High-level expert group on information systems and interoperability

Final report

May 2017

Legal Notice

This report is presented by the high-level expert group on information systems and interoperability. The group was set up under Commission Decision C/2016/3780 of 17 June 2016 setting up the high-level expert group on information systems and interoperability. The group comprised experts in the field of information systems and interoperability, nominated by Member States, Schengen associated countries, and EU agencies and bodies, and was coordinated by the Migration and Home Affairs Directorate-General of the European Commission.

The opinions and recommendations expressed in this document are those of the high-level expert group on information systems and interoperability and do not necessarily represent the views of the European Commission. Reproduction is authorised, provided the source (high-level expert group on information systems and interoperability) is acknowledged.

Further information

European Commission

Directorate-General for Migration and Home Affairs

Unit B.3: Information Systems for Borders and Security

B-1049 Brussels, Belgium

Email: HOME-HIGH-LEVEL-EXPERTS-GROUP@ec.europa.eu

See also the Register of Commission Expert Groups:

http://ec.europa.eu/transparency/regexpert/

Table of Contents

1. Introduction

The European Union currently faces the parallel challenges of migration management and the fight against terrorism, organised crime and cyberattacks. Threats are becoming ever more complex and transnational, so cooperation and information are becoming ever more important to ensure the safety and security of citizens across the European Union. It is essential to make full use of existing legislation and initiatives to promote information exchange among all those involved in the field of security. Joining up and strengthening the EU's border management, migration and security cooperation frameworks and information tools is vital.

As set out in the Commission's April 2016 Communication *Stronger and Smarter Information Systems for Borders and Security*[1]*,* citizens in the EU rightly expect that migration is effectively managed so that we have confidence in knowing who is entering the EU. They also expect that security for all remains a prime objective, to be achieved in part by ensuring that the EU manages its external borders and shares information effectively.

Information systems, by providing border guards, migration and asylum officials, and police officers with relevant information on persons, are essential for both external border management and internal security in the EU. The April 2016 Communication affirmed that there is room for improvement, whether in using or strengthening existing systems or developing new systems. One major path to this end would be through improving the interoperability of information systems, an objective endorsed by the European Council and the Council.

In May 2016, the Commission therefore decided to set up a high-level expert group on information systems and interoperability. It comprised experts from Member States and associated Schengen countries, and from the EU agencies eu-LISA[2], Europol[3], the European Asylum Support Office, the European Border and Coast Guard Agency (Frontex) and the EU Fundamental Rights Agency. The EU Counter-Terrorism Coordinator and the European Data Protection Supervisor also participated as full members of the expert group. In addition, representatives of the secretariat of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs and of the General Secretariat of the Council attended as observers (see Annex 1 for full list).

The EU Fundamental Rights Agency circulated to the group its draft paper *Fundamental rights and the interoperability of EU information systems: borders and security*[4]. An executive summary of the paper appears in Annex 3. In addition, the European Data Protection Supervisor and the EU Counter-Terrorism Coordinator submitted statements and these are annexed to the report.

In December 2016, the chair of the high-level expert group presented his interim findings and orientations based on the group's work over the first six

[1] COM(2016)205, 6 April 2016.

[2] European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

[3] European Union Agency for Law Enforcement Cooperation.

[4] http://fra.europa.eu/en/publication/2017/fundamental-rights-interoperability.

months of its operation. This final report now aims to present the consolidated conclusions of the expert group. As such, the report represents the views expressed by experts who were nominated in response to the Commission's invitation to Member States, associated countries, agencies and bodies. The views of these experts do not express or prejudge the official view of any of the nominating bodies in future deliberations on the subject.

1.1 The mandate of the group

As outlined in its scoping paper[5], the expert group was tasked to identify and address shortcomings and information gaps caused by the complexity and fragmentation of information systems at European level. It was given a core task of elaborating on the legal, technical and operational aspects of options to achieve interoperability of information systems, including their data protection implications.

The work of the group was 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 was to contribute to an overall strategic vision on how to make the management and use of data for both border management and security more effective and efficient, in full compliance with fundamental rights, and to identify solutions to implement improvements. In addition to the April 2016 Communication, which provided the main basis for the work of the expert group, the group was also guided by the roadmap on information exchange and interoperability that was endorsed by the Justice and Home Affairs Council of 10 June 2016.

As explained in the scoping paper, the high-level expert group had the ambition of providing a bridge between the technical expert level and the policy discussion at senior official level. It wanted to clarify and elaborate the sometimes confusing technical concepts that are used in the policy debate on information systems and interoperability. It aimed 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 had the ambition to spark and nurture new ideas and initiatives.

[5] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=24081&no=2.

Under the high-level group, three subgroups were set up to examine in detail the major issues and potential ways forward. These subgroups focused on existing systems, new systems and interoperability, respectively. Based on the discussions in the subgroups, the high-level group developed its conclusions and recommendations.

The specific tasks of the expert group, as laid down in the Commission Decision[6] under which it was set up, were 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; and*
- *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.*

1.2 The structure of this report

Fundamental rights, notably the importance of robust **data protection** safeguards, were addressed throughout all discussions in the group. It was a cross-cutting priority of high importance. The group's conclusions on this aspect are presented in Section 2 of this report.

Regarding the **existing systems**, the expert group discussed ways to improve the functioning of the Schengen Information System (SIS), Eurodac, Prüm and — to a lesser extent — the Visa Information System (VIS). It also looked into the cross-cutting priority of improving data quality and providing training, and ways to rationalise law enforcement access to systems. The findings of the group on these issues are summarised in Section 3 of this report.

For **new systems**, the expert group discussed the European Travel Information and Authorisation System (ETIAS) prior to the adoption of the proposal by the Commission, the proposed European Criminal Records Information System for third-country nationals (ECRIS-TCN), the proposed Entry/Exit System (EES), and the Directive on passenger name records (PNR). The group also looked into the question of whether the travel movements of EU citizens and other persons not covered by the EES should be recorded, and if so, in what way. The conclusions of the group on these topics are reported in Section 4.

[6] Commission Decision C(2016) 3780 of 17 June 2016, OJ C 257/3, 15.7.2016.

Most discussions were dedicated to the challenge of developing an **interoperability vision**. The group focused in particular on the benefits of parallel searches, a shared biometric matching service and a common identity repository. Interoperability with Europol data[7] and — to a lesser extent — Interpol data was also discussed, as were the potential benefits of establishing links with data contained in customs systems and the necessity of creating a single router for information exchange with carriers. Section 5 of this report presents the group's conclusions on these issues.

2. FUNDAMENTAL RIGHTS AND DATA PROTECTION

Respect for fundamental rights and data protection rules, as provided notably under the EU Charter of Fundamental Rights, was a bedrock of the work of the high-level expert group. This was clearly stated in the April Communication that gave rise to the group and it continued throughout its meetings. As already indicated, the European Data Protection Supervisor and the EU Fundamental Rights Agency participated as full expert members of the group.

Effective controls at external borders are necessary for the effective management of migration and to contribute to internal security. A proper exchange of information between Member States — the right information at the right time — is also necessary. The controls are not solely about identifying irregular migrants or terrorists or criminals. They can also serve to identify and protect persons such as victims of trafficking or abducted children. The fact that the Schengen Information System includes missing persons serves to enhance their protection. If Eurodac shows that a person is an asylum seeker, the person's data will not be shared with third countries, especially not with the country of origin.

More broadly, the right of free movement under Schengen can only be maintained with effective external border controls and full trust by Member States in the checks carried out by other Member States. Similarly, citizen and government support to receive refugees will only be maintained if strong and efficient security checks are put in place.

These and other examples demonstrate that technology and information systems for border management, migration and security can help public authorities to protect fundamental rights, for example the rights provided under Articles 1-5 of the EU Charter of Fundamental Rights. These include the right to life (Article 2) and the right to respect for one's physical and mental integrity (Article 3(1)). Moreover, Article 6 provides for everyone to have the right to liberty and security. In the group's view, this positive effect of information systems on the fundamental rights of persons is often ignored, and deserves more attention and emphasis.

Nevertheless, the processing of personal data envisaged in these systems also raises questions about their impact on the right to privacy and the protection of personal data. The group has been very sensitive to such potential privacy risks. The group has consistently noted that personal data

[7] With the entry into force of the Europol Regulation (EU) 2016/794, the reference to Europol systems, such as the Europol Information System (EIS), is no longer accurate in all circumstances. Under the Regulation, data can be submitted and processed for specific purposes, regardless of the processing systems. Therefore, where appropriate, reference is made in this document to *Europol data* in general.

should only be retained for as long as necessary for the purpose for which they were collected.

Information systems for border management, migration and security should be designed and implemented in compliance with all relevant data protection principles, and notably the requirements of necessity, proportionality, purpose limitation and quality of data. In this context, the Data Protection Directive[8] for the police and criminal justice sector will ensure that the data — of victims, witnesses, and suspects of crimes — are duly protected in the context of a criminal investigation or a law enforcement action. At the same time, harmonised laws will also facilitate cross-border cooperation of police or prosecutors to combat crime and terrorism more effectively across Europe. In addition, the General Data Protection Regulation[9] will — within its scope — enable data subjects to better control their personal data.

The group endorsed the principles of privacy by design and by default, and agreed that they should be explored and implemented to the maximum possible extent. It also argued that new thinking may be required to respect a high level of data protection while at the same time achieve interoperability and access to databases based on business needs of, notably, law enforcement authorities (see Section 3.2).

Technological developments enable new data protection concepts, especially for law enforcement purposes. Granting full access to and searching a particular system, only to realise that the system does not have information on a particular person, is not proportionate, not necessary and is rather a waste of time and effort.

New concepts based on searches would limit access to data while allowing users to take the right decisions with greater confidence, because the decisions are based on complete, reliable and up-to-date data. This is not about administrative convenience but is clearly in the public interest.

Information systems that are not (properly) used will produce no matches (or false matches), which may negatively impact the fundamental rights of individuals. Unsafe systems that can be easily hacked will bring personal data into the wrong hands, and could expose people to great risks. Appropriate security measures, adequate safeguards and effective redress mechanisms will therefore be part and parcel of any information system.

The group acknowledges that the early involvement of the European Data Protection Supervisor and the EU Fundamental Rights Agency in the design and further evolution of EU information systems is essential to ensure that EU systems fully comply with all relevant fundamental rights considerations.

[8] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (OJ L 119, 4.5.2016, p. 89).

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation (OJ L 119, 4.5.2016, p. 1).

Recommendations by the group

- The Commission should continue to fully associate the European Data Protection Supervisor and the EU Fundamental Rights Agency in the preparation of future initiatives addressing information systems in the area of justice and home affairs.
- All stakeholders should always consider all possibilities that technology offers for privacy by design solutions, both where this falls under existing legal frameworks and in future initiatives.
- For the implementation of any of the recommendations described in this report, the Commission should consider whether legislative changes may be necessary to ensure compliance with the data protection framework.

3. EXISTING SYSTEMS

Under this heading, the expert group was tasked to discuss the challenge of '*making existing systems more effective, process-oriented and user-friendly.'*

The expert group highlighted as a priority the cross-cutting issues of improving the quality of data submitted into the respective systems, and the possibilities for enhancing the efficiency of law enforcement access to systems such as Eurodac and VIS. In addition, it looked into each of the main systems separately, to explore the need and possibility of improving and strengthening the capabilities of these systems, including by improving or adding functionalities.

The group also took note of arguments that systematic consideration should be given to the possibility of associated countries being included in both existing and new systems.

This section of the report presents the main findings for existing systems.

3.1. Cross-cutting issue: data quality

Each information system used for processing data put in by human operators is prone to have data quality problems. This can have consequences not just for not being able to identify irregular migrants or terrorists, but also by affecting the fundamental rights of innocent people. Various automatic validation rules are thus implemented to prevent operators from making mistakes. Examples include checks on empty fields, checks on unallowed characters, checks on formats, checks on dates, and checks on inconsistencies.

The automated quality, format and completeness checks imposed or suggested by the (central) systems should be improved or completed. To prevent rejections on the central level, these checks then need to be implemented in an identical way at the point of input in the source systems where all end-users need to be adequately and continuously trained to use them correctly. Ahead of the suggestions set out in the chair's interim report, eu-LISA prepared a roadmap for enhancing the quality of data in EU large-scale IT systems. It was discussed in the relevant subgroups and also in the relevant Council groups and working parties. The group also considered that further analysis is required on the possible development of automated data quality control of the various data fields in SIS, VIS and Eurodac, and in any new systems, such as EES. Common data quality indicators are also required for the purpose of automated data quality control (see Figure 1).

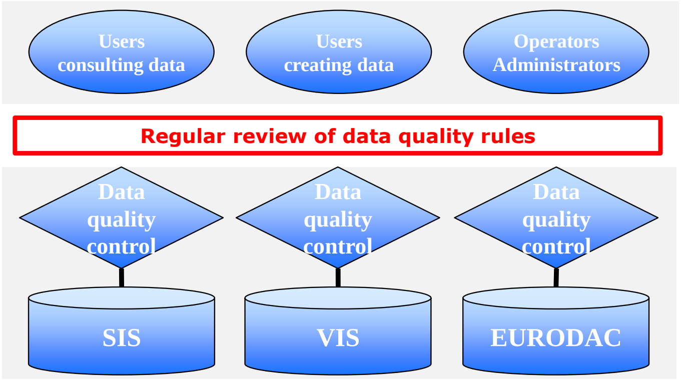

Figure 1 ***Improving data quality***[10]

In this context, a balance must be found between strict rules and end-user flexibility, while recognising the specificities of the information system and its user community. The collection of validation rules should be regularly reviewed with input by all user groups, to cope with business, organisational, technical and political changes. Member States remain responsible for the quality of their data. Therefore, the goal of such a data quality control mechanism will be for the central systems to automatically identify apparently incorrect or inconsistent data submissions so that the originating Member State is able to verify the data and carry out any necessary remedial actions. It is to be noted that, on 21 December 2016, the Commission's proposal concerning the Schengen Information System already reflected some of the discussions on data quality that took place in the high-level expert group. Similar to the approach taken in the Entry/Exit System proposal of April 2016 (listing the data allowed to be used instead of the exact reports to be generated), this SIS proposal aims to empower eu-LISA to produce data quality reports for Member States at regular intervals. This activity could be facilitated by a common data repository (see Section 3.1.1) for producing statistical and data quality reports. The same approach should be considered for the other systems — present and future — managed by eu-LISA. It can be noted that specific, dedicated data repositories have already been proposed for SIS, EES and ETIAS.

