European Data Protection Supervisor statement on the concept of interoperability in the field of migration, asylum and security

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 intiative 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 adressed.

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 intiatives 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 highights 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 acccess 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.