Frequently asked questions - Interoperability of EU information systems for security, border and migration management

Strasbourg, 12 December 2017

What is this proposal about?

Interoperability is the ability of information systems to exchange data and enable sharing of information. It improves the efficiency and effectiveness of Europe-wide information-sharing tools, by ensuring the technical processes, standards and tools that allow EU information systems to work better together. It means that authorised users (such as police officers, migration officials and border guards) have faster, seamless and more systematic access to the information they need to do their jobs.

Interoperability does not mean pooling all data or collecting additional categories of information. It does not entail data registered in one system being automatically shared across all other systems. Interoperability is about a targeted and intelligent way of using existing data to best effect while at the same time ensuring full respect of fundamental rights, in particular data protection requirements. It is about better protecting the EU's external borders, improving migration management and enhancing internal security for the benefit of all citizens.

Why do we need interoperability?

Over the past three years, threats to internal security have evolved and are still very much in evidence, as demonstrated by the series of terrorist attacks in several Member States and the increase in irregular crossings of the EU's external borders. These challenges have brought into sharper focus the urgent need to strengthen the EU's information tools for security, border and migration management.

Data management in these areas must be made more effective and efficient, in full respect of fundamental rights, to better protect the EU's external borders and improve internal security. Whilst EU information systems provide border guards and law enforcement officers with important security information on individuals, the current EU data management architecture still requires improvement in order to be able to provide the right information at the right time. In particular, making the various information systems at EU level interoperable — able to exchange data and share information so that authorities and officers have the information they need, when and where they need it – would help eliminate blind spots where people, including those involved in terrorist activities, may be recorded in different, unconnected databases under different aliases.

The interoperability proposal builds on the recommendations of the high-level expert group on information systems and interoperability. The expert group underlined the need to act to address the structural shortcomings identified by the Commission in April 2016:

- sub-optimal functionalities in some of the existing information systems;
- information gaps in the EU's data management architecture;
- a complex landscape of differently-governed information systems; and
- a fragmented data management architecture for borders and security where information is stored separately in unconnected systems, leading to blind spots.

Today's proposal responds to the needs identified during a transparent and extensive consultation process, including technical and consultative meetings with stakeholders and Member States, and involving the European Parliament and relevant authorities (European Data Protection Supervisor, EU Fundamental Rights Agency, EU Counter-Terrorism Coordinator). The proposal also takes on board the views expressed by interested stakeholders during a public consultation. Three studies were also commissioned to support the preparation of the proposal.

Which information systems are concerned by this proposal?

Today's proposal on interoperability is focusing on the information systems for security, border and migration management that are operated at EU level as well as those that are in the process of being developed or awaiting adoption by the European Parliament and the Council. The six systems include:

Three existing systems:

- the **Schengen Information System (SIS)** which contains a broad spectrum of alerts on persons (refusals of entry or stay, EU arrest warrants, missing persons, judicial procedure assistance, discreet checks) and objects (including lost, stolen or invalidated identity or travel documents);
- the **Eurodac system** with fingerprint data of asylum applicants and of third-country nationals who have crossed the external borders irregularly or who are irregularly staying in a Member State; and
- the **Visa Information System (VIS)** with data on short-stay visa holders.

Three systems that are still in preparation or development:

- the future **Entry/Exit System (EES)**, which has been adopted and will replace the current system of manual stamping of passports and will electronically register the name, type of travel document, biometrics and the date and place of entry and exit of third-country nationals visiting the Schengen area for a short stay;
- the **proposed European Travel Information and Authorisation System (ETIAS)**, which once adopted would be a largely automated system that would gather and verify security-related information submitted by visa-free third-country nationals ahead of their travel to the Schengen area; and
- the **proposed European Criminal Records Information System for third-country nationals (ECRIS-TCN system)**, which once adopted would be an electronic system for exchanging information on previous convictions handed down against third-country nationals by criminal courts in the EU.

The EES and the proposed ETIAS have been designed in such a way that they already present a degree of interoperability between themselves and with the VIS.

The scope of this proposal also includes **Interpol's Stolen and Lost Travel Documents (SLTD) database**,which should be systematically queried at the EU's external borders. The interoperability components would also make it easier to consult **Europol data** including via the proposed European Travel Information and Authorisation System.

