EUROPEAN COMMISSION
DIRECTORATE-GENERAL MIGRATION and HOME AFFAIRS

HIGH-LEVEL EXPERT GROUP ON INFORMATION SYSTEMS AND INTEROPERABILITY

Scoping Paper

1. INTRODUCTION

With a view to contributing to the improvement of the European Union's data management architecture for border control and security, the European Commission has established a high-level expert group on information systems and interoperability (HLEG). The HLEG brings together high-level representatives of the European Commission, EU Member States and associated members of the Schengen area, EU agencies (eu-LISA, Frontex, EU Agency for Fundamental Rights, European Asylum Support Office and Europol), the Counter-Terrorism Coordinator, and the Council Secretariat and the European Parliament Committee on Civil Liberties, Justice and Home Affairs as observers.

Effective information exchange between Member States and agencies is of key importance for the purposes of border management and law enforcement. This was emphasised in the European Agenda on Security and in successive conclusion of the European Council and the Council.

Over the years, information needs have been addressed by developing various information systems and databases that provide border guards, police officers and other authorities with relevant information on persons, in line with their respective purposes.

Recent security challenges, including an increased terrorism threat to the EU and its Member States, have led to the need to take a fresh look at the way in which the EU's data management architecture functions. As outlined in the Commission Communication on Stronger and Smarter Information Systems for Borders and Security of 6 April 2016 (*'the Communication'*) the expert group will identify and address shortcomings, and information and knowledge gaps, caused by the complexity and fragmentation of information systems at European level or for other reasons. It will elaborate on the legal, technical and operational aspects to achieve interoperability of information systems, including the data protection implications.

This work of the expert group will be guided by the following considerations:

- Information systems should be complementary. Overlaps should be avoided, and existing overlaps should be eliminated. Gaps will be appropriately addressed.
- A modular approach should be pursued, making full use of technological developments and building on the principles of privacy by design.
- Full respect of all fundamental rights — both for EU citizens and for third country nationals should be ensured from the outset in line with the Charter of Fundamental Rights.
- Where necessary and feasible, information systems should be interconnected and/or interoperable. Simultaneous searches of systems should be facilitated.

The objective of the expert group is to contribute to an overall strategic vision on how to make the management and use of data for border management and security more effective and efficient, and to identify solutions to implement improvements.

In addition to the Communication, which provides the main basis for the work of the expert group, the group will also be guided by the roadmap on information exchange and interoperability that was endorsed by the Justice and Home Affairs Council of 10 June 2016.

2. THE CHALLENGES

Looking at the current state of play on information systems and information management, the following four main challenges can be identified:

- to improve the **implementation** and use by Member States of existing systems;
- to make **existing systems** more effective, process-oriented and user-friendly;
- to consider the development of **new systems** to address identified gaps in the present information system landscape; and
- to develop an **interoperability vision** for the next decade that reconciles process requirements with data protection safeguards.

During the course of the period June 2016 – June 2017, the expert group will explore each of these challenges.

2.1. Improve the implementation and use by Member States of existing systems

Before speaking about the shortcomings of current systems, gaps in the information landscape and the need for more interoperability, it is important to consider what some perceive as the biggest gap of all: the sometimes limited implementation and use by Member States of systems that are already at their disposal.

In its Communication, the Commission announced that it will continue to **monitor and promote the better** use of systems by Member States. The Communication calls on Member States to maximise their use of the Schengen Information System (**SIS)**, both by inserting all relevant information and by consulting the system whenever required. Member States should establish electronic connections to **Interpol's** stolen and lost travel document database (SLTD) at all their external border crossings. They should also respect their obligation to enter and consult data on stolen or lost travel documents both in SIS and in the SLTD database, at the same time.

Member States should also automate the use of advance passenger information (**API)** data for checks against SIS and the SLTD database. Member States should fully implement and use the **Prüm** framework. The Communication also calls on **Europol** to make full use of its existing access rights for consultation purposes to SIS, the Visa Information System (VIS) and Eurodac. Synergies between the Europol Information System and other systems, notably SIS, should be strengthened. Member States should also make better use of the Europol Information System, Focal Points and SIENA[1].

