

What do data protection officers have to deal with in 2011?

Challenges for today and tomorrow at
the European Commission

Philippe Renaudière, Data Protection
Officer

Structure of the presentation

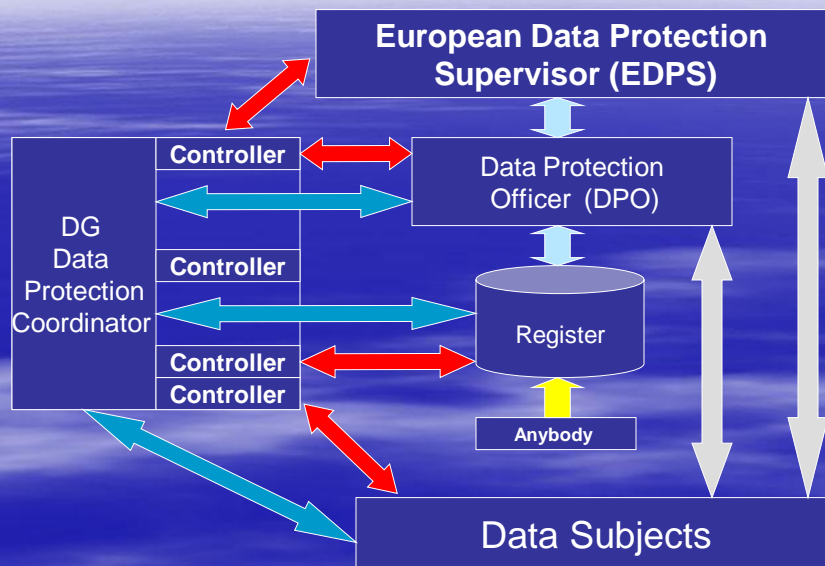
- Current situation/level of compliance
- Challenges:
 - Review of Directive in 2011
 - No IT Security? NO Privacy!
 - EU-Institutions going global!

Personal Data Protection in the Commission – Compliance

■ In a nutshell , compliance means that...

- processing operations on personal data must respect the principles of Regulation (EC) 45/2001
- (prior-)Information to Data Subjects has been ensured
- (prior-)Notification to Data Protection Officer (+prior-checking by EDPS where appropriate)

Interaction between Main Players



Current level of compliance

- 94 % compliance rate (886 processing operations identified /834 notified)
- prior-checks almost completed
- privacy statements available
- "corporate" and model notifications available
- web site, staff training , documentation, network of correspondents ,dedicated IT system, etc in place

Communication of the Commission COM(2010) 609

*'A comprehensive approach on
personal data protection in the
European Union'*

Main policy objectives

- Address the impact of **new technologies** and **modernise** the current framework
- Improve the **clarity and coherence** of the EU legal framework for personal data protection so to ensure a **high level of protection** throughout all Union policies
- Provide a stronger institutional arrangement for the **effective enforcement** of data protection rules

Main elements for a reform

1. Strengthening **individuals' rights**
2. Enhancing the **internal market** dimension
3. Reinforcing **data controllers' responsibility**
4. Revising the rules on **police and judicial cooperation in criminal matters**
5. The **global dimension** of data protection
6. Better **enforcement** of data protection rules

Strengthening the individuals' rights

1. Ensuring appropriate protection for individuals in all circumstances
2. Increasing transparency for data subjects
3. Enhancing control over one's own data
4. Raising awareness
5. Ensuring informed and free consent
6. Protecting sensitive data
7. Making remedies and sanctions more effective

Enhancing the internal market dimension

1. Increasing legal certainty and providing a level playing field for data controllers
2. Reducing the administrative burden
3. Clarifying the rules on applicable law and Member States' responsibility
4. Enhancing data controllers' responsibility
5. Encouraging self-regulatory initiatives and exploring EU certification schemes

The global dimension of data protection

1. Clarifying and simplifying the rules for international data transfers, including the “adequacy procedure”
2. Promoting universal principles

Data Protection and Information Security

- Regulation 45/2001 art 22:
 - 1. Having regard to the state of the art and the cost of their implementation, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.
 - Such measures shall be taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing.

Data Protection and Information Security

- Reg 45/2001 art 35
- The Community institutions and bodies shall take appropriate technical and organisational measures to safeguard the secure use of the telecommunications networks and terminal equipment, if necessary in conjunction with the providers of publicly available telecommunications services or the providers of public telecommunications networks. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

Controlling specific security measures in each processing operation

- Notification of ALL processing operations to the Data Protection Officer
- Notification to contain:
"a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 22 to ensure security of processing"

Cooperation with in-house IT Department

- **COMMISSION DECISION**
of 16 August 2006 C(2006) 3602 concerning the
security of information systems used by the European
Commission

"This Decision provides for security measures for the protection of the Commission's information systems and the information processed therein against threats to the availability, integrity and confidentiality of these systems and information"

(the measures) must be proportionate to the danger in terms of costs and functional or technical restrictions.

Cooperation with in-house IT Department

Article 5

Protection of personal data

The information systems security policy must guarantee a high level of protection of personal data and the processing thereof in accordance with Regulation (EC) No

45/2001, particularly Articles 21 to 23 and 35 to 37.

Article 11

Any new information system must from the design stage take account of the information systems security policy.

Training and Information of Staff

Notification of Data Breaches

Reform of e-privacy directive 2002/58:

- Directive 2009/136 of 25/11/2009
- Extension to other sectors: recital 59
- "Pending a review to be carried out by the Commission of all relevant Community legislation in this field, the Commission, in consultation with the European Data Protection Supervisor, should take appropriate steps without delay to encourage the application throughout the Community of the principles embodied in the data breach notification rules contained in Directive 2002/58/EC (Directive on privacy and electronic communications), regardless of the sector, or the type, of data concerned."

EU-Institutions going global!

- International transfers of data from Commission's data bases
- art 9 Regulation 45/2001: similar to directive but:
- NO BCR
- NO Safe Harbour
- NO sets of Contractual clauses...

Thank you for your attention!

- for more information, visit:
<http://ec.europa.eu/dataprotectionofficer/index.cfm>