The group considered that regular training for all groups of end-users and awareness raising, peer pressure and end-user feedback should be used to remedy poor data quality. Such a lack of quality can become apparent when performing, for example, *ex post* statistical reporting and audits to monitor and improve data quality.

3.1.1 Data warehouse

A complementary tool to improving data quality would be the creation of a data warehouse containing anonymised data extracted from the systems (see Figure 2). Each data field in the current SIS, VIS, Eurodac and future EES databases would be evaluated on its intrinsic properties for further, anonymous data analysis. These properties (not the original data!) would then be copied and regularly refreshed into an analytical system. This analytical system enables the processing of these raw anonymous data and

[10] Currently, Eurodac records fingerprints only but under the current proposal this will be extended to include alphanumeric data.

subsequent statistical reporting. While many reports can be (and are) created using the actual personal data in the parent systems, this is not a best practice for several reasons:

- all data, including personal data, is directly accessed, which is not always proportionate;
- complex reports constitute an extra processing burden on the system;
- it requires dedicated and secured reporting infrastructures for each system; and
- it prevents holistic 'cross-system' analysis by only looking at data from one system.

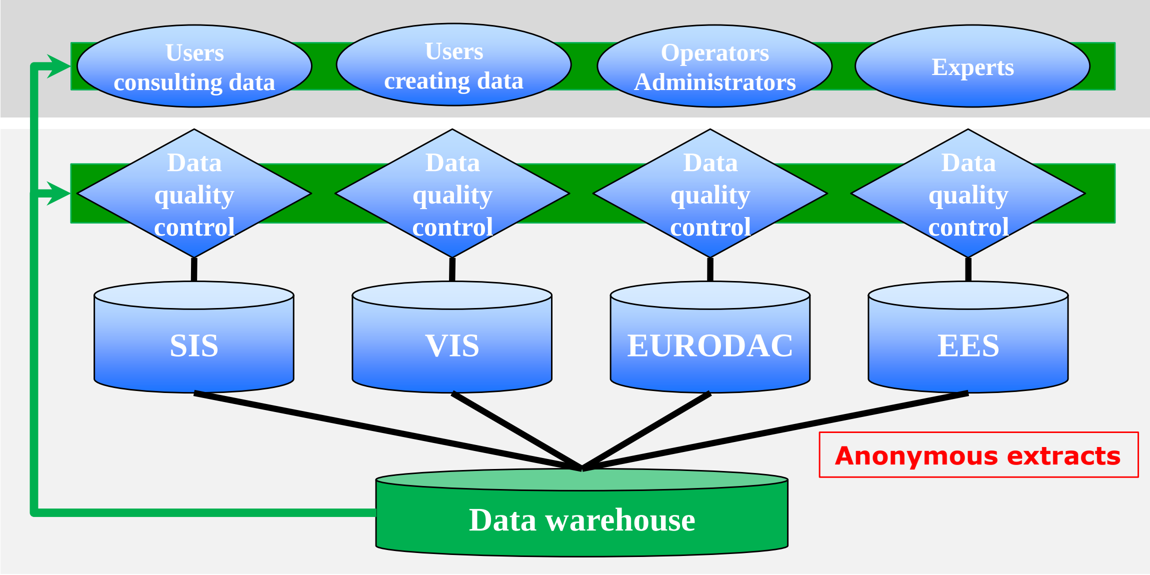

Figure 2 Data warehouse

In addition to avoiding these downsides in current practice, a data warehouse would be able to generate reports that will help Member States to make better use of the systems, including by taking informed decisions on EU policies in the area of migration and security. It would also provide valuable statistics for relevant agencies in these areas, to perform analytical reviews.

Examples include:

- the percentage of visa overstayers by country of first entry, grouped by third country;
- the percentages of nationalities that enter in a different Member State than the one indicated in the visa application; and
- the distribution of fingerprint quality by Member State, authority and parent system.

Establishing a data warehouse probably requires amendment of the legal instruments establishing the databases concerned.

Recommendations by the group

- Member States, the Commission and eu-LISA should implement as far as possible the data quality roadmap prepared by eu-LISA, focusing in particular on updated rules for scrutinising data quality and data quality reporting processes, and reinforced processes for peer reviews of data quality.

- Member States, the Commission, CEPOL[11] and eu-LISA — in cooperation with Europol and Frontex — should develop relevant training modules on data quality for staff responsible for feeding the systems at national level.

- The Commission, together with eu-LISA and its advisory groups, should work towards establishing — for all systems under the agency's operational responsibility — automated data quality control mechanisms and common data quality indicators, in addition to the system specific indicators already proposed or implemented. To this end, the accurate definition of specific metrics, indicators and tools is of utmost importance.

- The Commission, together with eu-LISA, should work towards establishing a data warehouse with anonymised data and the various examples of reporting that it would enable. This may require amendments to existing legal instruments or a new proposal.

3.2. Cross-cutting issue: law enforcement access

Access by Member State law enforcement authorities to information systems — including border management databases — can greatly contribute to the security of the EU. Access rules and procedures must be effective and efficient, whilst at the same time fully respecting the applicable data protection framework.

The two relevant existing systems (VIS and Eurodac) and the two proposed new systems currently under negotiation (EES and ETIAS) share a series of common features that aim to meet the above objective:

- *Procedure:* access requests need to be motivated and submitted in a specific case by way of an electronic form to a verifying authority (except for Europol access to VIS where no procedure is specified).

- *Conditions:* common conditions for access exist for the four systems, only the approach regarding a mandatory prior check in other databases differs.

- *Ex ante verification*: similar procedures exist for the four systems, except for Europol access to VIS where no verification or authorisation mechanism is specified.

- *Ex post verification*: possible for the four systems subject to various conditions.

- *Prior checks in other databases:* compulsory in Eurodac, EES and ETIAS but absent in VIS.

[11] European Union Agency for Law Enforcement Training.

- *Transfer of data to third countries or Member States that do not participate in the instrument:* not allowed, except in VIS under strict conditions.

Where differences between access rights and procedures exist, they result either from the specific functionalities of the system, or from the data protection *acquis* and the level of technical development at the moment of adopting the legal basis of the respective system.

Recent discussions in both the European Parliament and Council on law enforcement access to Eurodac and EES have revealed a desire to further rationalise and harmonise the applicable rules and procedures. The competent Council body, upon giving the mandate to the Presidency to start interinstitutional negotiations on the Entry/Exit System on 2 March 2017, called on the Commission to propose 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*'[12].

When discussing what such a framework should look like, the expert group considered the following:

- *Border and migration management* also serves to ensure *security* in the EU. Border checks and security checks often have the same objective, namely to identify a person. The mere fact that this person may be a suspect, perpetrator or victim of a crime should not complicate the procedure for accessing the systems. The four systems (VIS, Eurodac, EES and ETIAS) all have a direct relevance for internal security in the EU, and should therefore be readily accessible for law enforcement authorities, under well-defined conditions.

- In the context of law enforcement, a clear distinction should be made between access for identification purposes and access for investigative purposes. Law enforcement access rules should not necessarily apply in full when the systems are consulted for the purpose of identifying or confirming the identity of suspects, perpetrators or victims of a crime, (regardless of whether those persons are physically present during the check).

- The EU's new data protection legal framework sets out all applicable principles and rules. It ensures a very high level of protection of personal data. However, it does not prescribe in full detail the actual *application* of these principles and rules. This means that some of the approaches chosen so far to meet the relevant data protection principles — such as physically separate systems, cascading full access, logging of searches by law enforcement authorities — could be assessed and replaced by other approaches, provided that they meet the same level of protection as the result of a proportionality assessment between the different rights and interests[13].

[12] See Summary Record 7177/17 dated 21 March 2017 of the 2618th meeting of COREPER.

[13] See Section 2 Fundamental rights and data protection.

There was consensus in the group that the current rules for law enforcement access do not always meet operational needs. Similarly, there was general agreement to develop a single-search portal to query the relevant systems in one transaction. This would require refined rules on access and precision as to who exactly can query the systems for what purposes. Against this background, the following alternative approach could be considered.

In the group's view, law enforcement access to the systems for **identification purposes**[14] should not require prior authorisation or be subject to complicated procedures. It should be possible to consult the relevant systems in one single search on the basis of alphanumeric or biometric data. This could be accomplished by means of a two-step approach.

As a first step, a law enforcement officer would query all systems in parallel, performing, for data protection reasons, only a hit/no-hit[15] identification using the identity data of one or more specific persons. The officer would not have actual access to any data in any system. In the example below, both Eurodac and VIS seem to hold further information on the person in question. No information is available in the two other systems, and hence there is no need for further access to these systems.

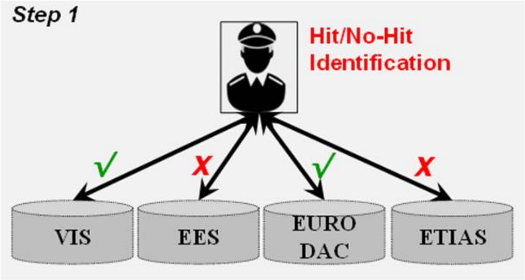

Figure 3 Hit/no-hit for identification (1)

In a second step, the officer would request full access to those information systems that generated hits, being VIS and Eurodac in this example. The officer would need to justify the need to access these systems, in line with access rights and purpose limitation principles. But knowing that both systems contain relevant data, there would be **no need for a specific sequence or cascade**. Such full access would remain subject to prior authorisation by a designated authority and would continue to require a specific user ID and logging.

[14] Identification in this context is to be understood as a search in various systems either to reveal an identity (use of biometric data) or to confirm a claimed identity (use of alphanumeric data). In both cases, the only objective is to detect the presence of data on one or more individuals. Identification of a person for non-law enforcement purposes, meaning the person is actually physically present at the time of the search, is provided for specifically in the Eurodac (Art. 17), VIS (Art. 20) and EES (Art. 25) Regulations.

[15] Hit/no-hit is fully comparable to flagging and has the same meaning for an end-user. This report makes a distinction between hit/no-hit and flagging as follows. Hit/no-hit is the result of a data-presence search in a system containing a certain category of data (i.e. SIS, VIS, EES). Flagging is the result of a data-presence search in a system combining multiple categories of data (e.g. shared biometric matching service, common identity repository).

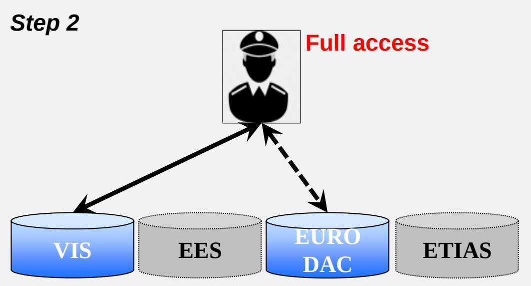

Figure 4 Hit/no-hit for identification (2)

For law enforcement access for **investigative purposes** (for example, within the context of the Entry/Exit System where the system is accessed for the purpose of reconstructing the travel history of a known suspect, perpetrator or victim of a crime) full access to one or several specific systems will be needed to obtain the specific information contained in that system (e.g. information on crossing of an external Schengen border). In this context, **a sequential cascade is irrelevant**.

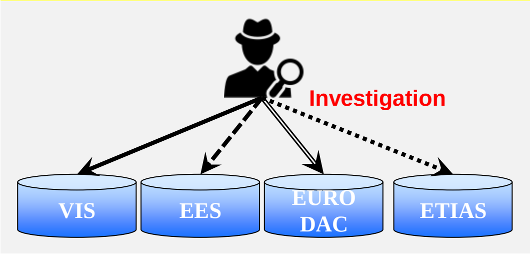

Figure 5: Law enforcement access for investigative purposes

Recommendations by the group

- The Commission should explore a new law enforcement access approach based on differentiating between: (i) identification and investigation, and (ii) normal processes and emergency situations.

- When the purpose is identification of a suspect, perpetrator or victim of a crime, the systems should be swiftly accessible without prior authorisation and in one search using, where possible, alphanumeric identity data, facial images or fingerprints. The queries should be logged and responses from the systems should in the first instance be provided on a hit/no-hit basis only.

- Only in case of actual hits should access to system data be necessary. This access should continue to require, except in emergency situations and under clearly defined conditions, *ex ante* verification and authorisation in accordance with the respective legal bases of the systems.

- Requests for investigations should continue to require, except in emergency situations and under clearly defined conditions, *ex ante* verification and authorisation. This should immediately lead to full access to all relevant systems and should not be subject to a cascade procedure.

- The co-legislators should examine, in the context of ongoing negotiations of relevant proposals, the possibility of granting direct access in emergency situations, under clearly defined conditions, as already proposed in the Eurodac proposal.

- The legal aspects of the above approach should be further assessed as a priority.

3.3. Improving the existing systems

3.3.1. Schengen Information System (SIS)

In December 2016, the Commission adopted new legislative proposals on SIS. The revised legal basis seeks, *inter alia*, to task eu-LISA with developing a data quality monitoring tool and enhanced statistical reporting. eu-LISA should also have a clearer role in testing, and in supporting SIRENE[16] Bureaux in technical activities.

