

# Panel Discussion: Regulating Privacy

Philippe Renaudière  
DPO  
European Commission  
ICOMP, Brussels,  
27/04/2009



# Interaction between DP Rules and Privacy Practices

- Role of the Data Protection Officer
- Incentive for companies to improve their privacy practices?
- How to make consumers more aware of the company's privacy practices?
- Third Party Certification?

# Role and Status of the Data Protection Officer

- Legal Framework: Directive 95/46 (for Member States) and Regulation 45/2001 (for EU Institutions)
- Practice at the European Commission

# DIRECTIVE 95/46

(art 18)

DPO ( Personal Data Protection Official\*)

mentioned in the context of the simplification or exemption from notification to the supervisory authority

\*"Détaché à la Protection des Données à caractère personnel"

# DIRECTIVE 95/46 Art 18

- Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions: (...)
- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
  - - for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
  - - for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

## Countries having opted for a DPO in their legislation

- Germany
- France
- Sweden
- The Netherlands

# DIRECTIVE 95/46

- DPO responsible in particular:
  - for ensuring in an independent manner the internal application of the provisions of the national legislation
  - keeping the register of processing operation containing the informations referred to in art 21 (2)  
"thereby ensuring that rights and freedoms unlikely to be affected"

# REGULATION 45/2001

- **Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data**

*Official Journal L 008 , 12/01/2001 P. 0001 - 0022*

- **Art 24**  
- "Each Community institution and body to appoint "at least one DPO (Data Protection Officer – Délégué à la Protection des Données)

**By now 39 institutions and bodies have appointed their DPO**

# REGULATION 45/2001

## Tasks of the DPO

- Ensuring that controllers and data subjects are informed of their rights and obligations
- co-operating with EDPS
- ensuring in an independent manner the internal application of the regulation
- keeping a register of processing operations
- notifying to EDPS processing operations likely to present specific risks (art 27)

## **REGULATION 45/2001**

### **Tasks of the DPO (continued)**

---

"this person shall thus ensure that the rights and freedoms are unlikely to be adversely affected"

# REGULATION 45/2001

## Tasks of the DPO: information

Information of data subjects and controllers on their rights and obligations:

- website (Intracomm)
- training
- individual consultations
- sensitisation and information campaigns for staff and management

# REGULATION 45/2001

## Tasks of the DPO: notifications

- Notification (art 25)
- controller to give Prior Notice to DPO
- notification contains: name/ address of controller, purpose, category of data subjects and data, recipients, time limit for blocking and erasure, proposed transfers to 3rd countries/international organisations, description of security measures

# REGULATION 45/2001

## Tasks of the DPO: Register

- DPO to keep a register of notified processing operations (art 26)
- Register contains "at least" same information as in notification to DPO, except security measures
- Register "may be inspected by any person directly or indirectly through EDPS"
- Situation in the Commission: Register is on line since 28 January 2007:

<http://ec.europa.eu/dataprotectionofficer/index.cfm>

# REGULATION 45/2001

## Tasks of the DPO: Prior-Check EDPS

- Notifications of processing operations to the EDPS for prior-checking (art 27)
  - health, suspected offences, offences, criminal convictions , security measures
  - evaluation of data subject's ability, efficiency and conduct
  - linkages between data processed for different purposes
  - exclusion individuals from right, benefit, contract

# REGULATION 45/2001

## Tasks of the DPO: Prior-Check EDPS

- Notifications of processing operations to the EDPS for prior-checking (art 27):
  - in general processing operations likely to present specific risks by virtue of their nature, scope or purpose
  - in case of doubt, consultation of the EDPS on the need for a prior-check

# REGULATION 45/2001

## Status of DPO

- Selected on the basis of his/her professional qualities and in particular expert knowledge on DP (24.2)
- Selection may not result in conflict of interest (important for part-time DPO) (24.3)
- appointed for a term of 2-5 years, eligible for re-appointment for a maximum total term of 10 years
- can only be dismissed with consent of EDPS (24.4)

# REGULATION 45/2001

## Status of DPO

- DPO registered with the EDPS after his/her appointment
- The institution to provide the DPO with the "staff and resources necessary to carry out his/her duties" (24.6)
- "With respect to the performance of his/her duties, the DPO may not receive any instructions"

# REGULATION 45/2001

## Further implementation rules

- to be adopted by each institution (Commission: June 2008)
- deal with tasks duties and powers of the DPO:
  - recommendations and advices
  - investigations on initiative or at the request of institution, the controller, the Staff Committee, and report back
  - may be consulted by anybody "without going through official channels"

# REGULATION 45/2001

## Further implementation rules

- no one to suffer prejudice for having reported a breach of the regulation to the DPO
- Controller to assist DPO, and give information in answer to his/her questions
- DPO shall have access at all times to the data forming the subject -matter of processing operations and to all offices, data protection installations and data carriers
- professional secrecy of DPO and his staff

# REGULATION 45/2001

## Position of DPO

- No enforcement power, but
  - if complaint to EDPS, DPO will be involved
  - possibility to bring any failure to comply with the regulation to the attention of the appointing authority for possible disciplinary action; in practice, the DPO receives and investigates complaints
  - non-compliance with DP regulation identified as a management risk

# The Challenges

- Compliance
- Integration
- Transparency
  
- Security
  
- Simplification

# The Way Ahead

## Data Protection Mainstreaming

- a 3 Pillar Action Plan (legal, organisation, people)
- DP recognised in Internal Control Standard, Audit and Risk Management
- DP recognised in IT development (including PETs)
- HR Dimension

# Data Protection Mainstreaming

- Identifying the data that needs to be protected
- Cross department analysis
- Strengthening the weakest links
- Simplification/Rationalisation
- Transparency (Internal and External)

# Conclusion

---

- DPO: a good example of self – compliance: reduces intervention from external supervisory body
- Helps developing a culture of data protection within the organisation
- Independence is key, but constructive attitude is equally important
- DPO to provide solutions

# Thank you for your attention!

for additional information:

<http://ec.europa.eu/dataprotectionofficer/index.cfm>

Or E-mail

[philippe.renaudiere@ec.europa.eu](mailto:philippe.renaudiere@ec.europa.eu)

+ Position Paper of the EDPS on the Role of Data Protection Officers (November 2005)

[http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28\\_DPO\\_paper\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28_DPO_paper_EN.pdf)