EUROPEAN COMMISSION
DIRECTORATE-GENERAL MIGRATION and HOME AFFAIRS

Directorate B: Migration and Mobility
Unit B.3: Information System for Borders and Security

High-level expert group on information systems and interoperability

Third meeting — 29 November 2016

Report

The meeting was opened by Olivier Onidi on behalf of Matthias Ruete, chair of the high-level expert group. He referred to the second progress report on the Security Union and the proposal for a European Travel Information and Authorisation System (ETIAS).

The focus of the meeting would be the draft recommendations received from subgroups. These recommendations — in particular on single-search interface, data quality, a shared biometric matching service and a common repository of data — would become the reference for the chair's interim report scheduled for December.

In addition, the European Data Protection Supervisor would speak on data protection aspects of the group's ongoing work.

The chair invited comments on the report of the previous meeting (20 September); these could also be given in writing. He gave notice that the Commission intended to bring forward the final meeting of the group from the end of May to the end of April.

Single-search interface (SSI)

The Commission presented the draft recommendations:

- Launch a proof of concept on the feasibility of creating a centralised single-search interface (or portal) at EU level capable of searching in parallel SIS, VIS, SLTD and EIS, and the future EES and ETIAS.
- A centralised SSI would not connect to national databases but national SSIs would be connected to the SSI at EU level for the querying of EU-systems.
- Explore the potential practical and operational challenges for Member States to fully exploit such a centralised SSI.
- Europol efforts to incorporate Europol data queries via QUEST in national SSIs should be supported in view of an eventual linkage to a central SSI.
- The centralised SSI solution to be explored and tested within the broader perspective of envisaging a common repository of data.
- Any design of a centralised SSI to respect the EU Charter on Fundamental Rights. Discussions should fully involve fundamental rights and data protection actors.

Comments from experts

There was support for the general terms of the recommendations. The main comments from experts related to the following:

- Support the proof of concept taking into account access rights and the need to operate with one language, which could help to future-proof systems.
- Keep technical and operational developments as simple as possible. Design the SSI in such a way that national systems are unaffected, and envisage a transitional period for access from national systems. The longer-term perspective of SSI (including costs and technical challenges) is an argument to make best use of existing systems.
- SSI should make accessible both alphanumeric and biometric data.
- There is an interest to access Europol data from national systems. Accelerate work on QUEST, and consider how it could support the development of an SSI. Consideration should also be given to linking with Interpol databases.
- Legal aspects should be fully considered.
- Consider including Eurodac and the European Criminal Records Information System (ECRIS) in the SSI, and whether the SSI is able to consult the SIS automated fingerprint identification system. Consider access to decentralised systems.
- Access to a future SSI for all systems would have to address the situation of those Member States that are not full Schengen states.
- Response times of such a system should be quick to facilitate fluidity at borders, and mobile solutions should also be considered for guest officers.
- Identify the channel to be used, for example SIS sTESTA.
- Workload being suggested for eu-LISA to be assessed in light of resources.
- A wider view should be taken of the data architecture in the justice and home affairs domain as a whole.

The Commission noted that several experts had commented specifically on legal aspects, access to biometric data and Interpol systems. These issues would be given particular attention in the further discussions to come. The suggestion to extend to decentralised systems was noted but would not be the immediate priority.

The chair, Matthias Ruete, concluded that there was broad support for a European search portal along the lines discussed. The first aim was to make access to European databases easier. The proof of concept would be launched as soon as possible and would consider system speed, databases to be covered, biometrics, data protection and — if possible — Interpol systems.

Data quality (SIS, VIS and Eurodac)

The Commission presented the draft recommendations to be pursued in cooperation with eu-LISA:

- Establish a framework for monitoring data quality at central level while respecting that responsibility for data quality rests with Member States.

- Establish rules for scrutinising data quality in each of the three systems.
- Establish a reporting process based on comprehensive quality indicators.
- Schedule a biannual peer review of data quality.
- Devise relevant training modules for staff at national level.

In due course, a data warehouse could a source for regular reporting.