Through further development and enhancement of the central and national elements of SIS, it would be expected that uninterrupted access to SIS data and strengthened data security will be guaranteed. The data held in alerts would be extended as a means to help authorised SIS users in locating and identifying people and to know more about the cases they face. The system will include new functionalities and a broadened scope (by including return decisions on irregular migrants). Moreover, the system will contain greater functionalities concerning the use of biometrical identifiers. The role of the responsible European agencies will be strengthened within their mandates, with a broadening of the access for Europol and the granting of access to the European Border and Coast Guard Agency (Frontex) and supporting teams.

Whilst the expert group has no formal role in the elaboration of legislative proposals, it did welcome these proposed improvements. The group also in particular discussed the question what role SIS can possibly play in the registration of border crossings of EU nationals and other persons enjoying free movement in the Schengen zone (see Section 4.4).

Capabilities of existing systems should where possible be maximised within existing legal frameworks. Within this category, an important improvement of SIS is the establishment of a central automated fingerprint identification system (AFIS) within SIS, which will enable the competent authorities to identify persons on the basis of their fingerprints. This would be an essential complementary measure to support increased document security and the fight against identity fraud. This AFIS project is currently carried forward by the Commission, eu-LISA and Member States. The search functionality with fingerprints will be available at central level at the beginning of 2018 and it will gradually be rolled out to all Member States in the course of 2018.

Recommendations by the group

- Member States should redouble their efforts to fully implement and use SIS in line with existing legal requirements. Where relevant, recommendations of SIS evaluation reports should be incorporated as a matter of utmost priority.

- The Commission, Member States and eu-LISA should continue to cooperate very closely to introduce technical and operational improvements of the SIS within the existing legal basis, with the AFIS functionality as their top priority.

[16] Supplementary Information Request at the National Entries.

3.3.2. Eurodac

In May 2016, the Commission proposed substantive amendments to the Dublin Regulation. It also proposed a recast of the Eurodac Regulation to ensure that the Dublin mechanism continued to have the fingerprint evidence it needed to determine the Member State responsible for examining an asylum application.

The proposed amendments to the scope of the Eurodac Regulation aim to allow Member States to also monitor secondary movements of irregular migrants who have not sought asylum, and to use that information to help facilitate re-documentation and return procedures. Negotiations on the recast Eurodac proposal have progressed quite quickly since May 2016. On the whole, the Council has broadly supported the direction of the Commission's proposal. However, in addition to the proposal, Member States requested amendments to be made to parts of the proposal that were not subject to the recast technique: specifically, to make it easier for law enforcement authorities to access Eurodac.

The group further discussed the issues raised in Council. It was argued that Eurodac should be part of an overall system environment that provides necessary information to law enforcement, asylum and migration authorities. Progress should be made on this general framework (see also Section 3.2), as well as in the particular context of Eurodac.

Recommendations by the group

- ➢ In addition to the general approach to facilitate access to systems for law enforcement authorities, the Commission should consider as a priority the technical, operational and legal feasibility of facilitating access for law enforcement, asylum and migration authorities to Eurodac.

3.3.3. Visa Information System (VIS)

The group noted that, in October 2016, the Commission adopted its report on the REFIT[17] evaluation of the Visa Information System (VIS), including its use for the purpose of law enforcement access and the use of biometrics in the visa application procedure on the basis of the Visa Code.

The evaluation report also concluded that the VIS needs to be further developed to address certain identified shortcomings (in particular on data quality but also on implementation, where the evaluation found that only one in two visas is ever checked) and to better respond to the new challenges in visa, border and migration policy. Among the measures envisaged, there were several for which support had been expressed in the group:

- where relevant, interconnectivity and interoperability with other information systems;
- the possibility of extending the VIS to contain data, including fingerprints, of applicants for long-stay visas, and residence documents (see also Section 4.5);

[17] Regulatory Fitness and Performance Programme.

- feasible options to improve access for law enforcement authorities while respecting the highest data protection standards;
- improving the quality of facial image to allow multimodal searches using biometrics, especially relevant at borders and for law enforcement purposes;
- lowering the fingerprinting age for children, to respond to concerns of human trafficking involving children and child abductions, and irregular migration involving minors;
- improving data quality in the system and facilitating the exchange of information and consultations for law enforcement purposes; and
- improving VIS capacity in terms of producing statistics and reports relevant for migratory trends and phenomena, to provide a more solid evidence basis for our policies in this area.

The group took note of information provided by the Commission, which is currently undertaking a number of studies in order to assess the feasibility of some of these developments in view of presenting a proposal for amending the VIS Regulation and the relevant aspects of the Visa Code.

Recommendations by the group

- ➢ Member States should redouble their efforts to fully use the VIS in line with existing legal requirements, in particular at external borders, in order to verify the identity of the visa holder and the authenticity of the visa. Where relevant, recommendations of VIS evaluation reports should be incorporated as a matter of utmost priority.
- ➢ The Commission, Member States and eu-LISA should continue to cooperate very closely to introduce technical and operational improvements of the VIS within the existing legal basis.

3.3.4. Prüm

Currently, some 20-22 Member States are connected to the automated exchange of DNA profiles, dactyloscopic data or vehicle registration data pursuant to the Prüm Decision. During 2016 and 2017, an increasing number of connections between Member States have been made. Some Member States are expected to connect very shortly.

The expert group explored how the operation of the Prüm Decision supports cross-border cooperation, in particular through the use of dactyloscopic data. Discussions focused on implementation issues and the need for Member States to put in place the necessary resources to make further progress in this respect, including by using Internal Security Fund — Police (ISF-P) funding through national programmes where appropriate. While there was some discussion on the governance of Prüm, there was no agreement on the way forward yet.

Among the issues suggested for consideration was the technical feasibility of an alternative connectivity via a ‘hub-and-spoke’ centralised Prüm router (or biometric single-search interface) replacing the current mesh network. This would limit the connectivity to one link per Member State while controlling, managing and reporting on the transactions centrally.

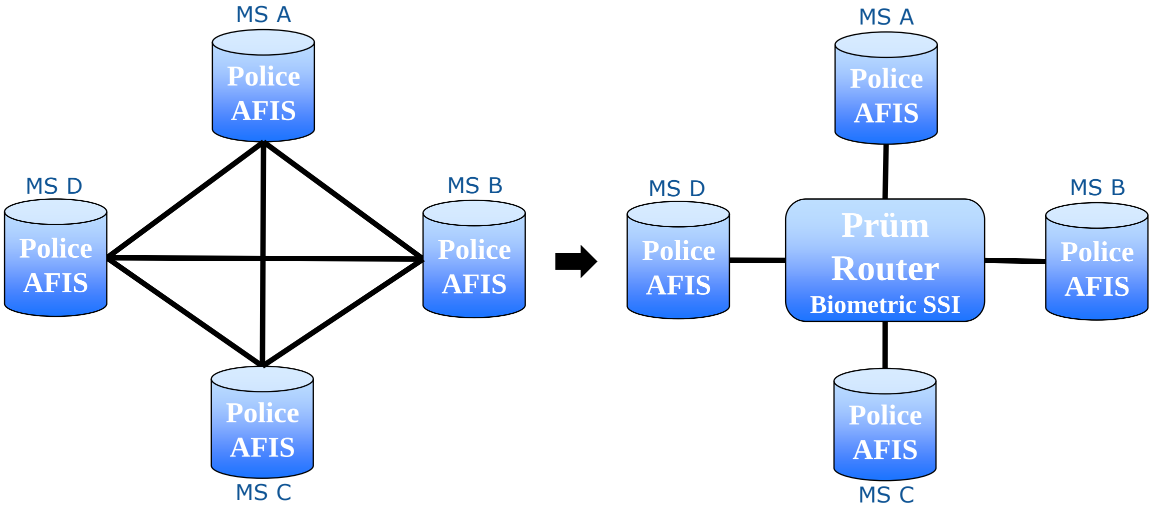

Figure 6 Migration towards a 'hub-and-spoke' centralised Prüm router

The hub-and-spoke model could provide an effective solution to overcome the connectivity challenges that Member States are faced with, notably when establishing information exchange facilities with Member States where current traffic is not very frequent. The group also had preliminary discussions on whether, once it is put in place, this model could also serve as a basis and an engine for further integration and centralisation of police cooperation under the Prüm framework.

Recommendations by the group

- Member States should fully implement and apply the Prüm Decisions without any further delay.

- While the first priority is for Member States to urgently complete their work in this area, the Commission, together with eu-LISA, should perform a feasibility study on migrating from a mesh network to a 'hub-and-spoke' connectivity via a centralised routing component. This feasibility study should also examine whether new functionalities, as appropriate, can be added.

4. NEW SYSTEMS

In addition to exploring existing systems, the expert group was also tasked to '*consider the development of new systems to address identified gaps in the present information system landscape.'*

The Communication *Stronger and Smarter Information Systems for Borders and Security* noted that while existing information systems cover a very broad spectrum of data that is required in the framework of border management, migration and security, there are also important gaps. Two of these were addressed through the presentation of legislative proposals for the establishment of an Entry/Exit System (see Section 4.1) and for a European Travel Information and Authorisation System (see Section 4.2). Two other potential gaps identified in the scoping paper were the following:

- Registration of travel movements of EU citizens: is such a system necessary, technically and operationally feasible, and proportionate? Are there alternative solutions to achieve the same objective? (See Section 4.4.)

- Repository of residence cards and residence permits: is such a system necessary, technically and operationally feasible, and proportionate? Do national databases exist on which an EU system could be built? (See Section 4.5.)

4.1. Entry/Exit System (EES)

In April 2016, the Commission proposed an Entry/Exit System (EES)[18] to register entry and exit data — and refusal of entry data — of third-country nationals crossing the external borders of the Schengen area and determining the conditions for access to the EES for law enforcement purposes.

The proposed EES Regulation envisages that the EES will be **interoperable** with the Visa Information System (VIS), to achieve border checks that are more efficient and rapid. A connection and direct access will be established between the central systems of the Entry/Exit System and the VIS (central EES accesses VIS and reciprocally VIS accesses EES). Interoperability between the two systems will avoid duplication of personal data (i.e. there will be no need to record fingerprints in the EES if fingerprints are already present in the VIS) and therefore will serve the principle of data minimisation. It will simplify the tasks of border guards and consular officers by providing, through one single operation, all the information and answers required to support their decision-making. The group very much welcomed this aspect of the proposal as a step toward tailor-made interoperability.

Negotiations with the co-legislators on the EES are currently ongoing. The final adoption of the proposals is targeted for the first half of 2017. This would allow eu-LISA to start developing the system still in 2017 in order for the Entry/Exit System to become operational in early 2020.

Recommendations by the group

- The Commission, involving eu-LISA as appropriate, should already prepare the necessary implementing acts so that they can become effective at the earliest opportunity after adoption by the co-legislators of the EES Regulation.
- eu-LISA should prioritise preparations for the development of the Entry/Exit System to be ready to start working once the co-legislators agree on the legal basis.

4.2. European Travel Information and Authorisation System (ETIAS)

In November 2016, the Commission presented a legislative proposal for a European Travel Information and Authorisation System (ETIAS).[19] All visa-exempt third-country nationals who plan to travel to the Schengen area will — prior to their trip — have to apply for travel authorisation through the system. The information gathered via the application, in full respect of fundamental rights, notably data protection, will enable advance verification of potential security or irregular migration risks.

[18] COM(2016) 194 final, 6.4.2016.
[19] COM(2016) 731 final, 16.11.2016.

Under the proposal, eu-LISA would host the system and be responsible for the technical management of the central system and the National Uniform Interfaces. Frontex would be responsible for setting up and operating the ETIAS Central Unit and for automated processing of applications. Europol will in particular be responsible for the establishment of the ETIAS watch list.

In line with the interoperability strategy proposed in the April Communication, the ETIAS proposal is designed to be **interoperable** with existing systems, and systems currently planned. The ETIAS system will also, where possible, reuse the hardware and software components of the EES, and its communication infrastructure, with a view to simplifying development and to reduce costs. Interoperability will also be established with the information systems to be consulted by ETIAS, such as the Visa Information System (VIS), Europol data, the Schengen Information System (SIS), Eurodac and the European Criminal Records Information System for third-country nationals (ECRIS-TCN). ETIAS will also be connected to Interpol's databases for Stolen and Lost Travel Documents (SLTD) and for Travel Documents Associated with Notices (TDAWN).

The group discussed ETIAS even before the Commission submitted its proposal. The group noted that, in several aspects, ETIAS already incorporates the new vision of interoperability, in particular for the purposes of border management, migration and security.

The proposal is currently before the European Parliament and the Council in view of starting negotiations in the third quarter of 2017. Once adopted, ETIAS will be developed by eu-LISA, in parallel with the EES. Provided the legal base is in place by the end of 2017, the system is planned to come into operation in 2021.

Recommendations by the group

- Once the ongoing legislative process is sufficiently advanced, the Commission should begin to prepare the implementing and delegated acts that are envisaged.

- eu-LISA, Europol and Frontex should make preparations for the development of the ETIAS System to be ready to start working once the co-legislators agree on the legal basis.

4.3. European Criminal Records Information System for third-country nationals

In January 2016, the Commission put forward a proposal[20] to extend the ECRIS system for the exchange of criminal records information to include information on convicted third-country nationals and stateless persons. Since then, discussions have demonstrated that the Council has a clear preference for creating a **centralised** reference database for this purpose. For such a centralised database to be created, a further legislative proposal from the Commission is needed. In the preparations for such a proposal, all relevant interoperability challenges, including in relation to ETIAS, are being considered.

[20] COM(2016) 7 final, 19.1.2016.

