

Introduction to European Data Protection

1. Origins and Historical Context of Data Protection Law

- Rationale for data protection
- Human rights laws
- Early laws and regulations
- The need for a harmonized European approach
- The Treaty of Lisbon
- A modernized framework

2. European Union Institutions

- Council of Europe
- European Court of Human Rights
- European Parliament
- European Commission
- European Council
- Court of Justice of the European Union

3. Legislative Framework

- The Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data of 1981 (The CoE Convention)
- The EU Data Protection Directive (95/46/EC)
- The EU Directive on Privacy and Electronic Communications (2002/58/EC) (ePrivacy Directive) – as amended
- The EU Directive on Electronic Commerce (2000/31/EC)
- European data retention regimes
- The General Data Protection Regulation (GDPR) (EU) 2016/679 and related legislation

European Data Protection Law and Regulation

- 1. Data Protection Concepts
- Personal data
- Sensitive personal data

- Pseudonymous and anonymous data
- Processing
- Controller
- Processor
- Data subject

2. Territorial and Material Scope of the General Data Protection Regulation

- Establishment in the EU
- Non-establishment in the EU

3. Data Processing Principles

- Fairness and lawfulness
- Purpose limitation
- Proportionality
- Accuracy
- Storage limitation (retention)
- Integrity and confidentiality

4. Lawful Processing Criteria

- Consent
- Contractual necessity
- Legal obligation, vital interests and public interest
- Legitimate interests
- Special categories of processing

5. Information Provision Obligations

- Transparency principle
- Privacy notices
- Layered notices

6. Data Subjects' Rights

- Access
- Rectification

- Erasure and the right to be forgotten (RTBF)
- Restriction and objection
- Consent, including right of withdrawal
- Automated decision making, including profiling
- Data portability

Restrictions

7. Security of Personal Data

- Appropriate technical and organizational measures
 - a. protection mechanisms (encryption, access controls, etc.)
- Breach notification
 - a. Risk reporting requirements
- Vendor Management
- Data sharing

8. Accountability Requirements

- Responsibility of controllers and processors
 - a. joint controllers
- Data protection by design and by default
- Documentation and cooperation with regulators
- Data protection impact assessment (DPIA)
 - a. established criteria for conducting
 - Mandatory data protection officers
 - Auditing of privacy programs

9. International Data Transfers

- Rationale for prohibition

- Adequate jurisdiction
- Safe Harbor and Privacy Shield
- Standard Contractual Clauses
- Binding Corporate Rules (BCRs)
- Codes of Conduct and Certifications
- Derogations
- Transfer impact assessments (TIAs)

10. Supervision and enforcement

- Supervisory authorities and their powers
- The European Data Protection Board
- Role of the European Data Protection Supervisor (EDPS)

11. Consequences for GDPR violations

- Process and procedures
- Infringements and fines
- Class actions
- Data subject compensation

Compliance with European Data Protection Law and Regulation

1. Employment Relationship

- Legal basis for processing of employee data
- Storage of personnel records
- Workplace monitoring and data loss prevention
- EU Works councils
- Whistleblowing systems
- 'Bring your own device' (BYOD) programs

2. Surveillance Activities

- Surveillance by public authorities
- Interception of communications
- Closed-circuit television (CCTV)

- Geolocation
- Biometrics / facial recognition

3. Direct Marketing

- Telemarketing
- Direct marketing
- Online behavioural targeting

4. Internet Technology and Communications

- Cloud computing
- Web cookies
- Search engine marketing (SEM)
- Social networking services
- Artificial Intelligence (AI)

a. Machine Learning

b. Ethical Issues