Ref. Ares(2017)3765711 - 26/07/2017

European Commission

INCEPTION IMPACT ASSESSMENT	
TITLE OF THE INITIATIVE	Interoperability of information systems for migration and security
LEAD DG – RESPONSIBLE UNIT	HOME – B3
LIKELY TYPE OF INITIATIVE	Legislative proposal — Regulation
INDICATIVE PLANNING	December 2017

This Inception Impact Assessment aims to inform stakeholders about the Commission's work in order to allow them to provide feedback on the intended initiative and to participate effectively in future consultation activities. Stakeholders are in particular invited to provide views on the Commission's understanding of the problem and possible solutions and to make available any relevant information that they may have, including on possible impacts of the different options. The Inception Impact Assessment is provided for information purposes only and its content may change. This Inception Impact Assessment does not prejudge the final decision of the Commission on whether this initiative will be pursued or its final content.

A. Context, Problem definition and Subsidiarity Check

Context

Responding to the increase in irregular border crossings into the EU and the threat to Europe's internal security as demonstrated by terrorist attacks, the Commission presented in April 2016 a Communication *Stronger and smarter information systems for borders and security (COM(2016) 205)*, initiating a discussion on how information systems in the European Union can better enhance border management and internal security. The major existing EU systems at that time were the Schengen Information System (SIS), the Visa Information System (VIS) and Eurodac (the EU asylum fingerprint database). As follow-up, the Commission set up in June 2016 a high-level expert group on information systems and interoperability to address the legal, technical and operational challenges to achieve interoperability. The high-level expert group was tasked to develop a joint strategy to make data management in the Union more effective and efficient, in full respect of data protection requirements, to better protect its external borders and enhance its internal security. The objective was to take a broad and comprehensive perspective on border management and law enforcement, taking into account also the relevant customs authorities' roles, responsibilities and systems. The Commission's 2017 work programme signalled the intention to make law enforcement and border management systems more interoperable.

In parallel, the Commission presented in April 2016 a revised proposal for a Regulation on the establishment of an Entry/Exit System (EES) (COM(2016) 194 final). The EES aims to ensure effective management of authorised short-stays, increased automation at border controls, and improved detection of document and identity fraud.

The new generation of EU systems have been designed with interoperability in mind, but this is not the case for the major existing EU systems: SIS, VIS and Eurodac. The EES proposal would establish interoperability with the VIS. The proposal (COM(2016) 731 final) for a European Travel Information and Authorisation System (ETIAS) of November 2016 also includes a general principle that it is built on the interoperability of information systems to be consulted (for example, EES, SIS, VIS, Europol data, and Eurodac).

Following the final report and recommendations of the high-level expert group in May 2017, the Commission announced, in the Seventh progress report towards an effective and genuine Security Union (COM(2017) 261), its intention to pursue work towards creating a European search portal capable of searching in parallel all relevant EU systems in the areas of borders, security and asylum, and to develop for these systems a shared biometric matching service and a common identity repository. These recommendations are to be part of a legislative proposal on interoperability under a new approach to the management of data for borders and security. This initiative also responds to the Council's call for a comprehensive framework for law enforcement access to the various databases in the area of justice and home affairs, with a view to greater simplification, consistency, effectiveness and attention to operational needs. In addition, the European Council conclusions of June 2017 invited the Commission to prepare, as soon as possible, draft legislation enacting the recommendations made by the high-level expert group.

Problem the initiative aims to tackle

There is a need for stronger and smarter information systems for borders and security. This requires overcoming the current shortcomings in data management and improving the interoperability of existing information systems. The main shortcomings hindering information exchange were indicated in the April 2016 Communication: sub-optimal functionalities of existing information systems; gaps in the EU's architecture of data management; a complex landscape of differently governed information systems; and a fragmented architecture of data management for border control and security. The work of the high-level expert group served to evaluate the operation of existing systems, to identify where new systems might be needed to address gaps, and to analyse

options to promote interoperability of the systems. Enhancing interoperability between information systems is fundamental to addressing the above challenges, especially as regards:

i. End-users — particularly border guards, law enforcement officers, immigration officers, visa officials, customs officers (when performing law enforcement tasks) and judicial authorities — who can be faced with a lack of complete and accurate data. Also, they do not always have fast and seamless access to all information that they need to perform their tasks (whilst respecting the access rights laid down in the legal instruments).
ii. Access by law enforcement authorities to non-law enforcement information systems for prevention, investigation, detection or prosecution of criminal offences is currently subject to diverse conditions that can hinder the efficiency of these activities.
iii. Identity fraud, which presents significant risks in an area without internal border controls. Such identity fraud must be detected and combated.
iv. The ETIAS system, as proposed by the Commission in November 2016, which would aim to gather information on all those travelling visa-free to the European Union in order to carry out migration and security checks in advance. The system would be based on interoperability with EES, SIS, VIS, Eurodac and Europol data. However the original proposal did not yet contain provisions to enable this interoperability. Therefore, this has to be established.

