PRESS RELEASE

EDPS/2018/04

Brussels, 16 April 2018

EDPS calls for wider debate on the future of information sharing in the EU

The EU needs a **smarter approach** to information sharing in order to address challenges relating to security and border management. **Interoperability**, the process of enabling large-scale EU databases to communicate and exchange information, might prove a useful tool, but it is also likely to have profound legal and societal consequences, the European Data Protection Supervisor (EDPS) said today, as he published his Opinion on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems. The Opinion follows a reflection paper published by the EDPS on interoperability on 17 November 2017.

Giovanni Buttarelli, EDPS, said: "*Competent authorities across the EU must be able to share information in order to manage current **migratory challenges** and **terrorist and crime-related issues**. Interoperability, implemented in a well-considered manner and in full compliance with fundamental rights, could prove useful in facilitating this. However, in their current form, the Commission's Proposals would alter the structure and operation of the EU's existing IT databases and change the way in which **fundamental legal principles** in this area have traditionally been interpreted. As the precise implications of this for the **rights and freedoms of individuals** require more clarity, **wider debate** on the future of information exchange in the EU, the governance of interoperable databases and the safeguarding of fundamental rights is needed.*"

The EU operates several large-scale IT databases, used by the competent public authorities in the Member States to manage issues relating to **migration, asylum and security** in the EU. Interoperability could help public authorities to manage these issues by facilitating the exchange of data held within the databases.

However, the current Proposals go further than this. For example, they would allow public authorities to access and use the data stored in EU IT systems for investigations relating to identity fraud and identity checks, and provide for the streamlining of law enforcement access to databases that do not contain law enforcement information. The EDPS acknowledges that law enforcement authorities need access to the best possible tools so that they are able to quickly identify the perpetrators of terrorist acts and other serious crimes. However, he also notes that allowing law enforcement authorities to routinely access information not originally collected for law enforcement purposes has implications for the protection of fundamental rights.

Of particular concern to the EDPS is the creation of a centralised database containing information about millions of non-EU citizens, including their biometric data. The scale of the database and the nature of the data to be stored within it mean that a data breach could harm a very large number of people. With this in mind, it is essential that **strict and appropriate legal, technical and organisational safeguards** are built into any database, and that particular attention is given to defining its purpose and conditions of use.

Both in legal and technical terms, the Proposals add another layer of **complexity** to existing and future EU databases with unclear implications for data protection and other fundamental rights and freedoms, as well as for the governance and supervision of the databases. Taking these uncertainties into account, the **EDPS calls for wider debate** on this issue before considering further steps in the implementation of the Commission's Proposals on interoperability.

Background information

The rules for data protection in the EU institutions, as well as the duties of the European Data Protection Supervisor (EDPS), are set out in **Regulation (EC) No 45/2001**. The EDPS is a relatively new but increasingly influential independent supervisory authority with responsibility for monitoring the processing of personal data by the EU institutions and bodies, advising on policies and legislation that affect privacy and cooperating with similar authorities to ensure consistent data protection.

Giovanni Buttarelli (EDPS) and **Wojciech Wiewiórowski** (Assistant EDPS) are the members of the institution, appointed by a joint decision of the European Parliament and the Council. Assigned for a five year term, they took office on 4 December 2014.

Large-scale IT systems: databases created by the EU are considered to be large-scale according to the number of people using the system for different purposes, the amount of data collected, stored, accessed, manipulated and the number of connections between components, among other things. SIS II, VIS and Eurodac are three examples of large-scale IT systems in the area of border and police control.

Personal information or data: any information relating to an identified or identifiable natural (living) person. Examples include names, dates of birth, photographs, video footage, email addresses and telephone numbers. Other details such as IP addresses and communications content - related to or provided by end-users of communications services - are also considered as personal data.

Processing of personal data: According to Article 2(b) of Regulation (EC) No 45/2001, processing of personal data refers to "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." See the glossary on the EDPS website.

EU Data Protection Reform package:

On 25 January 2012, the European Commission adopted its reform package, comprising two legislative proposals:

- a general Regulation on data protection which was adopted on 24 May 2016, applicable as of 25 May 2018; and
- a specific Directive on data protection in the area of police and justice, adopted on 5 May 2016, applicable as of 6 May 2018.

The official texts of the Regulation and the Directive are now recognised as law across the European Union (EU). Member States have two years to ensure that they are fully implementable in their countries by May 2018.

The European Data Protection Supervisor (EDPS) is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. He does so by:

- monitoring the EU administration's processing of personal data;
- advising on policies and legislation that affect privacy;
- cooperating with similar authorities to ensure consistent data protection.

The EDPS Opinion is available on the EDPS website. Questions can be directed to:
press@edps.europa.eu
EDPS - The European guardian of data protection
www.edps.europa.eu
Follow us on Twitter: @EU_EDPS