European Privacy Certification

Outline of the Body of Knowledge for the Certified Information Privacy Professional/Europe (CIPP/E™)

I. Introduction to European Data Protection

A. Origins and Historical Context of Data Protection Law

1. Rationale for data protection
2. Human rights laws
3. Early laws and regulations
4. The need for a harmonised European approach
5. The Treaty of Lisbon
6. A modernised framework

B. European Union Institutions

1. Council of Europe
2. European Court of Human Rights
3. European Parliament
4. European Commission
5. European Council
6. European Court of Justice

C. Legislative Framework

1. The Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data of 1981 (The CoE Convention)
2. The EU Data Protection Directive (95/46/EC)
3. The EU Directive on Privacy and Electronic Communications (2002/58/EC) – as amended
4. The EU Directive on Electronic Commerce (2000/31/EC)
5. European data retention regimes
6. The General Data Protection Regulation (GDPR) and related legislation

II. European Data Protection Law and Regulation

A. Data Protection Concepts

1. Personal data
2. Sensitive personal data
3. Pseudonymous and anonymous data
4. Processing
5. Controller
6. Processor
7. Data subject

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

1. Establishment in the EU
2. Non-establishment in the EU

C. Data Processing Principles

1. Fairness and lawfulness
2. Purpose limitation
3. Proportionality
4. Accuracy
5. Storage limitation (retention)
6. Integrity and confidentiality

D. Lawful Processing Criteria

1. Consent
2. Contractual necessity
3. Legal obligation, vital interests and public interest
4. Legitimate interests
5. Special categories of processing

E. Information Provision Obligations

1. Transparency principle
2. Privacy notices
3. Layered notices

F. Data Subjects' Rights

1. Access
2. Rectification
3. Erasure and the right to be forgotten (RTBF)
4. Restriction and objection

Pease International Tradeport · 75 Rochester Avenue. Suite 4 · Portsmouth, NH 03801 USA ·
+ 1 603.427.9200 · certification@iapp.org

5. Consent, including right of withdrawal
6. Automated decision making, including profiling
7. Data portability
8. Restrictions

G. Security of Personal Data

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

H. Accountability Requirements

1. Responsibility of controllers and processors
   a. joint controllers
2. Data protection by design and by default
3. Documentation and cooperation with regulators
4. Data protection impact assessment
   a. established criteria for conducting
5. Mandatory data protection officers

I. International Data Transfers

1. Rationale for prohibition
2. Safe jurisdictions
3. Safe Harbor and Privacy Shield
4. Model contracts
5. Binding Corporate Rules (BCRs)
6. Codes of Conduct and Certifications
7. Derogations

J. Supervision and enforcement

1. Supervisory authorities and their powers
2. The European Data Protection Board
3. Role of the European Data Protection Supervisor (EDPS)

K. Consequences for GDPR violations

1. Process and procedures
2. Infringements and fines
3. Data subject compensation

III.Compliance with European Data Protection Law and Regulation

A. Employment Relationship

1. Legal basis for processing of employee data

2. Storage of personnel records
3. Workplace monitoring and data loss prevention
4. EU Works councils
5. Whistleblowing systems
6. 'Bring your own device' (BYOD) programs

B. Surveillance Activities

1. Surveillance by public authorities
2. Interception of communications
3. Closed-circuit television (CCTV)
4. Geolocation

C. Direct Marketing

1. Telemarketing
2. Direct marketing
3. Online behavioural targeting

D. Internet Technology and Communications

1. Cloud computing
2. Web cookies
3. Search engine marketing (SEM)
4. Social networking services