EUROPEAN DATA PROTECTION SUPERVISOR

PRESS RELEASE

EDPS/2013/06

Brussels, 17 June 2013

Credible cyber security strategy in the EU needs to be built on privacy and trust

Cyber security is not an excuse for the **unlimited** monitoring and analysis of the personal information of individuals, said the European Data Protection Supervisor (EDPS) today following the publication of his **opinion** on the **EU's strategy on cyber security**. While there is a welcome acknowledgement of the importance of data protection principles for a robust cyber security policy, the strategy is **not clear** on how these principles will be applied in practice to reinforce the security of individuals, industry, governments and other organisations.

Peter Hustinx, EDPS, said: "*There is no security without privacy. So I am delighted that the EU strategy recognises that it is not a case of privacy versus cyber security but rather **privacy** and **data protection** are **guiding principles** for it. However, the ambitions of the strategy are not reflected in how it will be implemented. We acknowledge that cyber security issues have to be addressed at an international level through international standards and cooperation. Nevertheless, if the EU wants to cooperate with other countries, including the USA, on cyber security, it must necessarily be on the **basis** of **mutual trust** and **respect for fundamental rights**, a foundation which currently appears compromised."*

The overall aim of the EU strategy is to make the use of the **internet** and any network and information system connected to it, **safer** by enabling organisations in the EU countries to prevent and respond to cyber disruptions and attacks. The result would be to **foster trust** in individuals and organisations using the internet. However, the Commission Communication fails to take due account of the role of data protection law and of current **EU proposals** in promoting cyber security, such as the proposed Data Protection Regulation and the eTrust Regulation, among others. It also does not take into account the importance of factoring in protection at the inception of any system that contributes to cyber security - **privacy by design** - as a foundation for building trust. The result is that the strategy is not as effective and comprehensive as the Commission intends it to be.

While measures to ensure cyber security may require the analysis of some personal information of individuals, for instance IP addresses that can be traced back to specific individuals, cyber security can play a **fundamental role** in ensuring the protection of privacy and data protection rights in the online environment, provided the processing of this data is **proportionate**, **necessary** and **lawful**.

National data protection authorities (DPAs) play a **significant role** in ensuring that an appropriate level of security is applied to the processing of personal information, including on the internet and through network and information systems, and in **raising awareness** of the rules that apply to individuals and organisations in EU countries. Moreover, DPAs must be notified of any new operation by an organisation that involves the processing of personal information and of data breaches. Agencies such as Europol, ENISA and others listed in the strategy also need to liaise with them in the performance of their tasks. Although this is not reflected in the strategy, their role in contributing to cyber security must be acknowledged.

Background information

On 7 February 2013, the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy adopted a **Joint Communication** to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a **"Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace".**

On the same date, the Commission adopted a proposal for a **Directive** of the European Parliament and of the Council **concerning measures to ensure a high common level of network and information security across the Union**. This Proposal was sent to the EDPS for consultation on 7 February 2013.

Privacy and data protection are fundamental rights in the EU. Under the Data Protection **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. If in the opinion of the EDPS, the notified processing may involve a breach of any provision of the Regulation, he shall make proposals to avoid such a breach.

Personal information or data: any information relating to an identified or identifiable natural (living) person. Examples include names, dates of birth, photographs, e-mail addresses and telephone numbers. Other details such as health data, data used for evaluation purposes and traffic data on the use of telephone, email or internet are also considered 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).

Privacy by design: to build privacy and data protection into the design and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles.

Purpose limitation: personal information may only be collected for specified, explicit and legitimate purposes. Once it is collected, it may not be further processed in a way that is incompatible with those purposes. The principle is designed to protect individuals by limiting the use of their information to pre-defined purposes, except under strict conditions and with appropriate safeguards.

Data breach: any personal data kept by an organisation (usually a telecoms provider) that is (accidentally or deliberately) lost, stolen, destroyed, changed, accessed or disclosed.

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.