This proposal is not part of the REFIT agenda.

Subsidiarity check (and legal basis)

The main legal basis will be Article 74, Article 77(2)(a) and (b), Article 78(2)(e), Article 79(2)(c), Article 82(1)(d), Article 85(1), Article 87(2)(a) and Article 88(2) (to be examined further) TFEU.

Freedom of movement within the EU requires that the external borders are effectively managed to ensure security. Similarly, criminals or suspects can cross internal borders and evade detection. Member States have therefore agreed to address these challenges collectively, especially by sharing information through centralised EU systems in the area of justice, security and freedom.

Key EU-level common databases are in place or in the process of being put in place. Enhanced interoperability between these databases necessarily entails EU-level action. At the heart of the proposal is the improved efficiency and use of centralised systems managed by the European Agency for the operational management of Large-Scale IT Systems in the area of freedom, security and justice (eu-LISA). By reason of the scale, effects and impact of the envisaged actions, the fundamental objectives can only be achieved at EU level.

B. Objectives and Policy options

The objective of the initiative is to respond directly to the problems identified in Section A above.

i. Ensuring that end-users, particularly border guards, law enforcement officers, immigration officials and judicial authorities have fast and seamless access to all information that they need to perform their tasks.
ii. Facilitating and streamlining access by law enforcement authorities to non-law enforcement information systems where necessary for the prevention, investigation, detection or prosecution of criminal offences.
iii. Providing a solution to detect and combat identity fraud.

The situation where European IT systems are operated independently of each other at the central level and where the links between the data in different systems are only handled at national level after a reply is received, has shown its limits. A first (baseline) policy option therefore to continue with existing arrangements unchanged (notwithstanding the forthcoming EES and ETIAS systems) would risk failing to address the gaps and the fragmentation in the EU's architecture of data management that give rise to the problems for frontline officers.

A second policy option would be to pursue complete interconnectivity of information systems where data registered in one system will automatically be consulted by another system. While this could probably address the identified objectives to a large extent, it is considered that it would lead to unnecessary processing of information that is not strictly necessary and proportionate.

A third policy option would be to design the interoperability of systems in a focused way so that the information that is specifically sought can be delivered to the end-user at the required time, whilst respecting the applicable rules on access and data protection legislation. To this end, this initiative would seek to put in place three new facilities: a European search portal; a shared biometric matching service; and a common identity repository.

A centralised European search portal would be capable of searching various central systems (in particular, SIS, VIS, possibly the Europol data and Interpol's Stolen and Lost Travel Documents database, and possibly the future (centralised) European Criminal Records Information System (ECRIS) insofar as third-country nationals are concerned and the future EES, ETIAS and the new Eurodac). The single-search facility would enable a better use of existing information systems. The key objective is to ensure that border guards, law enforcement officers, immigration, officers, visa officials, customs officers and judicial authorities have the necessary information at their disposal at the required time to better protect the external borders and enhance internal security for the benefit of all citizens. Where the end-user does have access rights for one or more systems, a query under a European search portal would immediately deliver the information. Where end-users

would not have access to certain data in these central systems, a European search portal would provide access on a 'hit/no-hit' basis indicating the presence of relevant data in underlying systems without revealing that data. (In case of sensitive data, such as data on previous criminal convictions, the data controller (owner) could instead be notified). While this first level of access on hit/no-hit basis would be granted broadly, further access to underlying information would be granted in line with the provisions and safeguards in force regarding access. A centralised European search portal would therefore support the objective to ensure provision of information on a 'hit/no-hit' basis to the end-users concerned. In addition, it would be the means to deliver interoperability in practice.

A shared biometric matching service would facilitate the identification of an individual who may be registered in different databases. Biometric data, such as fingerprints and facial images, are unique and therefore more reliable than alphanumeric data to identify a person. The shared service would enable matching of biometric data held in various separate databases (linking identities). A query of the service would thus indicate whether a record potentially matching biometric data exists in IT systems linked to the shared biometric matching service, including in a system to which the person searching does not currently have access, but which could then be requested subject to provisions in force regarding access and data quality verification.