Questions to be addressed by the expert group:

- Feeding of systems: what are the reasons for the partial feeding of data by Member States in existing systems? Are there standing operation procedures and relevant IT tools in place to facilitate feeding into systems? What operational and legal reasons (exemptions), if any, are there for not sharing information?

- Consultation of systems: do all relevant and legitimate end-users have access to the systems when and where they need it? If yes, do they use this access as required? If not, what are the constraining factors?

[1] The Europol Secure Information Exchange Network Application.

- Data quality: can information be effectively used and compared? Are data inserted in a usable format (in the case of pictures, biometrics)? Are they semantically clear and in a usable language?

2.2. Make existing systems more effective, process-oriented and user-friendly

The Communication mentions SIS, Eurodac and VIS, as well as API, Prüm, Europol, the European Criminal Records Information System (ECRIS), the customs systems and the Interpol databases. Overall, these information systems produce useful results, and some of them perform very well, but shortcomings do exist. An example mentioned in the Communication is the fact that SIS does not contain a fingerprint-searching functionality. The Communication announces that an Automated Fingerprint Identification System (AFIS) for the SIS will be developed as a matter of utmost priority.

Since the adoption of the Communication, the Commission has also presented a proposal to revise the legal basis of Eurodac to further enhance its functionalities as regards irregular migration and return. Revised legal bases for SIS and VIS will be proposed following their recent evaluations on which reports will be issued shortly. The Commission will also assess the need to revise the legal basis for the processing of API data.

As regards the complexity and fragmentation of systems, the Communication recognises that border guards and police officers face practical difficulties in accessing multiple information systems at EU level. Simultaneous searches of systems should be facilitated, to ensure that all relevant information is available to border guards or police officers when and where this is necessary for their respective tasks, in line with appropriate access rights and in full compliance with data protection principles. To address this issue, the Communication announces that the Commission will explore, together with eu-LISA, how single search interfaces, as one of the four dimensions of interoperability (ref. paragraph 2.4 below), could be used to perform one-stop-shop simultaneous searches for all relevant systems without changing existing access rights.

Questions to be addressed by the expert group:

- What are the information needs of the main user groups (police, borders, customs, and counter-terrorism respectively)? What existing systems should they be able to access? Are these information needs restricted by legal (data protection) conditions?

- What are the experiences of Member States with single search solutions, notably where they combine searches of EU systems and national systems, or centralised and decentralised systems?

- What would be the added value of a centrally developed 'single search interface' (SSI), and what specifications would such a solution need to have? What would be the costs/benefit ratio of such a solution?

- How to ensure commonly recognised standard specifications for the exchange of information (a universally used messaging format)?

2.3. Consider the development of new systems to address perceived gaps in the present information system landscape

The Communication considers that not all the information requirements of border and police authorities are addressed by the existing systems. The establishment of passenger name recognition (PNR) and the new proposals for an Entry-Exit System (EES) for third country nationals cover two important gaps. However there are more issues to be looked at.

For **visa-exempted third-country nationals who arrive through land borders**, no information is available prior to their arrival at the Schengen external borders. (For people travelling by air, API and PNR provide relevant information). The Commission has launched a study on the necessity, technical feasibility and proportionality of establishing an EU travel information and authorisation system (ETIAS), the results of which will be available in October.

The Council's roadmap on information exchange and interoperability identifies further potential gaps that require further exploration. The travel movements of **EU citizens** and other **persons enjoying the right of free movement** are not registered. Information on EU citizens who are wanted, missing or subject to discreet or specific checks is entered in the Schengen Information System. Following the revision of the Schengen Borders Code, and notably the introduction of systematic checks of all travellers at external borders, the monitoring of this category of EU citizens will be ensured. The Council's roadmap indicates that there may be a case for creating an additional 'EES module' also for this category of person. The necessity, technical and operational feasibility and proportionality of such option shall be carefully assessed.