Comments from experts

There was general support for the recommendations. The main comments from experts related to the following:

- Need to be specific in defining 'data quality'.
- Improvements in data quality must be made in the short-term.
- Data warehouse not a priority for some but for others worth examining.
- Training at national level is too often neglected, and should also be promoted at European level. Training should also focus on feeding systems.
- Examine whether eu-LISA has the mandate and resources to undertake such actions.
- Need to develop specifications for digital photos and procedures to collecting digital data.
- Try to set common data quality standards applicable to all systems.
- There is a need to be able to reconcile identities across systems and data quality can support this, especially useful in identifying foreign terrorist fighters.
- Greater efforts should be made to raise standards of interoperability at EU level.

The chair concluded that data quality would be noted as a priority action in his interim report, taking account of the comments made.

Shared biometric matching service

The Commission presented the draft recommendations, noting that a shared biometric matching service would offer benefits not just to border control authorities but also for immigration and asylum authorities.

- To generate financial, maintenance and operational benefits, all relevant centralised EU systems (SIS, VIS, Eurodac, EES, possibly ECRIS and EIS) should in principle share the same biometric matching service, while fully respecting personal data protection rules.
- eu-LISA should analyse the technical and operational aspects of the possible implementation of a shared biometric matching service on the basis of the required new EES infrastructure with a view then to integrate other relevant systems.
- Europol could analyse how such a service could match biometric data from its data.

- The shared biometric matching service could be used to flag the existence of biometric data from other systems, while respecting the original data-access control of the parent system and the need to comply with data protection principles.

Comments from experts

Experts expressed general support for the approach.

- A shared service would offer operational and cost benefits.
- EES and VIS could be the first to use a shared biometric matching service as a prelude to further development, in due course to a common repository of data.
- Support was expressed for a centralised automated fingerprint identification system.
- Linking to ECRIS would depend on future developments since ECRIS is currently a decentralised system.
- Consideration could be given to extending the service to national systems, not just EU systems. Interest was expressed in whether such a service could also work with Prüm databases for police officers.
- The proposed flagging of possible data from other systems was of interest but access rights would have to be considered.

The chair concluded that there was broad support to examine the concept further and perhaps even to go beyond the databases currently envisaged. In particular there was interest in the proposed flagging but this would need to factor in data protection and privacy.

Common repository of data

The Commission presented the draft recommendations:

- Examine whether all relevant centralised EU systems (SIS, VIS, Eurodac, EES, possibly ECRIS and EIS) should not only share the same biometric matching service, but eventually also the same common repository of data that would also include alphanumeric data.
- eu-LISA to analyse the technical aspects of the establishment of a common repository of identity data, and Europol to do the same for its data.
- Assess whether a common repository of data would be in line with the objectives and principles of privacy by design.

Comments from experts

- A common repository would be a logical next step after a shared biometric matching service.
- Such a repository raises issues concerning data protection and fundamental rights but a repository can still be designed in a way that respects these aspects.

- Some caution necessary as the proposed repository appears as a very ambitious long-term project. A cost-benefit analysis is advisable.

The chair concluded that there was a general feeling that this should not be seen as an immediate priority but was still of sufficient interest to be studied further. That would be in particular for eu-LISA but also Europol.

Interconnectivity and law enforcement access

The group reviewed briefly the proposed recommendations:

- Interconnectivity of systems is complex from a legal perspective so the business need should be considered on a case-by-case basis.
- Interconnectivity could be of less interest if there is progress on single-search interface, the shared biometric matching service and a common repository of data.
- There is a need to identify the obstacles and solutions for law enforcement access, not only for Eurodac but also for EES and VIS, and whether there are technical solutions available.

Comments from experts

- Interconnectivity should not be pursued just for its own sake, especially if the other proposals can meet the needs expressed.
- Law enforcement access should indeed be examined, and officers should be given a clear picture of existing legislation and their access rights to the systems.

The chair concluded that interconnectivity and law enforcement would be kept under review for the future meetings of the group. He emphasized that the issues at stake are mainly of a legal nature, and will in any case need to be addressed in the ongoing negotiations on the relevant legislative instruments. Discussions in the expert group on possible technical solutions had not yet advanced sufficiently to be able to make clear recommendations.

