking measures (as in policy option 3.1) .

Following a detailed assessment of the impacts of the main policy options, the **package of preferred policy options** consists of **policy option 1.3, policy option 2.2 and policy option 3.3.**

Who supports which option?

Stakeholders are generally supportive of the development of smooth and timely information exchange and for further development of relevant structures and platforms.

Member States are expected to support most of the measures envisaged under the preferred option. At the same time, Member States are conscious of the importance of their national sovereignty in the area of law enforcement from an operational and procedural perspective. Positive opinions expressed at expert level may not be further shared at political level.

The main likely point of debate concerns the option 3.3 (making of Europol SIENA the mandatory channel of communication between Member States (unless otherwise ruled by EU law). Yet, this option has also been defended by Member States at Council: "*applying SIENA as the default communication channel would add to the streamlining of law enforcement information exchange, and increase the level of security in the context of police cooperation in the Union. By the same token, it would enable that efforts be focused on the development of a single instead of numerous solutions, thus fostering the objective of reaching enhanced EU internal security*".

The European Parliament is expected to verify the existence of strong data protection safeguards. Indeed, discussions with all stakeholders showed the importance of appropriate safeguards to ensure the respect of Fundamental Rights, and in particular the right to the protection of personal data.

C. Impacts of the preferred option

What are the benefits of the preferred options (if any, otherwise main ones)?

The preferred policy option, a game changer, would respond effectively to the identified problems while stepping up Europol' support to member States, with the final objective of **preventing, detecting and investigating criminal offences**, in full **compliance with fundamental rights**.

The **ultimate beneficiaries of the preferred option are the citizens**. They will directly and indirectly benefit from better crime fighting and lower crime rates. In terms of efficiency, the **main beneficiaries are national law enforcement authorities**.

What are the costs of the preferred options (if any, otherwise main ones)?

The preferred policy option requires investments at both EU and Member States' level. These costs would essentially concerns IT upgrades and training. These cost would vary significantly from one Member State to the next depending on the efficiency and effectiveness of their national Single Point of Contact and Police and Customs Cooperation Centres (if any).

The preferred policy option provides for efficient solutions to challenges which would otherwise have to be addressed at higher costs, show poor compatibility or which would be less efficient.

Some of the policy options are however difficult to quantify. According to Europol data, the costs associated with the integration of Europol SIENA in 20 Member States Case Management Systems (CMS) and the development of CMSs in 10 Member States are estimated to EUR 2.5 million (one-time investment needed). Efficiency benefits would offset these costs (fewer resources needed for case management, i.e. more resources spent on "solving cases").

The preferred policy option does not contain regulatory obligations for citizens/consumers, and therefore do not

create additional costs for these stakeholders either.
How will businesses, SMEs and micro-enterprises be affected?
The preferred policy option could have a small positive impact on small and medium-sized enterprises given increased demand for IT products and services.
Will there be significant impacts on national budgets and administrations?
<p>As mentioned above, the preferred policy option requires investments at Member States' level. These costs would essentially concerns IT upgrades and training. Some of the policy options are however difficult to quantify. These cost would vary significantly from one Member State to the next depending on the efficiency and effectiveness of their national Single Point of Contact and Police and Customs Coopepration Centres (if any).</p> <p>According to Europol data, the costs of developing a Case Management System at national level could be of EUR 150.000 (one-off) per Member State. Efficiency benefits would offset these costs (fewer resources needed for case management, i.e. more resources spent on "solving cases").</p> <p>The necessary IT upgrades in both SPOCs and PCCCs could amount to a maximum grand total of EUR 11,5 million (EUR 2.5 million for SPOCs + EUR 9 million for PCCCs).</p> <p>These costs (one-off investment), deemed acceptable, are proportionate to the identified problem and do not go beyond what is necessary to achieve the specific objective. The EU Internal Security Fund will provide support (essentially via national programmes).</p>
Will there be other significant impacts?
<p>The preferred policy option empowers Member States national and regional information hubs with a view to more effectively and efficiently access and share existing data.</p> <p>The preferred policy option also ensures the full alignment of a new Directive on information exchange and communication with the 2016 Data Protection Law Enforcement Directive. Such alignment ensures an explicit compliance with Fundamental Rights which is not currently the case with the 2006 Swedish Framework Decision.</p> <p>The preferred policy option meets an objective of general interest and is strictly limited to what is necessary and proportionate to achieve such objective.</p>
D. Follow-up
When will the policy be reviewed?
[Two] years after the transpositon deadline, and every [four] years thereafter, the Commission should submit to the European Parliament and the Council two reports. The first , assessing the extent to which the Member States have taken the necessary measures to comply with this Directive; the second , assessing its results against its objectives and the continuing validity of the underlying rationale and any implications for future options.