The Council's roadmap also notes the absence of a common database on **residence permits, residence cards and long-stay visas** issued by Member States. When holders of these documents cross the external borders, the decentralised management and absence of data exchange on these documents make it impossible for border guards to assess their validity and authenticity against a common database. Even though it is possible to establish through a biometric verification that the traveller is the legitimate bearer of a residence permit, this is not the case for residence cards and long-term visas as no common format exists. Also for this option the necessity, technical and operational feasibility and proportionality shall be assessed.

Questions to be addressed by the expert group:

- ETIAS: how to ensure that the system is feasible and effective, as well as interoperable with the future Entry-Exit System? What are the experiences of countries that already use such pre-arrival information systems?
- Registration of travel movements of EU citizens: is such a system necessary, technically and operationally feasible, proportionate? Are there alternative solutions to achieve the same objective?
- Repository of residence cards and residence permits: is such a system necessary, technically and operationally feasible, proportionate? Do national databases exist on which an EU system could be built?
- Remaining information gaps: are there any more gaps in the EU information landscape that need to be addressed through the creation of new systems?

2.4. To develop an interoperability vision for the next decade that reconciles process requirements with data protection rules

Interoperability is the ability of information systems to exchange data and to enable the sharing of information. The Communication identifies **four dimensions of interoperability**, each raising legal, technical and operational issues, including on data protection:

- a single search interface to query several information systems simultaneously and to produce combined results on one single screen;
- the interconnectivity of information systems where data registered in one system will automatically be consulted by another system;
- the establishment of a shared biometric matching service in support of various information systems; and
- a common repository of data for different information systems (core module).

The first option is already used by several Member States (ref. 2.2 above) and should be further developed and promoted as a first step. The second option has already been proposed for VIS/EES, and may be applied in relation to other systems. The third is a primarily technical issue, which follows from interconnection choices (it is planned that EES and VIS will share a common biometric matching service). It is also a technical requirement to arrive at the fourth option: the possible development of a **common repository of data**.

Such a common repository could constitute a core module that would contain the basic data (alphanumeric and biometric data). Other data elements and specific features of the different information systems (e.g. visa data) would be stored in specific modules. The core module and the specific modules would be connected with each other to link the respective data sets. This would create a **modular and integrated identity management for borders and security**. The common repository would facilitate the recognition of connections and provide an overall picture by combining individual data elements stored in different information systems. It could address the current knowledge gaps and shed light on blind spots for border guards and police officers.

Questions to be addressed by the expert group:

- In addition to VIS/EES, what other databases or systems should be interconnected?
- What would be the purpose, necessity, technical feasibility and proportionality of a common repository of data? Are there any existing national core module systems that can provide inspiration?
- What are the advantages and risks of the common repository of data from a data protection perspective?
- How could the current legal framework of the various information systems be adapted to enable the establishment of a common repository of data?
- What are the technical and operational implications of the gradual transfer towards a common repository of data?

3. EXPECTED OUTCOMES

The tasks of the expert group, as laid down in Article 2 of the Commission Decision under which it has been set up, are the following:

- *to give **advice and assist the Commission** in order to achieve interoperability and interconnection of information systems and data management for border management and security;*

- *to develop an overall **strategic vision** on the interoperability and interconnection of information systems and on a more effective and efficient data management for border management and security in the EU, including **suggestions of concrete follow-up actions** for the Commission for the short, medium and long term to better protect its external borders and enhance its internal security through enhanced information sharing;*

- *to establish **cooperation and coordination** between the Commission and Member States on questions relating to the implementation of Union legislation on the interoperability and interconnection of information systems and data management for border management and security in the EU.*

The high-level expert group has the ambition of providing a bridge between the technical expert level and the policy discussion at senior official level. It wants to clarify and elaborate the sometimes confusing technical concepts that are used in the policy debate on information systems and interoperability. It aims to create a platform for exchange of experience and knowledge between peers, which can help to overcome challenges at the national level, and contribute to a shared European vision on the way ahead. It also has the ambition to spark and nurture new ideas and initiatives.