An expert meeting was organised in January 2017 to discuss with the ECRIS community how the work of the high-level expert group can best be reflected with respect to ECRIS. The main issues discussed included:

- whether or not actual conviction information should be stored at central level in order to make it available for security and border control purposes;
- whether a central ECRIS-TCN database would be suitable for use in a European search portal; and
- how the use of criminal records information for ETIAS decisions can be best ensured.

The results of the ECRIS expert meeting have been considered by the high-level expert group. There was a clear interest on future-proofing the system so that it does not create obstacles to interoperability initiatives in the future. One issue for specific consideration in this context is whether ECRIS-TCN should be part of a future shared biometric matching service.

Recommendations by the group

- ➢ In its upcoming legislative proposal, the Commission, in close cooperation with eu-LISA, should ensure that the ECRIS-TCN system could make use of a future shared biometric matching service and, if appropriate, common identity repository.
- ➢ In its upcoming legislative proposal, the Commission should ensure that relevant data under the ECRIS-TCN system can be used in the context of assessing travel authorisation requests of third-country nationals.

4.4. Registration of border crossings of EU citizens and other persons not covered by the Entry/Exit System

In response also to political appeals made by some Member States, the expert group looked into the question whether it is possible, necessary and proportionate to register the crossings at external Schengen borders by EU citizens and other persons enjoying the right of free movement.

4.4.1 Systematic registration

The starting point for considering such an initiative would be the recent amendment of the Schengen Borders Code. This introduces the obligation for Member States to **systematically check** against relevant databases all persons enjoying the right of free movement under Union law (hereafter referred to as 'EU citizens') upon leaving and entering the Schengen area. In practice the 'relevant databases' refer currently to the Schengen Information System and the Interpol databases for Stolen and Lost Travel Documents (SLTD), and Travel Documents Associated with Notices (TDAWN).

Building on this new provision, a next step could be to make it obligatory for Member States to keep track of the fact that the check has been made, by **recording its time and place**. This information would make it possible for designated law enforcement authorities to reconstruct the travel history of persons of interest, including EU citizens, for the purpose of preventing, detecting and investigating acts of terrorism and other serious crime, under strictly defined conditions.

As regards the question of **how** such information could be recorded, the group considered two potential options:

- Option 1 would be based on an extension of the use of **SIS**-logs. Today, the SIS legal basis requires for data protection reasons that all data processing transactions be logged. Member States are required to log all transactions of data processing to be able to verify the lawfulness of this processing. It could be considered to also use these logs for law enforcement purposes.
- Option 2 would be to create a **separate repository** for registering external border crossings of EU citizens. When the travel/identity document of an EU citizen is read at entry or exit, the biographical information, the time and place, and the direction of the border crossing would be recorded and stored in a dedicated new database.

In both scenarios, the procedure would need to be light and fast. Biometrics should not be captured, and the duration of stay or leave should neither be checked nor computed. There would only be the recording of the identity and of the border crossing event at the same time as the person is checked against SIS. The traveller would not experience a difference compared with the situation without registering this information.

The consensus of the group was that Option 2 would be the favoured option to examine as a priority.

A possible third option — extending the Entry/Exit System to include EU citizens — was discussed but discarded. EES is a border and migration management system designed to ensure that third-country nationals visiting the Schengen area respect the rules of short-term stay, and do not become an overstayer. This purpose is, by definition, not relevant for EU citizens. The reason for also recording EU citizens in the EES would therefore not follow from the main purpose of the system, but only from its ancillary objectives in the area of law enforcement. The legal basis of the EES does not lend itself to such a far-reaching operational extension of the system.

Recommendations by the group

- ➢ The Commission and other stakeholders should, further discuss and explore the proportionality and feasibility of a systematic recording of border crossings of all EU citizens, using Option 2 as a basis.

4.4.2 Targeted registration of persons subject of a SIS alert

Alongside the options that would entail the registration of external border crossings of all EU citizens (see Section 4.4.1), the expert group also looked into the less intrusive possibility of narrowing down this registration to those persons who are believed to be involved in terrorism or other forms of serious crime. Today, persons who are considered as a threat to public and national security or are subject of an ongoing investigation should be the subject of a SIS alert and may be entered into SIS for a discreet or specific check. Currently, if such a person is checked, the hit information is shared with the Member State that issued the alert, by using a specific hit reporting form.

To achieve a 'targeted' registration of travel movements of individuals that are recorded in SIS and to enable the investigative use of this information across the EU, two options are possible:

- the **recording of time and place of achieved hits** on discreet and specific check alerts in the SIS central system; and
- the creation of a shared **repository of SIS-hit reporting forms**, which would allow all Member States to access hit forms that the owner of the alert agreed to exchange, on persons of particular interest to that country.

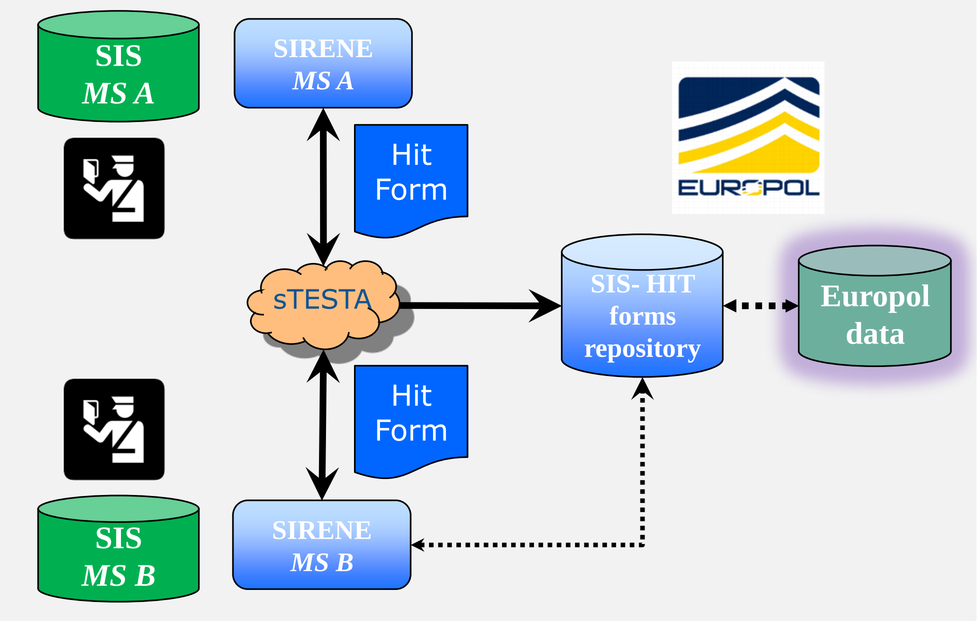

Figure 7 Repository of SIS-hit reporting forms

Moreover, should this central hit form repository be accessible by Europol, it would represent a substantial added value as Europol would be in the position to cross-check the information contained in the forms with its own databases and carry out further analysis. Moreover, it would allow Europol to form a complete picture about the movement of terrorist suspects and examine, for example, the preferred border crossings and meeting points throughout Europe and any change in their *modus operandi*.

Recommendations by the group

➢ The Commission, together with eu-LISA and Member States, should work towards both the targeted registration of achieved SIS hits and the improved availability of supplementary information contained in SIS forms.

4.5 Repository of long-stay visas, residence permits and cards, and local border traffic permits

Another information gap at EU level concerns the documents — whose issuance falls under the competence of Member States — that allow third-country nationals to stay for a longer period of time in the Schengen area: long-stay visas, residence permits and residence cards. In addition, local border traffic permits may present another information gap. A centralised repository could address the existing information gap on these categories of third-country nationals.

The essential issue to address is that today Member States have little means to check the validity of the above documents in the case where they are issued by another Member State. Each Member State only keeps a record of the long-stay visas, residence cards, residence permits or local border traffic permits that it issues itself. The authenticity and validity of these documents cannot be verified through a centralised system, even though the document gives its holder right of access and stay that go beyond the issuing Member State.

From a border control point of view, the authenticity of the document in combination with the identity of the holder cannot always be ascertained, and the validity of the documents cannot be checked. While short-stay visas are issued by one Schengen Member State but are valid for the whole Schengen area, **long-stay visas, residence permits and residence cards** authorise residence only in the Member State that issued them, but at the same time also gives the right to stay and free movement for the entire Schengen territory for up to 90 days in any 180-day period. As an example, in general,[21] a residence permit issued to a third-country national in Member State A does not allow that same third-country national to reside in Member State B; the residence permit holder can, however, travel to Member State B and stay for up to 90 days in any 180-day period. This same third-country national can also enter the Schengen area via any external border (so this could be via Member State A or B or any other) with his/her residence permit.

Apart from the border control point of view, there are also considerations of facilitation of border crossing and migration control that could be addressed when setting up such a repository. In the case of residence cards, there are also a series of rights and safeguards[22] attributed to residence card holders that facilitate the crossing of EU borders.

Although not a document for long stay or residence, the **local border traffic permit** also gives specific privileges to its holder. This permit and the conditions to be fulfilled in Local Border Traffic Agreements are defined in Regulation (EC) No 1931/2006, which constitutes a deviation from the Schengen Borders Code. The local border traffic regime simplifies border crossing, and allows the local border traffic permit holder to travel up to 30 km (in some cases 50 km) within the neighbouring Schengen country and stay in that area up to a maximum of 90 days. Storing these permits in a common repository could facilitate the control of their validity and reduce the risk of fraud and counterfeiting.

The idea of this repository was discussed in the subgroup on new systems. The conclusion was that there were a number of similarities (in terms of desired functionality, purpose and uses) with the VIS and hence that the VIS could potentially be developed further to address the needs mentioned. In this respect, the Commission's report on the VIS evaluation[23] suggests the

[21] This is the general rule but Directive 2014/66/EU and Directive (EU) 2016/801 allow mobility to a second Member State on the basis of the residence permit issued in the first Member State for longer periods.

[22] In particular, reference is made here to the 'Free Movement' Directive 2004/38/EC.

[23] COM(2016) 655 final.

extension of the VIS to include long-stay visas under one of the recommendations for further development of the system. This possibility was further discussed between the Commission and Member States as part of the consultations on possible future legal developments of the VIS, and was met with considerable support.

Recommendations by the group

- The Commission should, as a matter of priority, undertake a feasibility study for the establishment of a central EU repository containing information on long-stay visas, residence cards, and residence permits.
- The Commission should consider whether it is appropriate to include local border traffic permits in such a repository.

5. INTEROPERABILITY

The core task of the group was to address the legal, technical and operational aspects of various options to achieve interoperability of information systems. For the interoperability of systems, the expert group was tasked with '*developing an interoperability vision for the next decade that reconciles process requirements with data protection safeguards.'*

The Communication *Stronger and Smarter Information Systems for Borders and Security* defines 'interoperability' as the ability of information systems to exchange data and to enable the sharing of information. It distinguished four dimensions of interoperability, each raising technical, operational and legal 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.

The expert group has discussed each of these dimensions of interoperability in considerable detail. An important finding was that the second option (interconnectivity of systems) should only be considered on a case-by-case basis, while evaluating if certain data from one system needs to be systematically and automatically reused to be entered into another system.

Consider the example with two systems, A and B, that can be consulted via a single-search interface. The interconnectivity of system B with system A only makes sense if system A systematically and automatically needs to store and process data from system B. If no data reuse is necessary or if such reuse requires a human (legal) decision, the interconnection is without interest: the single-search interface is a better and sufficient option.

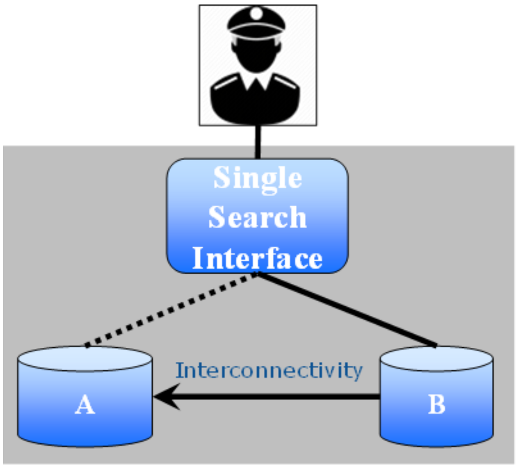

Figure 8 Single-search interface vs. interconnectivity

One real example is the interconnection of the proposed Entry/Exit System (EES) and the Visa Information System — as proposed in the draft EES Regulation — where data contained in VIS would be systematically and automatically consulted by the EES in order to store a very small subset of VIS data (visa sticker, number of entries, period of stay). This would enable the EES to process data on visa holders correctly while at the same time meeting the requirements of data minimisation and data consistency. The group considered that — provided sufficient progress is made on the other three dimensions of interoperability — there is less need for interconnectivity between systems for the sole reason of improving and facilitating access to and exchange of data.

The group therefore focused its discussions and reflections on the three remaining dimensions of interoperability: the single-search interface, the shared biometric matching service and the common identity repository. If these systems are developed, there will be value in undertaking a comprehensive technical review of the whole data architecture in the area of justice and home affairs.

5.1. Establishing a single-search functionality

The Commission issued a questionnaire on the use by Member States of single-search interface (SSI) solutions. A main finding was that all Member States use an SSI of some kind. Following discussion in the group, it was concluded that the development of a standardised national SSI is unnecessary and impractical.

However, the development of a **centralised** SSI or **European search portal** was considered promising. It would be capable of searching various central systems (SIS, VIS, possibly the Europol data, Interpol's Stolen and Lost Travel Documents database, 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) (see Figure 9). An assessment of such a European search portal would be undertaken, but it would be expected to require relatively minor technical changes on the national side.

