Works on Interoperability of EU Information Systems Can Start – Legal Framework Established

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

Thomas Wahl

On 22 May 2019, the new rules establishing a framework for interoperability between EU information systems in the field of borders and visa (Regulation (EU) 2019/817) and in the field of police and judicial cooperation, asylum and migration (Regulation (EU) 2019/818) were published in the Official Journal of the European Union (O.J. L 135). The Regulations that had been initiated by the Commission on 12 December 2017 (see eucrim 4/2017, pp. 174-175) were adopted by the Council on 14 May 2019. After publication in the Official Journal, the Regulations entered into force on 11 June 2019. The various interoperability components need technical implementation, however, which is why the date of the operational start of the components is determined by the Commission. It is expected that they can be applied by 2023.

AUTHOR

Thomas Wahl

Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2019, Vol. 14(2) eucrim pp 103 – 104

ISSN: 1862-6947

https://eucrim.eu

The two sets of Regulations had become necessary, because the legal bases of the information systems were different and the levels of EU Member States' involvement in the various databases varied. Nonetheless, both Regulations largely contain identical provisions.

The interoperability framework solves the problem that, to date, data are separately stored in various large-scale IT systems at the EU level, but the systems can principally not communicate with each other. This may lead to information gaps, e.g., information could get lost or criminals with several or false identities may remain undetected. The Regulations therefore pursue several different objectives (defined in Art. 2(1) of the Regulations):

- Improve effectiveness and efficiency of border checks at external borders;
- Contribute to prevention and combating of illegal immigration;
- Contribute to a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and safeguarding security in the territories of the Member States;
- Improve implementation of the common visa policy;
- Assist in examination of applications for international protection;
- Contribute to prevention, detection, and investigation of terrorist offences and other serious criminal offences;
- Facilitate identification of unknown persons who are unable to identify themselves or unidentified human remains in cases of a natural disaster, accident, or terrorist attack.

Hence, the interoperability framework focuses on the correct identification of persons and on combating identity fraud. At the same time, it will, *inter alia*, improve data quality and harmonise the quality requirements for data stored in EU information systems (cf. Art. 2(2)).

In order to achieve the objectives, the Regulations establish the following interoperability components and specify their purposes, use, queries, access possibilities, etc.:

- *European search portal (ESP)*: it enables the competent authorities of the Member States and the Union agencies to gain "fast, seamless, efficient, systematic and controlled access" to the EU information systems, to Europol data, and to Interpol databases. The ESP can be used to search data related to persons or their travel documents. The ESP does not change the access rights of the authorities/Union agencies. After having launched a query to the ESP (by submitting biographic or biometric data), the system indicates which EU information system or database the data belongs to. The ESP will not provide information regarding data in EU information systems, Europol data, and Interpol databases that the user has no access to under applicable Union and national law.
- *Shared biometric matching service (shared BMS):* it is a technological tool to match the individual's biometric data across different systems; it will regroup and store all biometric templates in one single location that are currently being separately used in the EU information systems. In this way, it will enable the searching and comparing of biometric data (fingerprints and facial images) from several systems.
- *Common identity repository (CIR)*: it contains biographical and biometric data of third-country nationals available in several EU information systems. It aims to increase the accuracy of identification through automated comparison and matching of data;
- *Multiple-identity detector (MID)*: it checks whether the biographical identity data contained in the search exist in other systems covered in order to enable the detection of multiple identities linked to the same set of biometric data.

An infographic provided for at the Council website illustrates how the tools work.

The Regulations apply to the following EU information systems:

- The Entry/Exit System (EES);
- The Visa Information System (VIS);
- The European Travel Information and Authorisation System (ETIAS);
- Eurodac;
- The Schengen Information System (SIS);
- The European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN).

Regulation 2019/818 also applies to Europol data to the extent of enabling them to be queried simultaneously alongside the EU information systems referred to. As regards personal scope, the Regulations apply to persons whose personal data may be processed in the EU information systems referred to and/or in the Europol database.

In order to mitigate interference into the rights and freedoms of the persons concerned, the Regulations include several safeguards, e.g.:

- Full access to data contained in the EU information systems that is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences, beyond access to identity data or travel document data held in the CIR, will continue to be governed by the applicable legal instruments;

- Authorised end-users cannot make adverse decisions for the individual concerned solely on the basis of the simple occurrence of a match-flag.
- Provisions regulate the log-keeping of queries, the obligations to (principally) inform individuals whether links to their person have been established, penalties for misuse of data, and liability.
- A web portal will be established for the purpose of facilitating the exercise of the rights of access to, rectification, erasure, and restriction of processing of personal data.

The web portal will be developed by the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). The Agency will also be responsible for the development of the interoperability components, the technical management of the central infrastructure of the interoperability components, data quality standards, etc.

The establishment of interoperability was hotly debated in the runup to the legal framework. In particular, data protection experts took a critical stance (see eucrim 1/2019, pp. 26-27). Despite this criticism and before the adopted legal framework becomes operational, Statewatch has reported that the EU is already thinking of making customs information systems interoperable with EU Information Systems in Justice and Home Affairs, e.g., the SIS. The working groups at the EU level will further explore the potential added value of cross-checking relevant goods and persons' data between customs and JHA databases.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union