EDPS Further Critical to Interoperability

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

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

ISSN: 1862-6947
https://eucrim.eu

On 16 April 2018, the EDPS presented his concerns on the recent Commission's legislative proposals on establishing a framework to ensure interoperability between existing and future EU information systems (see eucrim 4/2017, pp. 174-175). The EDPS' contribution (Opinion 4/2018) follows up the reflection paper issued in November 2017, in which the EDPS already eyed the plans of the EU institutions on interoperability.

Interoperability is defined as the ability of the EU's large-scale IT systems, such as the Schengen Information System, the Visa Information System, and Eurodac to exchange data and to enable information sharing. The EDPS' opinion of 16 April 2018 contains numerous general and specific recommendations for the proposed legislation.

In essence, the EDPS acknowledges the need for information sharing in order to manage current challenges, such as migration, terrorism, and cross-border crime. The EDPS points out, however, that the current plans would considerably alter the structure and operation of the IT systems. Interoperability would not only lead to purely technical changes but mark a "point of no return", according to the EDPS, with significant, complex effects to the interpretation of fundamental legal principles traditionally applicable in this area. As a consequence, the EDPS calls on the Commission and the EU legislators to engage in a wider debate on the future of information exchange in the EU, the governance of interoperable databases, and the safeguarding of fundamental rights (see also the press release EDPS/2018/04).

The EDPS further emphasizes that the current plans go beyond being a technical tool to (only) facilitate the use of the EU's information systems, since the proposal introduces new possibilities to access and use the stored data in order to combat identity fraud, facilitate identity checks, and streamline access to non-law enforcement information systems (such as those initially created for immigration purposes) by law enforcement authorities. A new central database would store a huge amount of personal data, including biometric data. A data breach could therefore harm a very large number of individuals, and such database could become a dangerous tool for fundamental rights. In addition, allowing law enforcement authorities to routinely access information not originally collected for law enforcement purposes has serious implications on the protection of fundamental rights and principles, in particular the purpose limitation principle.

Against this background, the EDPS recommends, *inter alia*, the following:

- Building the central database upon strong legal, technical, and organizational safeguards, clearly defining its purpose, and setting the conditions and modalities for its use;
- Clearly identifying and further assessing the problem of identity fraud among third-country nationals in order to make the legislation appropriate and proportionate;

- Regulating more strictly and precisely the access and use of data in cases of identity checks;
- Taking into account fundamental data protection principles, e.g. purpose limitation, during all stages of implementation of the legislation;
- Introducing the principles of data protection by design and by default.

The EDPS opinion is flanked by other opinions, such as those presented by the Article 29 Data Protection Working Party and by the Fundamental Rights Agency at nearly the same time.

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