The DPO and Accountability

DPO meeting
08 May 2015

The EDPS Strategy
2015-2019

Leading by example
What is meant by “Accountability”

- Shift from formal “responsibility” in current rules to enhanced responsibility

- Article 29 WP 173, Opinion 3/2010 of 13.7.10
  - expressly embed principle of accountability in the law, to ensure that data protection requirements translate into effective mechanisms that deliver real protection
Essential elements

- **To whom?** Accountability is towards DPAs, but also towards individuals.
- **How?** Current system of prior notification & prior checking will be replaced by *ex-post control*. In parallel, DPAs powers to enforce & to impose sanctions for non-compliance would be increased.
- **When?** Does not come only at the end. A proactive obligation to develop adequate data management in practice, considering entire life cycle.
  - Towards better data management in practice
  - Part of good administration
Accountability under the Reform

Draft Regulation, Article 22

1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

2. The measures provided for in paragraph 1 shall in particular include: (….)

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.
Examples of appropriate measures

- Internal procedures and written policies & procedures to be communicated to DS (Art. 11 & 12)
- Documentation (art 28)
- Implement security requirements (art 30)
- DPIA impact assessment (art 33)
- Designation of a DPO (art 35.1)
- Data protection by Design / Default (art 23)
- Verification procedures by internal or external audits (Art. 22(3))

➤ Develop a culture of data protection
Benefits of Accountability

• More effective compliance in practice
• Proactive data protection
• Reallocation of DPA resources
• Forward planning, risk management
• Removal of costs, especially notifications
DPO Network proposals on accountability  
(in relation to the review of Regulation 45/2001)

• Obligations of the controller to be more specified in relation to the different layers of controllership:
  • Controller= institution
  • Delegated controller= HoU
  • Delegates of delegated controllers= person actually carrying out the processing operation

• Are these specifications needed in a Regulation?
Role of the DPO

Existing powers:

- Investigation (also on own initiative)
- Access to personal data in all premises and on all carriers
Role of the DPO

Institution’s best partner in accountability

- **Ensure**
  - Help define a data protection strategy
  - Train key players in-house
  - Raise awareness of higher management

- **Demonstrate**
  - Keep the register (but simplified?)
  - Keep a repository of data protection complaints, transfers

- **Verify**
  - Set up mechanisms to keep register/policies/procedures/repository up to date
  - Conduct internal data protection audits
Role of the DPO

Need for enforcement powers?

• Pros
  – Proximity
  – Autonomy

• Cons
  – Concentrated responsibility
  – Independence
In sum:

• Accountability = bureaucracy?
• Less work for DPA/ more for DPOs?
• Ready to jump now/ or need more time?
Your turn!

Share your concerns or ideas:

- Identify topics
- Split in groups
- Report
- What’s next?
Thank you!

For more information:

www.edps.europa.eu
edps@edps.europa.eu

@EU_EDPS

The EDPS Strategy
2015-2019

Leading by example