The proposal does not cover national information systems or decentralised EU information systems.

What are the main elements of the Commission's proposal?

The four technical components of the proposal are:

- a **European search portal** — this tool will enable authorised users (for instance an authorised police officer) to carry out a single search and receive results from all the systems they are authorised to access, rather than searching each system individually. This will ensure that relevant and authorised systems are systematically and automatically checked.
- a **shared biometric matching service** — this will allow users to more efficiently search and cross-match biometric data (fingerprints and facial images) stored in the systems that they are authorised to access.
- a **common identity repository** — this will allow authorised users to more easily access biographical information about non-EU citizens stored in relevant systems, so that they can be more reliably identified.
- a **multiple identity detector** — this will verify whether the biographical data that is being searched exists in multiple systems, helping to detect multiple identities. It has the dual purpose of ensuring the correct identification of *bona fide* persons and combating identity fraud.

The Commission is also proposing three additional measures that will help the systems work more effectively together:

- creating a **central repository for reporting and statistics**, necessary for creating and securely sharing reports — prepared on the basis of anonymous statistical data — for policy, operational and data quality purposes.
- making the **Universal Message Format** the EU standard for the development of information systems in the area of justice and home affairs, including creating an appropriate governance structure for the format. This format creates a common technical language to describe and link pieces of data, in particular data relating to people and documents, which means that different systems can more easily compare data and work together. It will also make it easier to integrate new information systems and make them interoperable with existing systems.

- creating **automated data quality control mechanisms** and common quality indicators. It is crucial that Member States ensure the highest level of data quality when feeding and using the systems. To overcome problems that can arise from the input of data by human operators, automatic validation rules can prevent mistakes. The aim of these measures isto automatically identify apparently incorrect or inconsistent data submissions so that these can be checked and corrected as needed.

How will interoperability improve the current set-up of EU information systems?

The current EU information systems were each developed at a specific point in time, and for a specific purpose. This has led to a fragmented data management architecture for borders and security where information is stored separately in largely unconnected systems, leading to potential blind spots and a complex landscape of differently-governed information systems.

In light of the recent terrorist attacks in Europe and the increase in irregular migration in recent years, action needs to be taken to address this risk of information gaps and blind spots. The measures in this proposal will ensure the various systems can exchange data and share information so that authorised bodies and officers have the information they need to strengthen our borders and better protect Europe.

The proposed solutions will lead to faster, more systematic access to information for authorised users, simplifying the current complex and diverse access conditions to ensure that information is more easily available to people who have the right to see it, in line with the rights set out in the legislation governing each system. They will make it easier for end-users to determine when people have been registered with multiple identities, both facilitating travel for legitimate travellers and combating identity fraud. They will make it easier for authorised officers to reliably identify third-country nationals who are entering, or who are already on, the territory of the Schengen area.

There will also be technical benefits, making it easier for Member States to implement and integrate new information systems, strengthening and streamlining data security and data protection conditions in place for these six systems, and improving and harmonising data quality requirements for the systems.

What data will be affected by this proposal?

No additional information about people will be collected as a result of the interoperability measures in this proposal. The new functionalities will build on the existing and future EU systems, which will keep their own access rights: the Schengen Information System (SIS), the Visa Information System (VIS), Eurodac, the future Entry/Exit System (EES), the proposed European Travel Information and Authorisation System (ETIAS) and the proposed European Criminal Records Information System for third-country nationals (ECRIS-TCN system).

Each piece of data should be stored, added, modified and deleted in accordance with the respective legal basis that applies to that system.

Who will have access to the data in the systems? Will interoperability mean more people can see personal data?

Interoperability is not about undermining data protection – quite the contrary. The high existing standards of EU data protection laws will be maintained and will ensure that personal data is processed fairly and proportionately.

Today's proposal embeds these data protection rules – indeed, it is based on the principles of data protection by design and by default. It includes appropriate provisions limiting data processing to what is necessary for a specific purpose and granting data access only to those who need to know. Data retention periods (where relevant) are appropriate and limited.

Access to data is reserved exclusively for authorised staff (such as police officers, migration officials and border guards) of the Member State authorities or EU bodies that are competent for the specific purposes of each information system, such as police officers, border guards or migration officials, depending on the system. This access is limited to what is required for the performance of tasks in accordance with the purposes of the system.