A common identity repository would bring together alphanumeric data, such as names and dates of birth, that have been stored in the various information systems for border management and security. This would facilitate identification for the accessing officer and help to improve efficiency by avoiding duplication of data, reducing overlaps, and highlighting discrepancies in the data.

Through these three facilities, it will be simpler and faster for border guards, law enforcement officers, immigration officers, visa officials, customs officers and judicial authorities to consult the necessary and available information. This will facilitate their work and will lead to efficiency and cost savings. These innovations will also require that the quality and accuracy of the data in the different systems is ensured in order to guarantee that any action or decision taken using these new facilities is based on reliable information.

The combined use of the shared biometric matching service and the common identity repository will allow to detect multiple identities linked to same biometric data and will thereby reduce identity fraud considerably.

Access for law enforcement authorities will be improved by the flagging (hit/no-hit) functionality to be provided in the European search portal and the shared biometric matching service: this will provide a quick overview of available and potentially relevant information.

C. Preliminary Assessment of Expected Impacts

Likely economic impacts

Economic impacts will be limited to the design and operation of the new facilities. The costs will fall to the EU budget and to Member State authorities operating the systems.

Likely social impacts

The major social impact will be the enhancement of border management and increased internal security within the European Union. The new facilities will simplify and expedite the identification of individuals and will enable making cross-links to already existing, relevant information on these individuals — by authorities during border checks, for visa or asylum applicants, for police work — thereby enabling access to information that can support reliable decisions being made, whether relating to investigations of serious crime or decisions in the field of migration and asylum. The new facilities should also contribute to generate trust by ensuring that their design and use increases the security of European citizens.

Likely environmental impacts

No major environmental impacts are expected.

Likely impacts on fundamental rights

Interoperability will enhance border management and internal security. It will also provide new opportunities to offer more robust and timely protection, for example in the case of missing children, the protection of life and the physical integrity of potential victims of crime, or for the presumption of innocence of suspects through cross-checking or verification of data.

Implementing interoperability could have an impact in other areas, notably in terms of data protection. Where objectives of general interest, such as increasing public security, limit the right to the protection of personal data, full consideration will be given to providing adequate safeguards and ensuring that any measures will be strictly necessary and proportionate for achieving that objective. In particular, interoperability will need to be developed in line with the ‘data protection by design’ principle and respect the EU data protection legal framework and the Charter of Fundamental Rights.

Likely impacts on simplification and/or administrative burden

The initiative is designed to facilitate the work of border guards, law enforcement officers, immigration officers, visa officials, customs officials and judicial authorities in operating the EU centralised systems in the area of freedom, security and justice.

D. Data Collection and Better Regulation Instruments

Impact assessment

An impact assessment of the feasibility and impacts of this initiative, focusing particularly on the policy and legal aspects, including data protection aspects, will be prepared. The impact assessment will be accompanied by three separate technical studies (see next section) which will support the preparation of this initiative and inform the Commission's decision.

Data collection

Detailed background is available in the April 2016 Communication *Stronger and Smarter Information Systems for Borders and Security*, and in the final report of the high-level expert group on information systems and interoperability.

Studies are being undertaken in relation to each specific facility. The outcome of these studies will feed the impact assessment:

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

Consultation strategy

An online public consultation will be organised to seek views on the interoperability of EU information systems for borders and security. In addition to the general public, the main stakeholders addressed are practitioners in the fields of borders, law enforcement and security, as well as those active in a field of fundamental rights. The online questionnaire will be published first in English and other EU official languages will be added once translations are available. In any case, responses may be submitted in any EU official language.

It is also envisaged to hold dialogues as appropriate with Member States and Schengen associated countries, EU agencies (eu-LISA, Europol, the European Border and Coast Guard Agency, EU Fundamental Rights Agency, and European Asylum Support Office), the EU Counter-Terrorism Coordinator and the European Data Protection Supervisor and national data protection authorities. It is also intended to hold tripartite technical discussions with representatives of Parliament's LIBE Committee and the General Secretariat of the Council.

The results of the consultation activities will be summarised and published in a synopsis report.

Will an Implementation plan be established?

Under the initiative, no implementation plan as such is envisaged. Nevertheless, if it proves that guidance or training is required for Member State authorities to operate the new facilities, appropriate support will be provided.