Data protection and fundamental rights

The European Data Protection Supervisor spoke on the issue of interoperability, noting that the objectives — to do more with less, data minimisation and data quality — can be common with data protection. Data protection and data flows are not polar opposites and modern data protection could be a win-win for both data controllers and data protection authorities. It was essential for the group to agree a definition of interoperability, for policymakers to better define the ultimate political goal and to ensure from the earliest stages a very clear scenario in terms of pre-requisites and legal requirements.

Law enforcement agencies and border management bodies need to work more closely than ever before. Systems set up for different purposes and made available to different

officials can resemble silos, which can limit the purposes for which data are processed, but might be bad for efficiency and cooperation. Yet the need for better exploitation of data should respect in practice all data protection principles.

Interoperability should be about making sure that the right people can get the right data at the right time, subject to the necessary checks and balances. The goal should be an intelligent police, not all-knowing officials, and transparency for citizens. Data protection is one of the pillars of the EU. Systems development should serve the essential public interest, not administrative convenience.

The EDPS was ready to work with the group to prepare a better future, where EU databases for border management and for law enforcement better embed a modern set of core data protection principles. For example, interpreting the data minimisation principle as allowing, or encouraging, the merging of data from several databases may represent a misunderstanding of this concept. Other important principles are purpose limitation ('need to know') and privacy by design. The EDPS suggested that its Internet Privacy Engineering Network could be associated with the work on interoperability.

Courts have held that indiscriminate and indefinite collection and storage of personal information is unlikely to be lawful. Care should also be taken to ensure that systems development does not open the door to security vulnerabilities that hackers could exploit. Data minimisation is not about quantity, but about quality of the data.

Repeating that the work of the high-level expert group raises data protection and privacy challenges, the EDPS concluded that he was ready to work closely with the group to achieve the desired goals.

The representative of the Fundamental Rights Agency stated that interoperability poses both fundamental rights challenges as well as opportunities. It was important from the outset to address the legal safeguards – and hence fundamental rights guarantees – to be built in to any system. Reliability of data, its use, and who is using it, are key issues not only for end-users of a system but also for those persons whose data is being collected, stored and shared, especially those who may be in a position of vulnerability.

The FRA supported the comments by the EDPS and outlined additional legal aspects. Due consideration should be given to the impact on fundamental rights of the person concerned - such as the right to asylum, the right to family life, and the right to liberty and security of the person. Options should be considered for an individual to have a possibility to effectively rebut a false assumption if information held in databases is incorrect. There are potential risks to the safety of people — such as political dissidents — and their families if personal data end up in the hands of third parties.

Robust data security measures need to be in place. Concerns have been raised that oppressive regimes can put political opponents in the Interpol Database on Stolen and Lost Travel Documents, thereby limiting their possibilities to travel. Safeguards including logging of all uses, per purpose, and not only the user profile, would need to

be ensured. Administrative safeguards should be in place to prevent unauthorised sharing with third parties.

There should be a right of access to one's own data to correct or delete it, especially if a system is interoperable with another.

Oversight and the rule of law should be ensured by regular inspections by data protection authorities and related experts. Fundamental rights benefits in the area of biometric data enable abducted or missing children to be identified, or to flag individuals who have been alerted as victims of trafficking. These benefits can be undermined through underuse of databases. The FRA will continue to support the work of the high-level expert group.

The chair said that the essence of these arguments would be addressed in his interim report. One comment in response to the presentations was that the separation of migration and security systems — and whether that should be maintained —was being discussed more and more.

Other business

A suggestion was made that there could be an increasing need — in light of terrorist acts — to consider including EU citizens in some form of entry/exit system. The chair said that this would be suitable for discussion in the next meeting of the subgroup on new systems.

Conclusions

The chair concluded by stating that he would prepare a report, as chair of the group, on the basis of the discussions. The report would be made available in December. He also advised that his aim was for the group as a whole to present its final report by May 2017.