Interoperability between EU information systems (borders and visa)

2017/0351(COD) - 19/03/2018

Opinion of the European Data Protection Supervisor on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems.

In December 2017, the Commission published two legislative proposals for two Regulations establishing a framework for **interoperability between EU large-scale information systems**:

- a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) ;
- a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police, and judicial cooperation, asylum and migration).

The proposals would introduce new possibilities to access and use the data stored in the various systems in order to combat identity fraud, facilitate identity checks, as well as streamline access to non-law information systems by law enforcement authorities.

In particular, the proposals create **a new centralised database that would contain information about millions of third-country nationals, including their biometric data**. Due to its scale and the nature of the data to be stored in this database, the consequences of any data breach could seriously harm a potentially very large number of individuals. If such information ever falls into the wrong hands, the database could become a dangerous tool against fundamental rights. It is therefore essential to build **strong legal, technical and organisational safeguards**.

In this context, the EDPS stresses the importance of:

- further clarifying the extent of the problem of identity fraud among third-country nationals, in order to ensure that the proposed measure is appropriate and **proportionate**;
- formulating **more precisely** the possibility of consulting the centralised database to facilitate identity checks on the territory of the Member States;
- putting in place **effective safeguards** to protect the fundamental rights of third-country nationals in so far as systematic access to law enforcement systems could represent a serious breach of the purpose limitation principle.

More specifically, the EDPS makes the following recommendations:

- three of the six EU information systems the proposals seek to interconnect do not exist at the moment (the European Travel Information and Authorisation System ETIAS, the European Criminal Records Information System for third country nationals ECRIS-TCN and the EES entry /exit system), two are currently under revision (SIS and Eurodac) and one is to be revised later this year (VIS): the EDPS recalls the importance to **ensure consistency between the legal texts already under negotiation (or upcoming) and the proposals** in order to ensure a unified legal, organisational and technical environment for all data processing activities within the Union;
- **access to the data to identify a person during an identity check** would be allowed: (i) in principle, in the presence of the person and, where he or she is unable to cooperate and does not have document establishing his/her identity or, (ii) refuses to cooperate or, (iii) where there are

justified or well-founded grounds to believe that documents presented are false or that the person is not telling the truth about his/her identity;

- **access to the common repository of identity data** to establish the identity of a third country national for purposes of ensuring a high level of security should only be allowed where access for the same purposes to similar national databases (e.g. register of nationals/residents etc.) exist and under the same conditions;
- the proposal should **specify the conditions** related to the existence of reasonable grounds, the carrying out of a prior search in national databases and the launching of a query of the automated fingerprint identification system of the other Member States under Decision 2008/615/JHA, prior to any search in the common repository for identity;
- **the compliance with the conditions of access to even limited information** such as a hit/no hit should always be verified, independently of further access to the data stored in the system that triggered the hit;
- ensure in the proposals that the data stored in the **ECRIS- TCN** could be accessed and used solely for the purposes of the ECRIS TCN as defined in its legal instrument;
- **the fundamental data protection principles should be taken into account during all stages of the implementation of the proposals.** The obligation for eu-LISA and the Member States to follow the principles of data protection by design and by default should also be included in the proposals.

The EDPS has **additional recommendations** related to the following aspects of the proposals: (i) the functionality of the European search portal (‘ESP’), the shared biometric matching service (‘shared BMS’), the common identity repository (‘CIR’) and, the multiple identity detector (‘MID’); (ii) the data retention periods in the CIR and the MID; (iii) the division of roles and responsibility between eu-LISA and the Member States; (iv) the data subjects' rights; (v) the access by eu-LISA staff.

Lastly, the EDPS calls for a **wider debate** on the future of the EU information exchange, their governance and the ways to safeguard fundamental rights in this context.