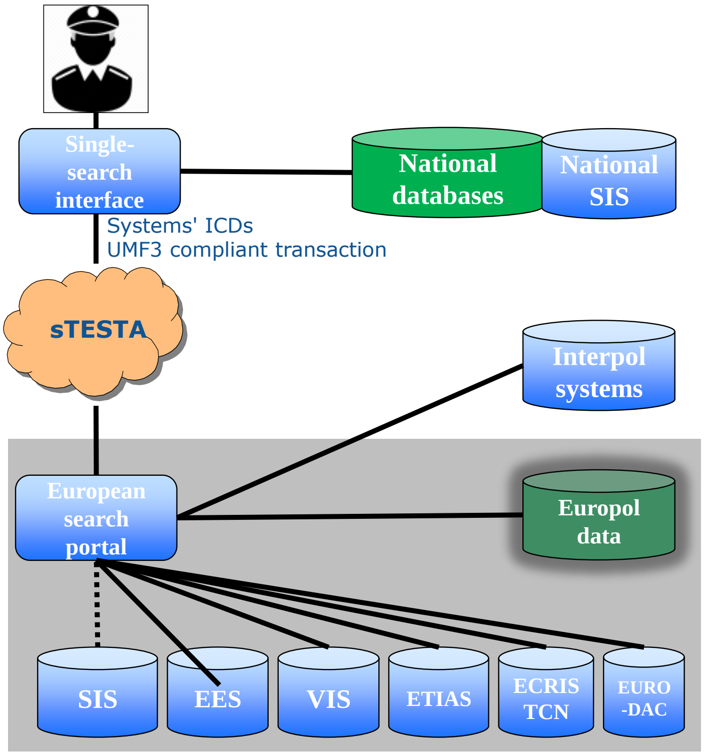

Figure 9 Conceptual view of a European search portal

A European search portal would not connect to national databases. Existing national SSI solutions would remain necessary for that purpose. These national SSIs (or in the future, potentially the National Uniform Interface of EES and further systems) would, however, be connected to the European portal for the querying of relevant EU systems in line with existing rules on access and use of the data. Also, the approach on law enforcement access for identification purposes to border and migration management systems (see Section 3.2) would require the development of a single-search interface giving access to the systems on a hit/no-hit basis.

The potential practical and operational challenges for Member States and relevant agencies to fully exploit the benefits of such a centralised SSI would need to be further explored. The expert group considered that Europol efforts to incorporate queries to its information systems via its web service QUEST (Querying Europol Systems) in national SSIs (including through a pilot project) are promising and should be supported: it is expected to go live in the first half of 2017. Looking to the future, the introduction of QUEST also anticipates the eventual linkage of the Europol data to a European search portal.

The possibility to search the Interpol systems (Stolen and Lost Travel Documents (SLTD) and Travel Documents Associated with Notices (TDAWN)) via a European search portal would greatly facilitate access to this international data (not all of which is available in European systems) in particular for consular affairs and asylum/migration entities.

The status of Interpol as an international organisation and the fact that these Interpol systems are (also) being fed by non-European countries will require a specific focus on data protection and other relevant fundamental rights issues.

The group concluded that creating a European search portal was necessary to address the needs of border management and law enforcement, and that it is technically feasible and, in principle, possible to do in full compliance with data protection requirements. However, further technical analysis is needed on how to implement a European search portal in practice, taking data protection aspects into account, and to analyse a possible integration of the National Uniform Interface of the EES into the concept.

Recommendations by the group

- The Commission and eu-LISA should work towards creating a European search portal capable of searching in parallel all relevant EU systems in the areas of borders, security and asylum. This should include an analysis (to be made together with Europol) of whether Europol data could be accessed through the European search portal and, if so, under what conditions.
- The Commission and eu-LISA should explore (in consultation with Interpol) whether Interpol databases could be accessed through a European search portal and, if so, under what conditions, taking into account the specific data protection implications of accessing Interpol systems.
- While respecting that Member States remain responsible for the management of user identities, the Commission, together with eu-LISA, should explore the possibility for specifying the parameters for users to access the systems through the European search portal (and shared biometric matching service) via implementation of user-group management at central level.
- The Commission should explore, together with the European Data Protection Supervisor and the EU Fundamental Rights Agency, the data-protection implications of the establishment of a European search portal, in particular for law enforcement access.

5.2. Building a shared biometric matching service

The legal instruments of SIS, VIS, Eurodac and the proposed Entry/Exit System do not prescribe the technical implementation details of the infrastructure that performs the fingerprint identification functions. Instead of a dedicated automated fingerprint identification system (AFIS) for each individual system, a shared biometric matching service could be implemented (see Figure 10). Whereas the former is only capable of matching fingerprints, the biometric matching service would be able to process both fingerprints and facial images. And rather than serving just one system, the shared biometric matching service would perform identifications and verifications for all the centralised systems (SIS, VIS, Eurodac, the proposed EES and the proposed ECRIS-TCN, and possibly the Europol data). This would not necessarily require any changes to the legal instruments as each parent system will by default only search within its own data, in line with existing rules on access and use of the data. Personal data protection rules enshrined in the legal bases of the systems will be respected by compartmentalising the data, with separate access control rules for each category of data.

A shared biometric matching service has a number of potential advantages:

- easier, better, more secure and cheaper operations and maintenance of one single biometric system (which are generally very complex systems) from one provider;

- cheaper to procure/implement one system instead of several separate systems; and

- the prospects of better data protection.

Recommendations by the group

➢ eu-LISA should analyse the technical and operational aspects of the possible implementation of a shared biometric matching service. Together with Europol, it should also be analysed how such a shared biometric matching service could also match biometric data from the Europol data.

➢ The Commission, together with eu-LISA and the Prüm stakeholders, should explore options for supporting the Prüm exchange and conduct a feasibility study into options for hosting national data from automated fingerprint identification systems in a shared biometric matching service on a voluntary basis.

5.2.1 Flagging

In addition to these economies of scale, a shared biometric matching service would also open the possibility for a very important innovation: it would enable single searches with biometric data. A person who is the subject of a check can be registered in several systems simultaneously — potentially under different identities — given the specific purpose of each system. Public authorities should be able to obtain reliable and up-to-date information about the status of such persons on the basis of possible matches from all relevant EU systems.

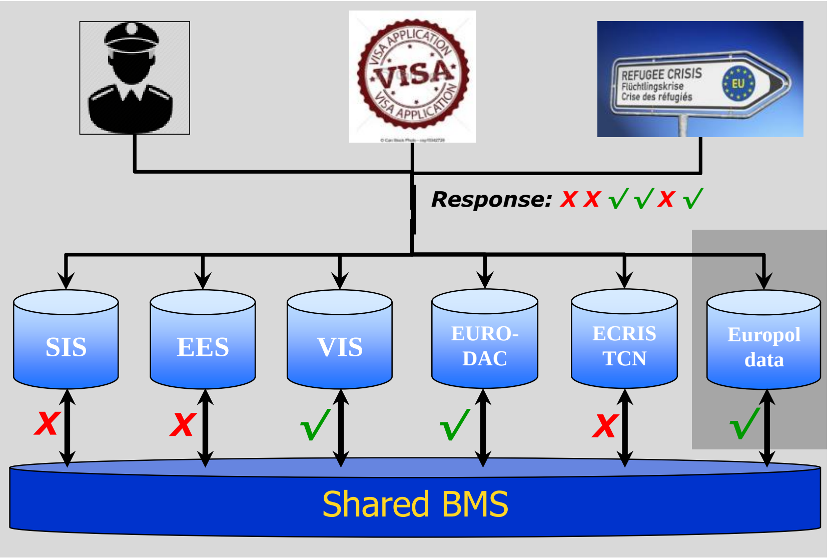

Figure 10 Shared biometric matching service (BMS) with 'hit flags'

While various scenarios can be envisaged, the group considered that the most solid in terms of data protection safeguards is based on hit/no-hit 'flags'. The shared biometric matching service would match biometric data from various 'parent systems' such as the proposed Entry/Exit System, SIS, VIS and Eurodac. At the same time, it could be designed in such a way as to respect the original data access control of the parent system and the need to comply with data protection principles and the requirements of necessity, proportionality, purpose and access limitation and quality of data. These aspects should be further explored with the European Data Protection Supervisor and the EU Fundamental Rights Agency. The shared biometric matching service could be designed in such a way that the specific search transaction from a parent system (a fingerprint search from Eurodac for example) would not only contain the specific data of that system (the asylum seeker's identity in the case of Eurodac) but in addition a flag indicating possible data from other systems.

These hit/no-hit flags would not contain any specific data. They merely indicate the possibility of finding specific data, on the person in question, in another system.

Reporting this flag to indicate the presence of data in other systems would require changes to the legal instruments of all systems for which such a flag is requested.

In addition to matching biometric data from EU systems, the shared biometric matching service could also host specified national data, thus potentially relieving Member States of having to operate and maintain complex and expensive biometric systems. This centralised hosting of national data could also be interesting for the Prüm exchange by providing a centralisation of searches and an improvement in performance.

The group concluded that creating a shared biometric matching service was necessary to address the needs of border management and law enforcement, technically feasible and, in principle, possible to do in full compliance with data protection requirements. However, there are further technical and operational aspects of establishing a shared biometric matching service that need to be addressed, including as regards the data protection implications.

Recommendations by the group

- The Commission and eu-LISA should explore the technical and legal aspects of utilising the future shared biometric matching service for the purpose of flagging the existence of biometric data from other systems.
- The Commission should explore, together with the European Data Protection Supervisor and the EU Fundamental Rights Agency, the data-protection implications of the flagging functionalities of a shared biometric matching service, in particular for law enforcement access.

5.3. Towards a common identity repository

The establishment of the shared biometric matching service would bring immediate advantages on its own. It should be complemented by the development of a common repository of alphanumeric identity data that would allow a complete view of all claimed biographic identities used by a person.

Starting with the biometric attributes of an identity, a further step could be to aggregate the common biographical attributes (such as name, date of birth, gender) from the various existing systems to a common identity repository (see Figure 11) which would:

- enable detecting and preventing identity fraud;
- improve data quality by detecting discrepancies in identity;
- enable limiting the access to personal details, other than the identity; and
- facilitate law enforcement searches using data-presence flags.

Establishing such a common repository would overcome the current fragmentation in the EU's architecture of data management for border control and security and the related risk of blind spots. This fragmentation results in the same data being stored several times. A common identity repository for all systems would help to avoid duplication and overlaps of data.

The identity records in the common repository would be linked to specific data that remain in the system that actually 'owns' this identity record. All established and future rules and limitations on access control are obviously also applicable to the records in the common identity repository.

The common identity repository and the shared biometric matching service would enable single identifications using biographical and/or biometric data, based on a hit/no-hit concept, in line with existing rules on access and use of the data. This could significantly facilitate the work of law enforcement entities while limiting unnecessary access to sensitive data.

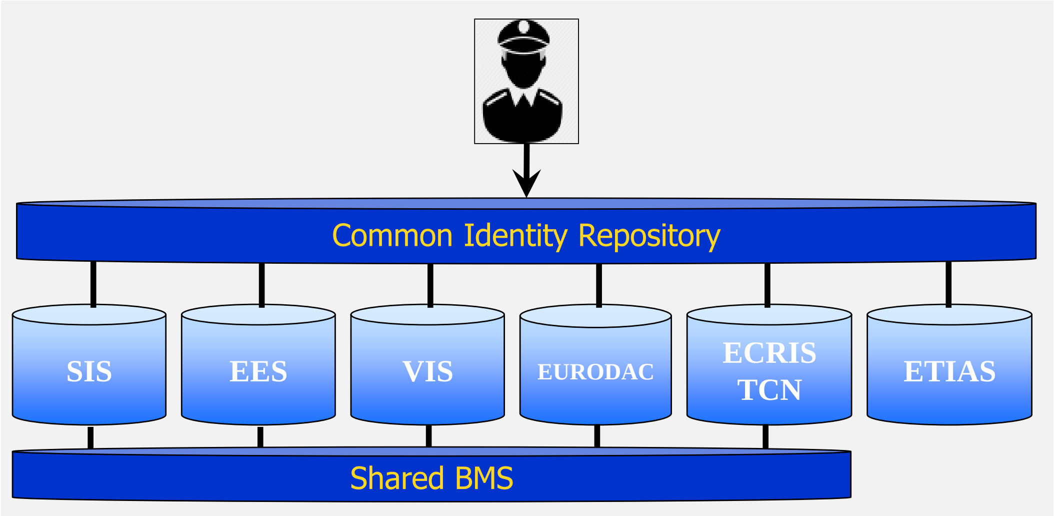

Figure 11 Conceptual view of a common identity repository

The Commission's legislative proposal for the establishment of the European Travel Information and Authorisation System (ETIAS) envisages already to put this concept into practice: *'ETIAS and EES would share a common repository of personal data of third-country nationals, with additional data from the ETIAS application (e.g. residence information, answers to background questions, IP address) and the EES entry-exit records separately stored, but linked to this shared and single identification file'*[24].

Building on the envisaged common EES/ETIAS repository, and assuming that a shared biometric matching service will be established, it would be an

[24] COM(2016) 731 final, 16.11.2016 (page 15).

additional step to also transfer biographical data of other central systems (SIS, VIS, Eurodac) into such a repository.

To avoid duplication of data, to facilitate further efficiency and to respect all data-protection safeguards, an identity repository:

- would be based on the use of read-only views[25];
- would provide aggregated views of identity data from all systems;
- would respect original data ownership of Member States and end-user access rights (certain data will be visible, other data will not be visible at all); and
- would enable flagging the existence of certain data via a hit/no-hit result, without showing the actual data

The group concluded that creating a common identity repository was necessary to address the needs of border management and law enforcement, and that it was technically feasible and, in principle, possible to do in full compliance with data protection requirements. However, further legal and technical analysis is needed on how to implement a common identity repository in practice, including as regards the data protection implications.