Today's proposal does not modify the rights of access – what it does is simplify and streamline the processes to access the data, ensuring that there is more systematic consultation of and checks against the data available and that it is available to authorised users more swiftly and efficiently. It proposes to establish access for police authorities to the common identity repository for the purpose of identity checks. And it streamlines the access of law enforcement authorities to non-law enforcement information systems for the purpose of prevention, investigation, detection or prosecution of serious

crime and terrorism.

How does the proposal facilitate and streamline law enforcement access?

To complement the interoperability components, the Commission is also proposing to **facilitate and streamline law enforcement access** to non-law enforcement systems by introducing a two-step data consultation approach. This approach will ensure that authorised law enforcement officials can more swiftly and efficiently access the information they require to prevent, investigate, detect or prosecute terrorism and other serious criminal offences.

Under the new two-step data consultation approach, a law enforcement officer would **first check** in parallel all the systems storing their data in the common identity repository in order to know whether information on the searched person existed in any of the systems. To ensure data protection, only a "hit/no-hit" reply would be given. The officer would not have access to any data in any system but crucially would know that such data existed.

In a **second step**, the officer would then be able to request full access to the information system(s) that generated hits, with an individual access request for and in line with the respective rules established by each system concerned. As at present, the officer would need to justify the need to access the system, in line with its access rights and purpose limitation principles with subsequent full access remaining subject to prior authorisation by a designated authority and continuing to require a specific user ID and login.

Once such a two-step data consultation approach applies, there will no longer be any need for a prior search in national databases and the launch of a prior search in the automated fingerprint identification system of other Member States under Decision 2008/615/JHA ('Prüm check').

Will interoperability have an impact on individuals?

Interoperability of information systems is a way to ensure that information is shared appropriately and efficiently with those who have both the need and the right to access it.

Ensuring efficient information sharing will also contribute to simplifying procedures for the individuals concerned. The systems involved – with the exception of SIS – focus exclusively on third-country nationals.

Securing the correct identification of a person will have a positive impact on the right to respect for private life, and in particular the right to one's identity (Article 7 of the Charter), and also the right to good administration.

The processing of personal data for the purposes of interoperability *fully respects human dignity and integrity*, with particular attention paid to vulnerable groups such as children, the elderly and persons with a disability.

Overall, the measures will help reassure EU citizens that any third-country national on the European territory has a known genuine identity and a valid reason to be there. Furthermore, the interoperability measures will strengthen the capability of the EU to combat crime and terrorism and to ensure security.

How will fundamental rights be protected when interoperability is in place?

The proposal secures a balance between the many different fundamental rights in play, for example the rights to security, the right to life, the freedom from slavery for victims of human trafficking, the right to privacy and the protection of personal data.

The proposed interoperability solutions are complementary components to existing information systems, or systems under development: they will not modify the balance already ensured by each of the existing central systems as regards their positive impact on fundamental rights.

In many respects the proposal represents a more proportionate approach – for example by allowing police officers to consult records on a hit/no hit basis – rather than requiring an application to consult a person's entire visa file.

In preparing the proposal, the Commission has involved the relevant authorities (European Data Protection Supervisor, EU Fundamental Rights Agency).

How are data security risks minimised?

The measures set out in this proposal will be put in place alongside the necessary safeguards to ensure that data, especially personal and sensitive data, is accessed appropriately, and stored securely and in line with the rules set out in the legislation for each system.

To minimise potential security breaches, the Commission is not proposing the option of complete interconnectivity of information systems where data registered in one system would automatically be

consulted by another system. Instead, the focus is on new components to facilitate searches across the individual systems while respecting existing access rights.

What will be the cost of the proposed interoperability solutions?

The Commission estimates the proposal to have an overall one-off cost of approximately €155 million to ensure systems are able to work together on a technical level, offset by annual net savings of approximately €53 million in training costs, national update and maintenance costs and efficiency savings.