4. ORGANISATIONAL ASPECTS

The working method of the high-level expert group will aim at synergising all relevant experiences and assessments, which in the past were too often developed and discussed in silos. The group will invite experts from all relevant backgrounds to present experiences, knowledge and insights, including from non-EU countries. The group will also seek the input of the European Data Protection Supervisor and national data protection authorities in the Article 29 Working Party.

The high-level expert group will draw on existing expertise. It will take account of relevant findings from research and previous discussions in relevant Council configurations and the European Parliament. Where necessary to complete its picture of the current situation, the group may also conduct its own analysis (e.g. through questionnaires to Member States, external studies, etc.)

The high-level expert group is chaired by Matthias Ruete, Director-General of DG HOME, and is supported by a secretariat in DG HOME.

4.1. Five HLEG meetings

In addition to the meeting of 20 June, four more meeting of the HLEG are planned. The provisional planning of these meetings is as follows:

20 September 2016 (tbc): focusing on **existing systems**, both on the aspect of implementation (item 2.1 above) and reinforcement (item 2.2).

29 November 2016 (tbc): focusing on data gaps and the need to develop **new systems** (item 2.3).

February 2017: focusing on the challenge of making systems **more interoperable** including possibly through the establishment of a common repository of data (item 2.4)

May 2017: drawing **conclusions** on each of the four items discussed.

To feed and facilitate discussions of the HLEG the Secretariat will prepare **discussion papers** and **background documents** for each of the meetings. The Chair may also invite other members of the HLEG (notably Agencies) to contribute in writing to the proceedings of the group.

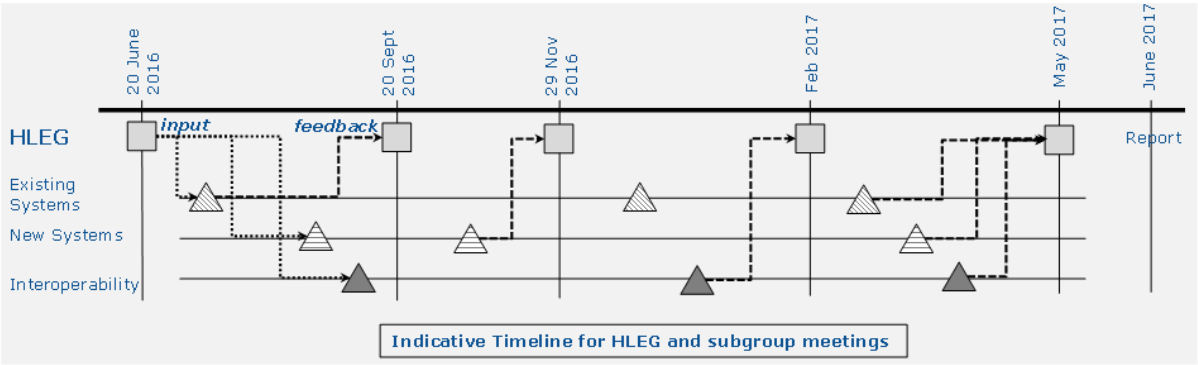
4.2. Three subgroups

It is planned to set up dedicated **subgroups** for the purpose of examining specific questions identified by the HLEG. These groups will allow for a deeper discussion in more restricted format (maximum 10 Member States experts per subgroup). Participants in these groups will be selected on the basis of proven expertise and experience.

It is envisaged to have one subgroup for each of the three major clusters discussed by the HLEG: **existing systems, new systems and interoperability**.

The subgroups will receive input from the HLEG and will report back to the HLEG.

The timing and interrelation of meetings would be as follows:



Following the last meeting of the HLEG in May 2017 the Commission will prepare a Report to the European Parliament and the Council in June 2017. The Report will present the main findings of the HLEG and propose concrete actions for follow-up.

European Commission / DG HOME
June 2016