iapp

CIPP/E
BODY OF KNOWLEDGE

VERSION 1.3.1

EFFECTIVE DATE: 10/02/2023

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
   a. OECD Guidelines and the Council of Europe
   b. Convention 108
4. The need for a harmonized European approach
5. The Treaty of Lisbon
6. Convention 108+
7. Brexit

B. European Union Institutions

1. European Court of Human Rights
2. European Parliament
3. European Commission
4. European Council
5. Court of Justice of the European Union

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) (ePrivacy Directive) – as amended
4. The EU Directive on Electronic Commerce (2000/31/EC)

5. European data retention regimes
6. The General Data Protection Regulation (GDPR) (EU) 2016/679 and related legislation
   a. Relationship with other laws (Payment Services Directive 2, Data Governance Act, Regulation (EU) 2018/1725, etc.)
7. NIS Directive (2016) / NIS 2 Directive (2022)
8. EU Artificial Intelligence Act (2021)

II. European Data Protection Law and Regulation

A. Data Protection Concepts

1. Personal data
2. Sensitive personal data
   a. Special categories of personal data
3. Pseudonymous and anonymous data
4. Processing
5. Controller
6. Processor
   a. Guidelines 07/2020 on the concepts of controller and processor in the GDPR
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
   a. Guidelines 3/2018 on the territorial scope of the GDPR

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
   a. Guidelines 01/2022 on data subject rights - Right of access
2. Rectification
3. Erasure and the right to be forgotten (RTBF)
   a. Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR

4. Restriction and objection
5. Consent, including right of withdrawal
6. Automated decision making, including profiling
7. Data portability
8. Restrictions
    a. Guideline 10/2020 on restrictions under Article 23 GDPR

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
    b. Guidelines 01/2021 on Examples regarding Personal Data Breach Notification
    c. Guidelines 9/2022 on personal data breach notification under GDPR
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 (DPIA)
    a. established criteria for conducting
5. Mandatory data protection officers
6. Auditing of privacy programs

I. International Data Transfers

1. Rationale for prohibition
    a. Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR
2. Adequate jurisdictions
3. Safe Harbor, Privacy Shield, and the Transatlantic Data Privacy Framework
    a. Schrems decisions, implications of
4. Standard Contractual Clauses
5. Binding Corporate Rules (BCRs)
6. Codes of Conduct and Certifications
    a. Guidelines 04/2021 on codes of conduct as tools for transfers
7. Derogations
    a. Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679
8. Transfer impact assessments (TIAs)
    a. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

J. Supervision and enforcement

1. Supervisory authorities and their powers
    a. Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority
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. Class actions
4. 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)
   a. Guidelines 3/2019 on processing of personal data through video devices
4. Geolocation
5. Biometrics / facial recognition

C. Direct Marketing

1. Telemarketing
2. Direct marketing
3. Online behavioural targeting
   a. Guidelines 8/2020 on the targeting of social media users

D. Internet Technology and Communications

1. Cloud computing
2. Web cookies
3. Search engine marketing (SEM)
4. Social media platforms
   a. dark patterns
5. Artificial Intelligence (AI)
   a. machine learning
   b. ethical issues