The budget requested over nine years amounts to €425 million as the following items are also covered:

- €225 million for eu-LISA which is the Agency that builds, maintains and operates the central systems for border control, migration and security.
- €136 million for Member States to cover the changes to their national systems in order to use the interoperability components, and a budget for the training of the substantial end-user community.
- €49 million for Europol to cover the upgrade of their systems to the future volume of messages to be handled and the increased performance levels.
- €5 million for the European Border and Coast Guard Agency that will have to validate the initial data load of the common identity repository (CIR). This is a one-off exercise and limited to a year.
- €2 million for CEPOL to cover the preparation and delivery of training to operational staff so that interoperability is properly understood and used.
- €8 million for the Commission in order to cover its work during the implementation of the interoperability measures.

The budget for the implementation of the interoperability initiative has been included in the ISF Borders Regulation financial instrument.

What are the next steps?

The proposed Regulation will be sent to the European Parliament and the Council for discussion and adoption, in line with the normal legislative process.

Once adopted, the new Regulation will come into effect once all the necessary interinstitutional, technical and legal arrangements have been made to implement the proposals.

Which Member States are affected by the proposals? Why are there two regulations and not one?

Together, the two proposed regulations organise a single concept of interoperability between information systems that have their respective rules on access and their respective legal bases. Interoperability does not intend to change the rules on access of the different systems. The interoperability initiative has to respect the differences between the information systems in terms of legal basis – which is why it is necessary to present two separate regulations.

The provisions of the proposal will also apply to countries with different levels of participation in the different databases concerned, which are centred on those Member States within the Schengen zone. Two different regulations are also needed in order for the measures to take into account these differences and apply effectively in all these countries, and be in line with the legal rights and obligations in relation to each of the underlying systems in place in each country.

Some of the information systems that will benefit from interoperability are a development of the part of the Schengen acquis that relates to borders and visas in which Ireland and the UK do not participate. This is the case of VIS, EES and ETIAS. Other information systems that will benefit from interoperability are open to the opt-in of Ireland and the UK. This is the case of Eurodac and ECRIS-TCN.

In the case of Denmark, pursuant to a Protocol to the treaties, Denmark participates in the Schengen acquis relating to borders and visa on the basis of international law. Denmark also participates in the Dublin and Eurodac acquis on the basis of an international agreement concluded in 2006. Denmark will be able to benefit from interoperability solutions developed by the Commission's proposal.

Norway, Iceland, Switzerland and Liechtenstein are associated with the development of the Schengen acquis relating to borders and visa on the basis of international agreements that are known as Schengen association agreements. Moreover, they are associated with the development of the Dublin and Eurodac acquis on the basis of other agreements – these four countries will be able to benefit from interoperability as developed by both proposals.

Background – the way towards interoperability

In April 2016, the Commission presented a Communication on Stronger and smarter information systems for borders and security to initiate a discussion on how EU information systems can improve border management and internal security.

In June 2016, as a follow-up to the April 2016 Communication, the Commission set up a high-level expert group on information systems and interoperability in order to address legal, technical and operational challenges to achieving interoperability between central EU systems for borders and security. The high-level expert group was also asked to identify and address shortcomings and potential information gaps caused by the complexity and fragmentation of information systems.

The group's final report was published in May 2017 and set out a range of recommendations. It concluded that it is necessary and technically feasible to work towards the following three solutions for interoperability and that they can, in principle, both deliver operational gains and be established in compliance with data protection requirements:

- a European search portal;
- a shared biometric matching service; and
- a common identity repository.

Responding to the expert group's report and recommendations, the Commission set out, in the Seventh progress report towards an effective and genuine Security Union, a new approach to managing data for borders and security, where all centralised EU information systems for borders, security and migration management will be interoperable, in full respect of fundamental rights.

For More Information

Proposal for a Regulation establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)

Proposal for a Regulation establishing a framework for interoperability between EU information systems (borders and visa)

Commission Staff Working Document: Impact Assessment (part 1)

Commission Staff Working Document: Impact Assessment (part 2)

Commission Staff Working Document: Executive Summary of the Impact Assessment

12th Progress Report towards an effective and genuine Security Union

Press release: Security Union: Commission closes information gaps to better protect EU citizens

Factsheet: Security Union - Closing the information gap

Factsheet: EU Information Systems

Eurobarometer - Europeans' attitudes towards security

MEMO/17/5241

Press contacts:

Natasha BERTAUD (+32 2 296 74 56)
Tove ERNST (+32 2 298 67 64)
Kasia KOLANKO (+ 32 2 296 34 44)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email