Ref. Ares(2022)1237735 - 18/02/2022

European Commission

CALL FOR EVIDENCE
FOR AN IMPACT ASSESSMENT

TITLE OF THE INITIATIVE	Security-related information sharing − reciprocal access for frontline officers in the EU and key partner countries
LEAD DG (RESPONSIBLE UNIT)	DG HOME/B3
LIKELY TYPE OF INITIATIVE	*to be determined*
INDICATIVE TIMETABLE	Q4-2022
ADDITIONAL INFORMATION	-

A. Political context, problem definition and subsidiarity check

Political context

The letter of intent accompanying President von der Leyen's 2021 State of the Union speech refers to a new initiative for a legislative proposal on a framework to enable reciprocal access for frontline officers to security-related information shared between the EU and key partner countries. This initiative aims to counter shared security threats. It has been included in the Commission work programme 2022.

Problem the initiative aims to tackle

In recent years, the EU has adopted and implemented a wide range of actions to strengthen security within its borders (e.g. a new interoperable IT architecture). **Access to information is key** to further strengthen internal security but also to strengthen security in partner countries in order to create a common, larger area of high-level security. In contrast to, e.g. the United States, the EU is not making critical security-related information available **beyond its borders** to frontline border guards and police officers in partner countries. Meanwhile, terrorism and its financing as well as organised crime, e.g. i) illicit drugs and arms trafficking, ii) migrant smuggling, iii) trafficking in human beings, and iv) child sexual abuse and exploitation are not constrained by borders.

While Europol acts as a hub for the (indirect) information exchange between partner countries and Member States, cooperation agreements between Europol and partner countries do not provide for making data available directly and in real time to frontline border guards or police officers. Whereas it is possible to share sensitive security-related information with trusted Interpol members via the **Interpol systems**, it is not clear whether this sufficiently enables the exchange of actionable information[1] directly with frontline border guards and police officers. At present, there is no EU mechanism in place to systematically make critical and actionable partner-country sourced information available directly and in real time to frontline border guards or police officers in the Member States[2]. Several bilateral or multilateral arrangements between Member States or the EU and some partner countries allow for information to be exchanged with partner countries for investigative purposes. This initiative would go one step further.

A **tailor-made new European solution** would have the benefit of creating a common EU approach. This should enable: i) all frontline border guards and police officers in the Member States to access actionable data from partner countries[3], and ii) frontline border guards and police officers in partner countries to access information provided by all Member States. Therefore, it could make it possible for the partner countries to cooperate with the EU as a whole on a reciprocal basis. Furthermore, regarding potential partner countries, it would provide transparency on the minimum conditions and expectations from the EU side concerning data protection and

[1] For example, information related to people involved in serious criminal activities (organised crime or terrorism), objects connected to such activities as well as information related to missing persons, people who are sought to assist with a judicial procedure, people in danger and non-EU country nationals subject to an entry ban.

[2] These could be border guards carrying out border control as defined by the Schengen Borders Code and police and other law enforcement officers (security services in charge of combatting cross-border crime, terrorism and other threats affecting internal security of the EU and its Member States and of partner countries).

[3] Such as countries geographically close to EU borders, including potential future EU members, and countries with which the EU has already established close cooperation on security-related matters

fundamental rights standards.

Basis for EU action (legal basis and subsidiarity check)

Legal basis

The legal basis giving the EU the right to act could include the following Articles from the Treaty on the Functioning of the European Union (TFEU): i) 16(2) on data protection; ii) 77(2) on measures to be adopted to ensure a policy on borders checks, asylum and immigration is developed; iii) 82 on judicial cooperation in criminal matters; and iv) 87 on police cooperation. This depends on the final scope of the proposal. On the basis of the legislative act, international agreements with the partner countries will be necessary under Article 216 TFEU on international agreements.

Practical need for EU action

The initiative is in the area of shared competence. The problem cannot be solved by the Member States acting alone as this would not ensure that data are exchanged systematically and instantly between all Member States and key partner countries. EU action would ensure that, for the first time, a common tool is established with common safeguards and conditions allowing frontline officers in the EU and in key partner countries systematic and instant access to security-related information.

