Archives and Data protection

What does EDPS expect from EU institutions?

Preliminary considerations

45th ICA/SIO annual meeting
Luisa Palla - EDPS
Brussels, 21 May 2019
What does EDPS expect from EU institutions?

EU context

Data protection and archiving

Towards compliance
EU context
Legal framework

Data Protection
Regulation (EU) 2018/1725

Archives
- Regulation (EEC, Euratom) 354/83
- Council Regulation (EC, Euratom) 1700/2003
- Council Regulation (EU) 2015/496
EU context
The players

European Data Protection Supervisor (EDPS)

Data Protection Officer (DPO)

Controller

Historical Archives

HAEU Florence
EU context
The EDPS

Supervise
EU institutions and bodies

Advise
the EU legislator

Monitor
technological developments

Cooperate
with other data protection authorities
- member & secretariat of EDPB

The EU’s independent data protection authority
Archiving in Regulation (EU) 2018/1725

Article 13

• Processing for archiving purposes ... shall be subject to appropriate safeguards, ... for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation ...

Recital 33

• Union institutions and bodies should provide for appropriate safeguards ... in Union law, which may include internal rules adopted by Union institutions and bodies in matters relating to their operation.
Principles, rights, obligations

- Fairness, lawfulness, transparency
- **Purpose limitation**
- **Data minimization**
- Data accuracy
- **Storage limitation**
- Integrity, confidentiality

**Accountability**

- **Transparency & information**
- **Access**
- **Rectification**
- **Erasure (right to be forgotten)**
- Restriction of processing
- Objection to processing
- Data portability
- Automated individual decision making

**Accountability** of the controller

- **Security** of processing
- Data protection ***by design and by default***
- Confidentiality of electronic communications
- Controllers – Processors

**Records** of processing operations

- DPIA, Prior consultation of EDPS
- **Cooperation with the EDPS**
- Notification of **personal data breaches** to EDPS and communication to the data subject
Archiving purposes: specificities

- Further processing not incompatible with initial purposes
- Longer storage permitted, with conditions
- Individuals’ rights: Union law (incl. internal rules) may provide for derogations (with conditions & safeguards)
Towards compliance (1)

**Embed data protection in policies & practices**
- establish internal rules to support defensible disposition and defensible preservation
- give clear information on derogations to individuals’ rights

**Risk assessment & balancing act**
- identify and evaluate potential risks and mitigation actions
- balance data protection - preservation and access to information

**Cooperate with DPOs and other relevant actors**
- share specific expertise
- aim at consistent approach
Towards compliance (2)

Focus on security measures

- secure elimination
- secure preservation
- access proportionate to potential risks

Document processing activities & approach to personal data handling

- demonstrate compliance
- documentation as basis for risk assessment

Common sense + think data protection!
Towards compliance (3)

Processing operations
• what personal data
• how (documentation)
• who (roles/responsibilities)

Identify, Review Comply

Data protection obligations
• accountability
• specific conditions

Identify, Assess, Implement, Review
Comply

Risks involved
• for individuals concerned
• for the controller
• risks of the processing

Identify, Assess, Handle, Review

Appropriate safeguards
• organisational measures
• technical measures
• contractual clauses

Identify, Assess, Implement, Review
thank you!

For more information:
www.edps.europa.eu
edps@edps.europa.eu