The inclusion of identity data from the Europol data might prove to be too complex, given the differences in end-users and different access-control and sensitivity markers. This particular situation would be remedied through the use of the European search portal, searching the Europol data using the same identity data used to search the identity repository.

Recommendations by the group

- ➢ The Commission, in cooperation with eu-LISA and Europol, should work towards establishing a common identity repository.

- ➢ The Commission should explore, together with the European Data Protection Supervisor and the EU Fundamental Rights Agency, the data-protection implications of the establishment of a common identity repository, in particular for law enforcement access.

5.4. Cross-cutting issue: promoting the use of the Universal Message Format (UMF)

Each information system uses a specific data model to organise and store the various properties of data processed. The specific interface or message format — often described in an interface control document — used to interact with the information system is closely linked to this data model and each interface will thus be different and continue to exist.

The Universal Message Format (UMF) is one step towards creating a universal standard at national and EU level that can be used to orchestrate interactions between multiple systems in an interoperable way.

[25] A view is an up-to-date snapshot of some of the original data. It neither copies nor allows modification of data. It is a perfect reflection of the original data. A view is like a pair of glasses, one can see different things depending on the type of lens.

The group concluded that the further promotion and use of UMF offers important benefits. The group noted that UMF facilitates the use of single-search interfaces but for existing information systems some form of 'translation' or reformatting will always be necessary.

Recommendations by the group

- The Commission, together with eu-LISA, Member States, Europol and Interpol, should consider ways to establish a UMF governance at EU level, enabling a structured decision-making process and change management mechanism. Such governance would ensure that the development of UMF is fully reflected in all existing and future EU large-scale systems and would facilitate the continuous interaction between the operational and the technical level.
- At the technical level, eu-LISA should invest in the creation of 'translators' between UMF and SIS/VIS interface control documents, focusing first on persons and documents. The possibility to incorporate these capabilities into the future National Uniform Interface could also be explored.

5.5. Interoperability with Europol and Interpol

5.5.1 Europol

The new Europol Regulation (EU) 2016/794, applicable as from 1 May 2017, fully equips Europol with the means to strengthen its role as the EU criminal information hub, by paving the way to integrated data management. The scope of access to Europol data for end-users will be defined by the purpose(s) (identification of links; thematic and strategic analysis; and operational analysis) instead of by the system. This will increase efficiency and rapidity of data processing.

The EU has already made substantial steps towards granting Europol wider access to relevant EU databases, including the future Entry/Exit System.

Europol has already the right to access and search directly data entered into the Schengen Information System (SIS) for arrests, for discreet and specific checks and for objects for seizure. So far, Europol has carried out a relatively limited number of searches in SIS. The recently installed capability to launch batch searches facilitates more structured cross-checking of relevant Europol data against the SIS.

The revised SIS proposals extend Europol's access to include all relevant alert categories. Also, the SIS-AFIS that is currently being developed (see Section 3.3.1) will be accessible by Europol under the conditions set down in the current SIS regulation. Still in SIS, it is being discussed to establish a hit-reporting forms repository, which should preferably be accessible for Europol (see Section 4.4.2). In the short-term in any case, Member States should systematically share the SIS hit reporting forms with Europol's analysis project *Travellers*.

Access for Europol to VIS and Eurodac for consultation purposes has been legally possible since 2013 and 2015 respectively, but has so far not been achieved. Europol should accelerate the ongoing work to establish the connection to VIS and Eurodac.

The proposal on ETIAS provides for an important role for Europol in closing the gap in security checks on visa-free travellers: the systematic checking against Europol data, including a dedicated ETIAS watch list; the involvement of Europol in the follow-up of any hits against its data; and allowing Europol to consult the ETIAS database. In particular, this allows Europol to bridge joint efforts in border protection with those for the prevention and combating of serious organised crime and terrorism. As the EU criminal information hub, it can add value in this respect, interconnecting various information flows necessary to fight the clearly intertwined dimensions of terrorism, migrant smuggling and other serious crime.

Furthermore, in order to close the gap in information sharing, i.e. with regard to foreign terrorist fighters, it is necessary to continue a consistent three-tier approach, by monitoring any links between data sets on foreign terrorist fighters in SIS, the Europol Information System (EIS) and the relevant analysis projects at Europol. This would be beneficial for both the EU law enforcement community and the border guards who, for example, do not have the same access to information from third countries that Europol has.

With regard to different dimensions on interoperability:

- the expert group welcomes Europol's efforts to incorporate QUEST in national SSIs and the fact that this also anticipates the eventual search of the Europol data via a European search portal (see Section 5.1);
- the group supports the idea that the shared biometric matching service would also serve Europol; and
- as regards the common identity repository, the expert group would again welcome Europol data becoming part of the system.

Recommendations by the group

- ➢ Europol should redouble its efforts to make full use of its existing access rights for consultation purposes to SIS, VIS and EURODAC.
- ➢ The Commission and Europol should explore and promote synergies between the Europol data and other systems, notably the SIS.
- ➢ Member States should as of now systematically share information held in the SIRENE hit reporting forms with Europol's analysis project *Travellers*.
- ➢ Europol should continue its important work on QUEST, including in support of the development of national single-search interfaces.
- ➢ The Commission, eu-LISA and Europol should closely cooperate on the assessment of the feasibility of including Europol data in the development of the European search portal, the shared biometric matching service and the common data repository.

5.5.2 Interpol

The group had an exchange with Interpol on their approach to interoperability. Interpol aims to enable police and border control officers to obtain, when needed, all relevant law enforcement information that is available in its various databases, and to provide a platform for a secure exchange of information between the Interpol National Central Bureaux of its member countries. Its strategy as a worldwide hub for police is to advance interoperability, including through supporting regional data formats such as Universal Message Format and undertaking a mapping and gap analysis of databases for law enforcement access.

Biometric data are a priority for Interpol. Interpol supports wide access to databases, highlighting in particular its databases for Stolen and Lost Travel Documents (SLTD) and Travel Documents Associated with Notices (TDAWN). The group's discussions addressed whether the envisaged European search portal should also include at a later stage the Interpol databases. Experts however suggested to concentrate first on EU central databases such as SIS, VIS, Eurodac and others before investigating further the possibility to include Interpol databases.

The status of Interpol as an international organisation and the fact that Interpol systems are (also) being fed and consulted by non-European countries will require a specific focus on data protection and other fundamental rights issues.

Recommendations by the group

- In due course, the Commission should consider the technical, operational and legal feasibility of including Interpol databases under a European search portal, taking into account the specific data protection issues.

5.6. Interoperability with customs systems

Customs authorities are also a crucial actor in the multi-agency cooperation at the external borders. They have various systems and databases that contain data on movements of goods, identification of economic operators and risk-related information that can be used to reinforce internal security. These systems also have their own controlled, restricted and secure infrastructure (Common Communication Network), which has proven its viability. The expert group therefore considered it necessary to create synergies and convergence between information systems and their corresponding infrastructures for both EU border management and security and for customs operations.

The borders and security systems discussed by the expert group are generally about people. Customs systems would allow the identification and tracking of goods received by persons or economic operators, known or suspected to be involved in organised criminal or terrorism activities. Customs systems can offer an alternative approach whereby people can potentially be identified through the goods that they send or receive, and the addresses involved.

All transport means (air, maritime, road, rail, post, inland waterways, intermodal) can be used to smuggle, for example, explosives and their precursors, weapons, firearms and ammunition.

Details of all these movements of goods by different transport means are electronically reported to the customs advance cargo information system (currently the import control system) prior to their arrival from third countries at the EU's external borders. Goods data is risk-assessed by customs systems using common risk criteria. Future reform of the import control system would see it collect more and better quality trade data, making this data available to all customs concerned, not just those of the Member State of first entry to the EU. Such a common repository would enable relevant law enforcement data to be used securely to better target potential security risks (closing knowledge gaps for overall security in relation to organised crime, terrorism...) when it comes to goods movement.

Customs risk analysis expertise and risk information should also be integrated in the Passenger Information Unit processes under the new Passenger Name Records (PNR) Directive.

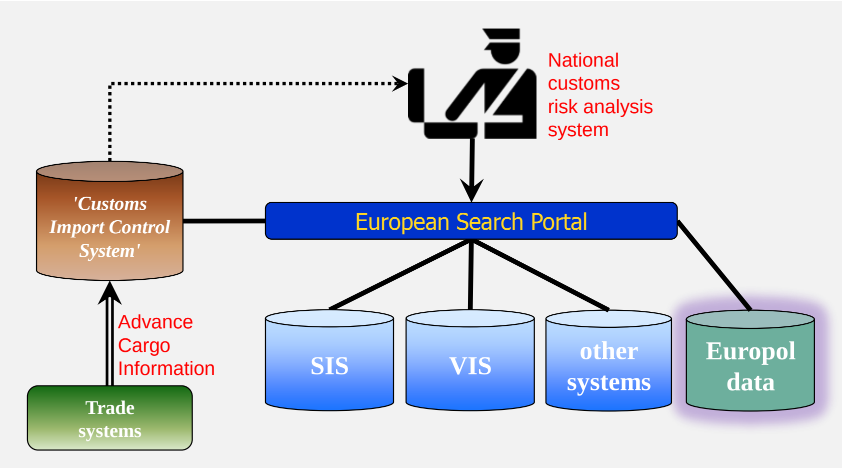
National customs risk analysis system
'Customs Import Control System'
European Search Portal
Advance Cargo Information
Trade systems
SIS
VIS
other systems
Europol data

Figure 12 Customs repository and the European search portal

The group discussed possible options for making customs systems more interoperable with the security and border management systems, including SIS and Europol data, including possibly through a future European search portal. To examine the feasibility and proportionality of establishing such a system, more detailed exchanges will be required between those running customs systems and those running security and border management systems.

Recommendations by the group

- The Commission should organise an expert meeting with security, border management and customs experts on the options of promoting interoperability across the respective systems. The experts should consider the technical, operational and legal feasibility of establishing interoperability across the relevant systems.

- The Commission and Member States should continue to develop the import control system.

- The Commission should launch a feasibility study to explore further the technical, operational and legal aspects of interoperability with customs systems.

5.7. Communication with carriers

The April 2016 Communication pointed to the need to increase the added value of advanced passenger information (API) data by establishing automated cross-checking of this data against relevant databases. It also envisaged the possibility to include an obligation for Member States to require and use API data for all inbound and outbound flights. This requirement would be complementary to the processing of passenger name record (PNR) data and further enhance the effectiveness of the latter in identifying high-risk travellers.

5.7.1 Advance passenger information

Member States currently receive API data in a batch format (the complete passenger list) exchanged directly between the airline and the Member State.

In the near future, interactive API data will be necessary to enable carriers to check a travel authorisation and to check remaining authorised stay (EES & VIS) in the absence of stamps in the passport. This exchange will need to take place between all airlines and the EES/ETIAS central system.

While it is not impossible to arrange these two distinct data flows with all airlines concerned, experts were keen to explore a different way to transfer these data from carriers to the relevant entities in Member States and at central level.

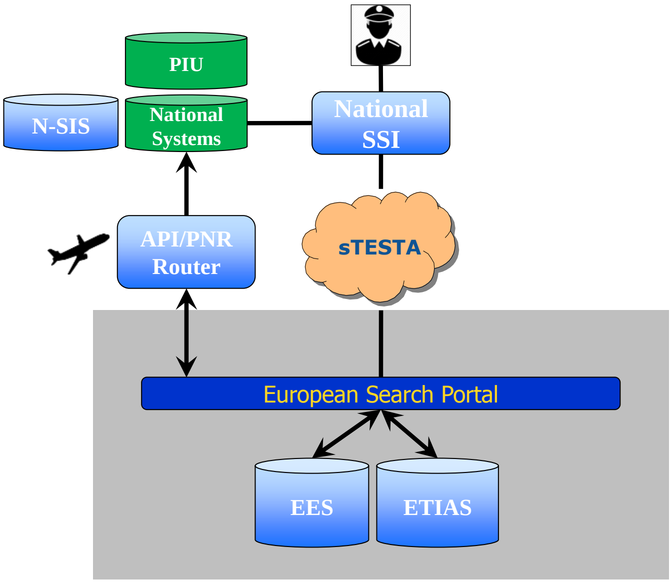

Figure 13 A centralised router for API data

This could include Member States opting, on a voluntary basis, for a single router or hub, perhaps hosted by eu-LISA, that would collect such API data from air carriers and transfer them to the Member States and central entities, subject to legal and technical assessments.

The API hub would act as a single point of contact for a carrier to deliver these types of API data, which would then be forwarded to the relevant central and national entities.

Recommendations by the group

➢ The Commission should undertake a feasibility study on a centralised mechanism for advance passenger information (API), including the need for a centralised router. The aim would be to enable interested Member States to have a one-stop-shop connectivity for airlines and providing API data both to national systems and to central systems (EES, ETIAS).

5.7.2 Passenger name records

The group noted that Member States are required to ensure implementation of the PNR Directive by May 2018 and urged that Member States ensure its full implementation according to the schedule set down in the legislation. Any possible future assessment should not affect or delay the ongoing implementation activities, and notably the ability of Member States to receive PNR data directly from air carriers.

Once Member States have implemented the PNR Directive and set up a national Passenger Information Unit (PIU) by May 2018 at the latest, they could benefit from a support tool to facilitate the connectivity with air carriers. This could strengthen the effectiveness of the national PIU when Member States apply the PNR Directive.

In order to facilitate the coverage of carrier data, the above-mentioned API router could be reused (for certain airlines, by certain Member States) to also transfer PNR data.

Recommendations by the group

- Member States should ensure the full implementation of the PNR Directive according to the schedule set down in the legislation.
- The Commission should consider extending the feasibility study for the implementation of a centralised API router and also analyse its use for passenger name records (PNR). The aim would be to enable interested Member States to have a one-stop-shop connectivity for airlines and providing PNR data to national systems.

