



PRESS RELEASE

EDPS/2018/09

Brussels, 07 November 2019

EDPS calls for a pragmatic and balanced approach in the fight against crime

In a world transformed by **new technologies**, it is vital to ensure that law enforcement and judicial authorities have access to the necessary information and tools that are effective in the **fight against terrorism** and other **crimes**. However, any initiative in this field must fully respect the EU Charter of **Fundamental Rights** and the EU **data protection framework**, the Assistant European Data Protection Supervisor (EDPS) said today, as he published his [Opinion](#) on a new EU legal framework for gathering electronic evidence (e-evidence) in cross-border cases.

Wojciech Wiewiórowski, Assistant EDPS, said: *“New technologies have opened up new avenues for cross-border criminal activity across national borders. Evidence of criminal activity is now, in many cases, electronic, and not always easy for the competent authorities to access, due to limitations based on the traditional concepts of geographical jurisdictions. Ensuring EU authorities have effective and efficient means to access information stored in another State is essential to the security of the European Union. However, it cannot come at the expense of the rights and freedoms we enjoy as EU citizens. A balance must be found which provides for greater **EU security** without compromising fundamental rights and data protection principles.”*

Law enforcement authorities are increasingly faced with *cross-border situations*, where the information they need is stored electronically in another State. The Commission’s Proposals on e-evidence, published in April 2018, would introduce two new types of binding orders for criminal proceedings, allowing for **access to data stored by service providers** that may serve as evidence (Production Orders), or for the **preservation of this data by service providers in anticipation of subsequent requests** for access (Preservation Orders). It would streamline procedures within the EU, facilitating and accelerating access to data cross-border.

Today’s EDPS Opinion on e-evidence aims to provide the EU legislator with new input on the 2018 Proposals. In particular, it focuses on the need to ensure that **all necessary safeguards** are in place. This includes providing for the **increased involvement of the judicial authorities in the enforcing Member State** in the process of gathering cross-border electronic evidence.

In addition, the EDPS calls for **clearer definitions of data categories** in the proposed Regulation. This includes ensuring that they are consistent with existing definitions of data categories in EU law. The balance between the types of offences for which Production Orders could be issued and the categories of data concerned must also be reassessed, taking into account case law issued by the Court of Justice of the EU.

Since their publication, the Council has adopted general approaches on the Proposals and the European Parliament has issued several working documents. Related developments have also taken place at international level, including the launch of negotiations with the United States on cross-border access to e-evidence, as well as work in the Council of Europe on a Second Additional Protocol to the Cybercrime Convention. The EDPS has consistently supported the objectives of streamlining procedures and speeding up access to e-evidence, providing constructive advice to put in place sustainable arrangements with non-EU countries in his Opinions on the [negotiating mandate for an EU-US agreement on cross-border access to e-evidence](#) and on the [Budapest Cybercrime Convention](#).

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 the new [Regulation \(EU\) 2018/1725](#). These rules replace those set out in [Regulation \(EC\) No 45/2001](#). The EDPS is an 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. Our mission is also to raise awareness on risks and protect people's rights and freedoms when their personal data is processed.

Wojciech Wiewiórowski (Assistant EDPS), was appointed by a joint decision of the European Parliament and the Council on 4 December 2014 to serve a five-year term.

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.

Privacy: the right of an individual to be left alone and in control of information about his or herself. The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and the European Charter of Fundamental Rights (Article 7). The Charter also contains an explicit right to the protection of personal data (Article 8).

Processing of personal data: According to Article 4(1) of Regulation (EU) No 679/2016, processing of personal data refers to "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." See the [glossary](#) on the EDPS website.

The European Data Protection Supervisor (EDPS) is the independent supervisory authority for the protection of 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;
- monitoring and advising technological developments on policies and legislation that affect privacy and personal data protection;
- carrying out investigations in the form of data protection audits/inspections;
- cooperating with other supervisory authorities to ensure consistency in the protection of personal.

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](#)