B. Objectives and policy options

The objective is to produce a European solution allowing, through one single channel, frontline officers in all Member States systematic and instant access to security-related information from partner countries, and frontline officers in partner countries access to such information provided by all Member States.

Policy options

1. **Baseline scenario**: security-related data would continue to be exchanged under current and planned mechanisms (bilateral or multilateral arrangements between Member States, EU and partner countries, Europol cooperation agreements, Schengen Information System (SIS) alerts based on partner country information, Interpol systems, Prüm framework, etc.).
2. **Instrument outlining a data exchange mechanism with partner countries (reciprocity to be decided on a case by case basis):** security-related data would be exchanged following a request for information from one partner to the other without direct access to information in a database:
   a) **non-legislative instrument** – model negotiating directives for future international negotiations with partner countries; or
   b) **legislative instrument** – setting out the terms and conditions for exchanging data with partner countries on the basis of which future negotiating directives for international negotiations with partner countries would be developed.
3. **Legislative proposal setting out the terms and conditions for exchanging security-related data with partner countries and setting up the technical solution for this purpose (reciprocity to be decided on a case by case basis)**:
   a) **separate databases** kept by each partner with each partner getting direct or indirect access to the information stored in the separate databases; or
   b) **single shared database** inspired by the SIS model[4], but separate from the SIS.

Options 2 and 3 would need to be accompanied by memorandums of understanding or international agreements with partner countries – primarily those geographically close to EU borders, including potential future EU members – and countries with which the EU has already established close cooperation on security-related matters.

C. Likely impacts

The initiative will ensure increased security in the EU as frontline officers will have direct access to security-related information from partner countries, enabling them to take instant action in case someone representing a threat is located. It will also enable frontline officers in partner countries to take action based on security-related information shared with them by EU Member States. Furthermore, it will have an impact on fundamental rights, in particular on the rights to privacy and to protection of personal data. It will be ensured that the initiative respects the Charter of Fundamental Rights.

By ensuring increased security in the EU and in partner countries, the initiative could also help protect the fundamental rights of EU citizens. The initiative will ensure that these benefits are available to all EU Member States on an equal footing. The initiative will also add burden, as EU Member States will have to add and access

[4] The SIS database is designed to boost existing security measures by maintaining identification information on individuals and entities for the purposes of national security, border control and law enforcement. It allows for information exchanges between national border control, customs and police authorities ensuring that the free movement of people within the EU can take place in a safe environment. It contains alerts on people, such as those wanted for arrest or who are not entitled to enter or to stay in the Schengen area, as well as information on certain property, such as banknotes, cars, firearms and identity documents that may have been stolen, misappropriated or lost.

security-related information for a new purpose and follow up on possible hits. However, synergies for Member States' procedures will be sought to reduce this additional burden as much as possible.

D. Better regulation instruments

Impact assessment

An impact assessment is being conducted to support the preparation of this initiative and feed into the Commission's decision. The likely timing of the impact assessment process is Q3 2022.

Consultation strategy

A public consultation will be conducted in Q1/Q2 2022 to give stakeholders a chance to share their views, in particular on how the initiative i) contributes to security and the protection of the EU's external borders, and ii) safeguards the protection of data subjects' rights and fundamental rights. The consultation will target the general public, civil society organisations, industry and other stakeholders. Consultation activities:

- public consultation will be made available on the 'Have your say' portal
- duration: at least 12 weeks
- languages of consultation and replies: all official languages
- results available on: the Commission's central public consultations page, on 'Have your Say'.

As part of the preparation of the impact assessment, targeted consultations will also take place with: i) the European Parliament; ii) Member States; iii) EU Agencies and bodies such as the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), the European Border and Coast Guard Agency; the European Data Protection Supervisor; Europol; and the Fundamental Rights Agency

The consultation will be promoted on the DG HOME website. The factual summary report will be published on the consultation page 8 weeks after the public consultation has closed. Furthermore, a synopsis report, which includes a summary of all consultation results, will be prepared.

Why we are consulting?

The consultation will give stakeholders a chance to share their views, in particular on how the initiative i) contributes to security, and the protection of the EU's external borders, and ii) safeguards the protection of data subjects' rights and fundamental rights.

Target audience

The consultation will target the general public, civil society organisations, industry and other stakeholders.