PRESS RELEASE

EDPS/2016/08

Brussels, 21 March 2016

EDPS guide to securing information and business continuity

In his **Guidance** on *Information Security Risk Management* published today, the European Data Protection Supervisor (EDPS) advises EU institutions on how to ensure a secure and trustworthy digital environment for the information that is essential for the functioning of their services.

Wojciech Wiewiórowski, Assistant Supervisor, said: *"The security of personal data is a legal requirement, but it is also necessary in the interests of organisations that rely on the use of information for their daily business. It is essential that they maintain appropriate security levels for information since the value and efficiency of their work is so dependent upon it. I urge the hierarchies in the EU institutions to engage in the tailored development and use of information security risk management processes to address the specific needs of their organisation."*

Different organisations are exposed to different security risks to the information they use, so state-of-the-art risk assessment methods provide an efficient way of identifying the appropriate solutions for the specific risks faced by an institution and can justify the use of financial and IT resources to develop those solutions.

Information security risk management for personal data requires specialist expertise in information and IT security as well as data protection. Data Protection Officers (DPOs) should support information and IT security experts in the development of these processes.

Technical security solutions alone cannot solve the issue of information security. An organisation's hierarchy is ultimately responsible for the enforcement of decisions that affect applications and the IT infrastructures that support them. Management has to support the development and implementation of policies and to mobilise the resources required to counter the information risks that an organisation faces.

While this Guidance document is primarily aimed at the EU institutions, anyone interested in data protection might find it useful; the Data Protection Regulation applicable to the EU institutions (Regulation (EC) No 45/2001) is similar in many respects to the data protection Directive (EC) 95/46), which is implemented into the national laws of EU Member States, as well as in Iceland, Liechtenstein and Norway.

This Guidance will continue to be useful with the entry into force of the new General Data Protection Regulation which maintains the principle of risk management for security and strengthens overall responsibility and governance requirements, by explicitly introducing the principle of **accountability** in respecting data protection obligations.

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 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.

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 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.

Article 22 of Regulation 45/2001: contains the legal requirement for EU institutions to mitigate the risks when processing personal data;

- In their analysis, Information Security Risk Management must also cover information security risks affecting personal data;
- From their analysis, a set of suitable security measures may be defined and implemented.

Security measures protecting personal data cannot be defined generically since they must come from the Information Security Risk Management process, which takes into account the specific context in which personal data is processed.

Information Security experts specialise in developing ways to protect information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction.

IT Security experts specialise in developing ways to protect information using various forms of technology to create, store, use and exchange such information against unauthorised access, misuse, malfunction, modification, destruction, or improper disclosure.

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 Guidance document 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