6. CONCLUSION

The high-level expert group has agreed extensive recommendations based on the productive discussions that took place in its meetings.

As regards the core task of the group to address the legal, technical and operational aspects of four options to achieve interoperability of information systems, the group concludes that it is necessary and technically feasible to work towards the following three instruments for interoperability and that they can, in principle, be established in compliance with data protection requirements: a European search portal, a shared biometric matching service and a common identity repository. In the group's view, the option of interconnectivity of systems should only be considered on a case-by-case basis, while evaluating if certain data from one system needs to be systematically and automatically reused to be entered into another system.

The group had a specific mandate and schedule for delivering its report and it is now for the Commission, Member States and stakeholders to consider the recommendations.

The group took an ambitious and far-reaching approach, deeming this is necessary given the challenges faced by all those responsible for the information systems in the areas of border security and migration management. The group acknowledges that its recommendations will present challenges in taking them forward and implementing them. It hopes that the Commission will gain the support of the European Parliament and the Council so that work can begin as soon as possible.

Annexes

Annex 1 — Members of the high-level expert group on information systems and interoperability

The group was chaired by the Director-General of the European Commission's Directorate-General for Migration and Home Affairs. It included high-level representatives of the following:

EU Member States:

Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
United Kingdom

Schengen Associated Countries:

Liechtenstein
Norway
Switzerland

EU agencies:

European Union Agency for Fundamental Rights (FRA)
European Border and Coast Guard Agency (Frontex)
European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)
European Asylum Support Office (EASO)
European Union Agency for Law Enforcement Cooperation (Europol)

EU institutions/bodies

European Commission
EU Counter-Terrorism Coordinator
European Data Protection Supervisor (EDPS)

Observers

Secretariat of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee)
General Secretariat of the Council

Annex 2 — Overview of meetings of the high-level expert group on information systems and interoperability

The high-level expert group met five times.

At the high-level group’s first meeting in June 2016, experts established its working methods and timeline. On substance, they agreed on the need to exploit the existing information-sharing environment — notably for the Schengen and visa information systems (SIS and VIS) and Eurodac — and to build upon it after having identified gaps. The group committed to examine various means to improve the interoperability of systems: single-search interface; a shared biometric matching service; and a common repository of data.

In its June meeting, the group also decided to set up three subgroups, one each to examine existing systems, new systems and the interoperability of systems. The subgroup on existing systems has met twice, on new systems once, and on interoperability three times. These subgroups report back to the high-level group with their conclusions and proposed recommendations.

The high-level group’s second meeting took place in September. The group emphasised the importance of ensuring the highest standards of data quality and using systems to their potential. The discussions reflected a sentiment that existing systems and practices should be improved before thinking of developing new ones. One particularly promising path to be considered would be a single-search interface for accessing EU systems. The group also acknowledged the need to address conditions of access for law enforcement purposes, and governance of systems generally. When considering information gaps, the group reacted to the Commission’s latest thinking, thereby providing input for the subsequent Commission proposal to establish a European travel information and authorisation system (ETIAS).

In the third meeting, in November, the group considered a set of preliminary recommendations based on the work so far in the subgroups, primarily on single-search interface, data quality and a shared biometric matching service. It also considered the need to identify the obstacles and solutions for law enforcement access, not only for Eurodac but also for the Entry/Exit System (EES) and VIS, and whether such obstacles could be overcome by technical solutions. At this meeting, it was also restated that the group’s work is firmly based on all relevant data protection and fundamental rights considerations.

The fourth meeting took place in February 2017. At this meeting, the group broadly endorsed the chair’s interim report as a basis for the main conclusions and recommendations for the final report of the group. It also considered other specific issues related to certain systems (SIS, Eurodac, Prüm, PNR and ECRIS for third-country nationals) upon which this report gives further guidance.

The final meeting of the high-level expert group, in April 2017, was to conclude an agreement on the group’s report.

Annex 3 — EU Fundamental Rights Agency — Executive summary of the paper *Fundamental rights and the interoperability of EU information systems: borders and security*[26]

This annex is submitted by the EU Fundamental Rights Agency, which is solely responsible for its content.

The EU Fundamental Rights Agency (FRA) appreciates having been invited to participate in the high-level expert group on information systems and interoperability. The FRA also appreciates that the group has considered possible implications on fundamental rights throughout its work.

Interoperability between EU information systems in the areas of borders and security aims to assist in the decision making by providing a more complete picture about a person. Such information systems cover mainly non-EU citizens, including short-term travellers, asylum seekers, and third-country nationals with criminal records.

Depending on the technical solution chosen, interoperability can create additional fundamental rights challenges or amplify those already present in existing systems. At the same time, interoperability can provide new opportunities to offer more robust and timely protection, for example in the case of missing children.

Due to the underlying aim of interoperability — providing easy and quick access to information about third-country nationals — a number of the challenges are linked to the right to private life (Article 7 of the Charter of Fundamental Rights) and the protection of personal data (Article 8 of the Charter). Furthermore, the actual broader availability of data can in itself have additional implications — positive or negative — on, for instance, the right to an effective remedy (Article 47) or the prohibition of torture and inhuman or degrading treatment or punishment (Article 4), liberty and security of person (Article 6), integrity of the person (Article 3), the right to asylum (Articles 18) and prohibition of collective expulsion (Article 19), rights of the child (Article 24) and equality before the law (Articles 20).

Protection of personal data

According to Article 8 (1) of the Charter, everyone has the right to the protection of their personal data. Article 7 stipulates the right to respect for private life. Any interoperable solution or solutions selected for the EU information systems will need to be designed in a manner which does not unduly affect core data protection principles. Data protection by design and by default (commonly referred to as 'privacy by design') is often highlighted as a precondition for establishing interoperability in line with core data protection principles.

Alphanumerical data can be unreliable for establishing the identity of a person, whereas the use of biometric data makes the matching significantly more reliable. Interoperability needs to respect the special sensitivity of biometric data, which require additional safeguards to be considered when such data are processed.

[26] http://fra.europa.eu/en/publication/2017/fundamental-rights-interoperability.

Interoperability should not lead to the processing of more — biometric or alphanumeric — data than necessary for the existing purposes under the individual legal instruments. Technical solutions chosen must limit access only for authorised purposes and to authorised staff and must provide for automated deletion of data to comply with legally set retention times. The biometric matching service and the single search interface should not be programmed to actually store data, but only to match it.

If interoperability solutions envisage the possibility to show 'flagged' hits, which would inform the officer about the existence of additional data that he or she is not authorised to access, adjustments will be necessary to the legal instruments establishing the different information systems. The knowledge of the existence of additional information about the person, such as an entry in ECRIS or SIS II, possibly under another name, may support the identification of the person and influence the decision-making.

Interoperable databases may be highly attractive for those trying to access personal data by illegal means, not only organised crime groups but potentially also hackers linked to foreign states. One of the pillars of any interoperable solution must therefore be strong data security measures. Particularly mobile devices would need to be secured against unauthorised access. In instances when officers may request indirect access to information stored, effective verification procedures are necessary to determine if the requesting person is authorised to receive the information.

Because interoperability will make access to data easier it increases the chances that data are unlawfully shared with third countries. This risk would be exacerbated if 'flagged' hits would be accessed, as a hit in Eurodac would indicate that the person is an asylum seeker. Safeguards would need to be in place to ensure that the rules on sharing of data with third countries as laid down in the individual legal instruments are adhered to also in case of interoperability.

Right to an effective remedy

Data stored in information systems may not always be accurate and therefore not always reliable. Interoperability provides the authorities with increased opportunity to become aware of inaccuracies. Authorities should, therefore, develop standardised procedures for automatic verification with data stored in other IT systems and correct inaccurate data immediately. On the other hand, if the personal data which are re-used are incorrect, interoperability may possibly lead to inaccurate information being taken over from one system to another. Mistakes are not necessarily due to the accuracy of the data, but also to administrative errors, for instance if the biometric data is attached to the alphanumeric data of another person.

Due to the high degree of credibility attached to biometric data as well as the technical complexity of its processing, it is difficult to rebut errors based on biometrics. To give effect to the right to rebut a false assumption based on biometric data, the authorities would need to be ready to address plausible arguments presented by the data subject.

Complying with the duty to inform may be additionally complicated in a situation of interoperability. The officer accessing the databases would first need to be clearly aware of which database he or she is consulting, which may not be obvious when consulting several information systems. Not ensuring the right to information may make it impossible for the person concerned to exercise his or her right to access own data and have it rectified where necessary, which is a recognised fundamental rights in Article 8(2) of the Charter.

Rights of the child

Article 24 of the Charter emphasises the best interests of the child as a key principle of all actions taken in relation to children by public authorities and private actors. Interoperability may magnify some pre-existing risks in the case of children, particularly as the child had no say in the parents' decision to migrate.

The physical development of the child may reduce the reliability of matches based on biometric data, particularly after a longer period of time. Matches based on fingerprints older than five years, or on a facial image, should therefore always be subject to further checks and verified against other available data.

Information on criminal records may have a disproportionate impact on children, for example when they relate to immigration offences for which the children cannot be held responsible. In light of the vulnerability of children, consideration should be given to either excluding information on criminal records of children from the scope of the interoperable solutions altogether, or to limiting the availability of this information to very serious crimes committed by children.

Interoperability can support the detection of missing children or children subject to trafficking in human beings and facilitate a targeted response. This requires the systematic recording of missing children in SIS II, an additional focus on child protection in the individual IT systems, particularly in Eurodac, as well as functioning referral mechanisms and tailor-made training of practitioners who may encounter children in need of protection.

International protection

Under EU law Article 18 of the Charter protects the right to asylum. Effective access to international protection also forms the basis for the protection from refoulement, which is reflected in Article 19 of the Charter.

Through interoperability, identity frauds will be more easily identified. However, the use of false documents should not have an undue impact on decisions to grant international protection, as many seek to hide their identity when fleeing their country of origin in order to protect themselves, while others may be physically unable to obtain the documents necessary for legal entry (such as a passport and visa) when escaping from a conflict zone. Moreover, information originating from third countries that may be consulted through interoperability should not be taken at face value, for instance, oppressive regimes may include information about opponents in the Interpol database SLTD (Stolen and Lost Travel Documents) to prevent them from leaving the country.

Interoperability may have beneficial effects for persons seeking international protection. By ensuring that the status as an applicant for international protection is visible also when consulting other systems, it would reduce the risk of apprehension, detention or return, and also contribute to respect for the principle of non-refoulement. Past records in other systems may also help establish the identity of an undocumented person forced to flee persecution or other risk of harm.

Rights of migrants in an irregular situation

Making the EU's information systems interoperable can contribute to more efficient immigration law enforcement, as a number of systems can simultaneously be accessed to determine if a person who has been stopped has the right to stay. Certain enforcement measures have a disproportionate impact on their ability to enjoy basic rights protected by the Charter, such as the right to education (Article 14), the right to health care (Article 35) and the right to an effective remedy (Article 47), which must be provided to everyone, without discrimination.

Due to the risk of apprehension irregular migrants become afraid of approaching health services or send their children to schools. Victims of crime may be reluctant to approach the police for fear that this would lead to their removal, which puts them at risk of further victimisation and allows perpetrators to go unpunished. FRA's guidelines on the rights-compliant apprehension of migrants in an irregular situation (2014) recommends amongst others that there should be possibilities for victims and witnesses to report crime without fear of being apprehended, which is of particularly importance as interoperability supports the security agenda.

Risk of unlawful profiling

The data contained in information systems can be used for risk assessment or profiling. The use of sensitive data for profiling is exceptionally permitted where it is necessary for reasons of substantial public interest, on the basis of EU or Member State law. Even where the profiling is based on public interest stipulated in law, it will still be considered unlawful where it is discriminatory in nature, either directly or indirectly. In the words of the Racial Equality Directive (2000/43/EC), discrimination occurs 'where one person is treated less favourably than another is, has been or would be treated in a comparable situation on grounds of racial or ethnic origin.' Article 11 (3) of the Data Protection Directive (EU) 2016/680 explicitly prohibits any profiling that results in discrimination on the basis of sensitive data. Automated risk assessment or profiling would, therefore, have to be based on algorithms that are not primarily or solely determined by personal characteristics that reveal sensitive information such as, race, ethnicity, health, sexual orientation, and religious beliefs. By increasing the availability of this information contained in individual databases, interoperability may increase the risk of discriminatory profiling.

At the same time, access to additional information due to interoperability may help reduce the likelihood of discriminatory risk assessment based on sensitive personal data. This is because it would allow to conduct more focused searches based on a combination of non-sensitive criteria instead of relying on a limited number of sensitive categories.

Conclusion

Interoperability involves both risks and opportunities for fundamental rights. Receiving the full picture about a person contributes to better decision-making. To this end safeguards need to be in place to ensure the quality of the information stored about the person and the purpose of the data processing. Such safeguards should prevent unauthorised access and unlawful sharing of information with third parties. To ensure the right to an effective remedy, practical possibilities to rebut a false assumption by the authorities as well as to have inaccurate data corrected need to be in place.

Interoperability can support the detection of missing children or children subject to trafficking in human beings and facilitate a targeted response. This requires the systematic recording of missing children in SIS II, and an additional focus on child protection in the individual IT systems. Interoperability can also contribute to respect for the principle of non-refoulement by ensuring that the status as an applicant for international protection is visible also when consulting other information systems. Risks for discriminatory profiling may be reduced if a combination of non-sensitive criteria is used instead of relying on a limited number of sensitive categories.

Annex 4 — European Data Protection Supervisor — Statement on the concept of interoperability in the field of migration, asylum and security

This annex is submitted by the European Data Protection Supervisor, who is solely responsible for its content.

