



## EDPS: Enforcing EU data protection law essential for rebuilding trust between EU-US

The strict **enforcement** of existing **European data protection laws** is an essential element for **restoring trust** between the EU and the USA said the European Data Protection Supervisor (EDPS) today.

Peter Hustinx, EDPS, said: "*The rights of EU citizens to the protection of their privacy and personal information are enshrined in EU law. The mass surveillance of EU citizens by US and other intelligence agencies disregards these rights. As well as supporting a privacy act in the USA, Europe must insist on the strict enforcement of existing EU legislation, promote international privacy standards and swiftly adopt the reform of the EU data protection Regulation. A concerted effort to restore trust is required.*"

In his Opinion on the Commission Communications on **Rebuilding Trust in EU-US Data Flows** and on **the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU**, the EDPS said that measures must include the effective application and enforcement of the instruments regulating international transfers between the EU and the USA, in particular the existing Safe Harbour principles.

In addition, the reformed EU rules on data protection should provide for **clarity and consistency**, particularly in terms of addressing issues such as the conditions for data **transfers**, processing personal information for **law enforcement purposes** and **conflicts in international law**. It is, therefore, essential that progress is made **quickly** to thwart the attempts serving political and economic interests to **restrict** the fundamental rights to privacy and data protection.

The large-scale **monitoring** of users' communications is **contrary** to EU data protection legislation as well as the EU Charter of Fundamental Rights. In a democratic society, users should be **certain** that their **rights to privacy, confidentiality of their communications and protection of their personal information** are respected. Any exceptions or restrictions to fundamental rights for national security purposes should only be permissible if they are strictly **necessary, proportionate and in line with European case law**.

It is essential that fundamental rights are enforced through **existing legislation** as well as **stronger** laws and agreements in **future** in order to restore the **confidence** that has been seriously undermined by the various surveillance scandals. In a **democratic society**, intelligence activities should always respect the **rule of law** and the principles of necessity and proportionality.

## **Background information**

Privacy and data protection are fundamental rights in the EU. Data protection is a fundamental right, protected by European law and enshrined in Article 8 of the Charter of Fundamental Rights of the European Union.

More specifically, the rules for data protection in the EU - as well as the duties of the EDPS - are set out in [\*\*Regulation \(EC\) No 45/2001\*\*](#). One of the duties of the EDPS is to advise the European Commission, the European Parliament and the Council on proposals for new legislation and a wide range of other issues that have an impact on data protection. Furthermore, EU institutions and bodies processing personal data presenting specific risks to the rights and freedoms of individuals ('data subjects') are subject to prior-checking by the EDPS.

**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).

**Safe Harbour Principles:** These are a set of privacy and data protection principles that, together with a set of frequently asked questions (FAQs) providing guidance for the implementation of the principles, have been considered by the European Commission to provide an adequate level of protection. These principles were issued by the Government of the United States on 21 July 2000.

US organisations can claim that they comply with this framework. They should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) - under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce - or to the jurisdiction of another statutory body that will ensure compliance with the principles implemented in accordance with the FAQs. See also: [Adequacy decision](#) in the EDPS glossary and the Article 29 Working Party [website](#).

For more information on the EU data protection reform, we refer you to a [dedicated section](#) on the EDPS website.

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. For more information: [press@edps.europa.eu](mailto:press@edps.europa.eu)

**EDPS - The European guardian of data protection**

[www.edps.europa.eu](http://www.edps.europa.eu)



Follow us on Twitter: [@EU\\_EDPS](#)