Introduction

The European Data Protection Supervisor (EDPS) appreciates having been invited to join the high-level expert group on information systems and interoperability and been given the opportunity to express his comments. He supports the Commission's initiative to reflect on an overall strategic vision on how to make the management and use of data, both border management and security, more effective and efficient in full compliance with data protection. He acknowledges the considerable work done by the group in this respect. He observes that, beyond data protection, the current legal framework sets an objective limit to the simplification of existing systems.

The EDPS is not in a position to endorse all the conclusions referred to by the high-level expert group in its final report on existing systems, new systems and interoperability of systems. Full compliance with data protection requirements can, in his view, only be assessed having a comprehensive and further detailed picture of the measures and solutions envisaged by the group. Since the EDPS had the opportunity to follow more closely the work of the subgroup on interoperability, he would like to share in this statement some preliminary comments on the concept of interoperability as envisaged by the Commission.

In his role as advisor and supervisor, the EDPS will continue to monitor developments closely. He welcomes and appreciates the intention of the group to associate him in further discussions and expects to be consulted in any case where the Commission presents initiatives and/or proposals in this area.

Background and challenges

The current framework

Currently, an individual's personal information related to migration and asylum matters, police cooperation and the management of the EU's external borders is collected, used and stored in several distinct large-scale IT systems that are not interconnected with each other. This configuration is the result of various factors: the specific needs at the time of the creation of the information systems, and the institutional, policy and legal contexts in which these needs were addressed.

With the recent influx of migrants and also terrorist attacks in Europe, pressure is growing to increase the EU's capacity to reduce irregular migration, to ensure effective and efficient border management and to enhance internal security. This has prompted the European Commission to launch a process towards the interoperability of information systems in the fields of migration, asylum and security as mentioned in the Commission Communication of 6 April 2016 *Stronger and Smarter Information Systems for Borders and Security*.

Interoperability

Interoperability is commonly referred to as to the ability of different information systems to communicate, exchange data and use the information that has been exchanged. Through the interoperability of EU large-scale information systems, the Commission's objective is to ensure that the competent authorities get the right information at the right time.

The EDPS supports initiatives aiming at developing effective and efficient information management. He also recognises the need for better sharing of information to manage migratory challenges and tackle terrorist and crime-related issues. Furthermore, interoperability as envisaged by the Commission is an ambitious project from a legal perspective, not only because of data protection requirements, but also given the complexity of the current legal framework. In this regard, the EDPS would like to stress that the main obstacles to a sustainable interoperability arise from the current legal basis of the information systems rather than merely from data protection principles.

Data protection safeguards

As a first step, interoperability will build on existing (and proposed new) information systems based on the current fragmented legal framework composed of various legal instruments adopted to address specific needs at a given time. The EDPS stresses the importance in a second stage, to reflect on a more consistent, coherent and comprehensive legal framework in view of the ultimate objectives in terms of migration, asylum and police cooperation.

The EDPS highlights that technology and technical solutions come in support of policies. It is therefore fundamental to first clearly specify the policy objectives and analyse the core needs at all levels to determine the most appropriate technical solutions. Situations where technical choices appear to be driving political decisions can never be accepted. Furthermore, starting with the policy objectives and then analysing the core needs is necessary in order to respect key principles of data protection. Privacy by design notably requires to limit the requirements to what is strictly necessary before moving on to the implementation of these requirements.

The EDPS welcomes that the European Commission stresses the importance of data protection, in particular the principle of purpose limitation and user's access rights, when developing interoperability. Interoperability should indeed never lead to a situation where an authority not entitled to access or use certain data can obtain access via another information system or could access more data than those that it actually needs.

Interoperability will also introduce a fundamental change to the current architecture of large-scale IT systems: from a *closed environment per system*, we will move to a *shared environment* where there will be connectivity between those systems. The information security consequences of such a decision cannot be underestimated and a proper information security analysis needs to be considered before implementing any change that may endanger the security of all systems.

Proposals of the Commission on interoperability in its Communication of 6 April 2016

In its communication, the Commission distinguishes four dimensions of interoperability: a single-search interface, a shared biometric matching system, the interconnectivity of information systems and a common repository of data.

Single-search interface (SSI)

The SSI would be a European search portal capable of searching in parallel all relevant EU information systems. The objective is to give the user a faster and easier access to the information stored in the systems. Instead of having to query each system separately, the user could query several systems simultaneously and get a combined result on one single screen.

As long as this solution fully complies with purpose limitation and access rights (i.e. the user accesses only the information he/she is allowed to access and exclusively for the purpose(s) of the different systems), the EDPS does not have major concerns.

Shared biometric matching service

The biometric matching service would allow to match biometric data from existing (and future) EU information systems. The biometric matching service would be used as a single-search interface where queries are made on the basis of biometric data instead of alphanumeric data. The EDPS also understands that the Commission intends to use the biometric matching service to highlight through flags whether information is, or is not, available in other information systems. Both these options raise issues on purpose limitation and access rights that would require careful analysis. The EDPS recalls that the existence or lack of flag(s) constitutes as such personal data since it contains already some information about an identifiable person (e.g. the person is subject to an alert in the Schengen Information System). As a consequence, the user who is not allowed to access personal information stored in a specific system should not get access to any of this information, even if this information would be limited, for instance, to such a flag.

Furthermore, the EDPS highlights that it is fundamental to first determine the objectives of the flags, from a data protection perspective and also for operational aspects. Knowing that information exists without knowing what to do with it is useless in the decision-making process and contrary to the data protection principle of data quality.

Common identity repository

The Commission also suggests to further explore the possible establishment of a common identity repository, starting with the biometric attributes of an identity to further include common biographical attributes from the various existing systems into the common repository.

The EDPS stresses that a common (and centralised) identity repository raises serious issues in terms of data protection. The use of unique identifiers to collect information on the individuals from several databases is either strictly prohibited in some countries or framed by a legal framework.

The EDPS acknowledges the efforts made to clarify the reasons for creating such a common identity repository, especially by improving the accuracy and quality of identification data but also managing further access to these data. The EDPS considers that this essential step needs to be complemented by the specification of the ultimate purpose(s) and core needs justifying when such data will be used.

The various options to achieve the stated purposes should then be analysed taking into account their impact on fundamental rights. This is indeed an important prerequisite to allow a full assessment of the necessity and proportionality of the solution proposed. The EDPS stresses that merging information from databases should not automatically lead to the merger of their objectives, conditions of processing, and access management.

As regards the *interconnectivity of information systems*, the EDPS understands that this option is no longer followed by the Commission.

Annex 5 — EU Counter-Terrorism Coordinator — Statement on the report of the high-level expert group on information systems and interoperability

This annex is submitted by the EU Counter-Terrorism Coordinator, who is solely responsible for its content.

The EU Counter-Terrorism Coordinator congratulates the Commission on the excellent and comprehensive report. He welcomes the impressive work by the Commission and all stakeholders of this inclusive process. A lot of progress has been achieved on this complex topic in a short period of time, based on high quality work.

The EU Counter-Terrorism Coordinator is convinced that interoperability of information systems is an issue where the EU can achieve major progress and make a real difference. We need a paradigm shift in the way we deal with information systems. Interoperability is a priority at the highest political level. As the European Council has stated in its Conclusions of 18 December 2015: 'The recent terrorist attacks demonstrate in particular the urgency of enhancing relevant information sharing, notably as regards […] ensuring the interoperability of the relevant databases with regard to security checks.' More than 80 % of EU citizens are asking for more European actions in the field of security and counter-terrorism. We owe them an efficient and pragmatic response. As the group's report states, citizens will only continue to support core fundamental rights such as the free movement in the Schengen area and admission of refugees if the security checks are efficient to a maximum extent.

Feeding and consulting EU databases to a maximum extent is key to fighting against terrorism in an increasingly complex and transnational world. Given the threat picture, the current fragmentation of EU databases and the separation of border security, migration and counter-terrorism purposes of databases no longer reflect reality. The Lisbon Treaty makes information systems combining these interlinked objectives legally possible.

The EU Counter-Terrorism Coordinator is profoundly attached to **data protection** and welcomes the active involvement of the European Data Protection Supervisor and the EU Fundamental Rights Agency in the high-level expert group. The concept of **privacy by design** on which the report puts a lot of emphasis is not exhausted yet. More creative solutions, such as homomorphic encryption, should be considered in order to reconcile data protection principles and access to the data. It is very important to note that the EDPS states that the main obstacles are, indeed, the current legal basis of the information systems and not the data protection principles.

There is an urgent need to move forward quickly to implement all the interoperability solutions outlined in the report in an ambitious way.

The **single-search interface (or European search portal)** and the **shared biometric matching service** are necessary to speed up and facilitate alphanumeric and biometric searches. It is in the EU's strong security interest that the EU databases are indeed checked to the maximum extent, for example at the borders: this is what the two proposed solutions would help to make happen in practice. It will be important to integrate as much as possible Europol databases and also explore which Interpol databases can be included. It is crucial that **flags** indicate that information is available in systems to which the person consulting the single-search interface or the shared biometric matching service does not have access. In a second step, access to the systems can then be asked. Not showing flags risks making the single-search interface and the biometric matching service a lot less effective, as there is no longer a comprehensive overview of all systems in one search and important information may be overlooked. Separate requests just to know whether there is information in the system are not practical and too time consuming, the opposite of what the portals are meant to achieve. If, from a data protection perspective, legislation needs to be adapted to achieve these flags or hit/no-hit results, that should be done. The shared biometric matching services should not only be for fingerprints but also **other biometric data** such as facial images, which are the biometrics of the future.

The EU Counter-Terrorism Coordinator highlights that the establishment of a **common identity repository** is an urgent need and that the Commission, in cooperation with the eu-LISA and Europol, should work to implement it as soon as possible. Indeed, we need to have the most reliable possible means to establish identities. A common repository has considerable added value in addition to the single-search interface and the shared biometric matching service because it would allow to identify identity fraud by cross-matching biometric and alphanumeric data.

As the EDPS points out, it is not the data protection rules but the current legal framework of the various information systems that sets limits. Therefore, the **legal basis of the various systems should be reviewed and adapted where necessary**. Data protection rules do not require the limit of a purpose to one only. Where necessary, the purpose should be adapted to include both security and migration/border management. This is already the case in the forward-looking ETIAS proposal, which can in many ways be a model for future legislation (multiple purpose, centralised system, strong involvement of Europol and Frontex).

Law enforcement access to the various databases should be reviewed and streamlined to meet the business needs. If the information systems are too complex, they will not be used by the law enforcement authorities. Cascades for law enforcement access and specific types of biometric searches (such as for facial images) should be abolished because they restrict the available information and complicate the procedures involved. Time is often of the essence in the fight against terrorism. We should not prejudge the need of motivation and prior authorisation of access, but also explore alternatives. It would be difficult to explain to citizens that relevant information about a terrorist suspect had been collected but could not be accessed.

The **Eurodac** purpose should in the future also include security to facilitate appropriate law enforcement access. Alphanumeric searches in Eurodac should be enabled to strengthen interoperability.

The possibility to further modernise and expand the use of the **Prüm** system as a border security tool for quick and frequent checks on a hit/no-hit basis and the connection of the hub-and-spoke system to the biometric matching service should be explored.

To increase the efficiency of the information systems, it is crucial to enhance the use of **biometric data**. It is important that Member States should already feed information systems with biometric data. It is important to develop immediately a facial image search function for the Schengen Information System, ideally within the shared biometric matching service.

The EU Counter-Terrorism Coordinator welcomes the **close involvement of EU agencies in the high-level expert group** and recommends further strengthening of this. Europol access to Eurodac should be improved. We should also explore how to improve access for Frontex to the EU databases. It would be good to task Europol and Frontex to outline the interoperability and access business needs from an operational perspective to underpin future discussions.

To conclude, like the EU Fundamental Rights Agency, the EU Counter-Terrorism Coordinator thinks that interoperability represents major opportunities. The work of the expert group has demonstrated that the obstacles are less technical than political. Major progress has been done. The report should be considered as a starting point. We now have to quickly transform these propositions into concrete actions. The EU Counter-Terrorism Coordinator will continue to fully support the process of achieving ambitious interoperability solutions at EU level.

Annex 6 — Abbreviations and glossary

API	Advance passenger information
AFIS	Automated Fingerprint Identification System: system capable of capturing, storing, comparing, and verifying fingerprints.
BMS	Biometric matching service
CEPOL	European Union Agency for Law Enforcement Training
ECRIS	European Criminal Records Information System
EDPS	European Data Protection Supervisor
EES	(proposed) Entry-Exit System
EIS	Europol Information System
ESP	European search portal
Eurodac	European Dactyloscopy
Europol	European Union Agency for Law Enforcement Cooperation)
ETIAS	(proposed) European Travel Information and Authorisation System
eu-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
FRA	European Union Agency for Fundamental Rights
Frontex	European Border and Coast Guard Agency
ICS	Import control system
Interpol	International Criminal Police Organisation
PIU	Passenger information unit: unit to be set up in each Member State to receive the PNR data from carriers.
PNR	Passenger name record
Prüm	Police cooperation mechanism for exchanging information on DNA, fingerprints and vehicle registration data
QUEST	Querying Europol Systems (Europol web service)
SBC	Schengen Border Code
SIENA	Secure Information Exchange Network Application
SIS	Schengen Information System (sometimes referred to as of the 2nd Generation — SIS II)
SLTD	(Interpol’s) Stolen and Lost Travel Documents database
SSI	Single-search interface
sTESTA	secured Trans European Services for Telematics between Administrations (to be upgraded to TESTA-NG (next generation))
TDAWN	(Interpol’s) Travel Documents Associated with Notices database
UMF	Universal Message Format: format of messages to allow compatibility between information systems
VIS	Visa Information System