Certified Information Privacy Professional (CIPP/E) + Certified Information Privacy Manager (CIPM)

Course Length: 4 days

Course Overview

CIPP/E: European Data Protection covers essential pan-European laws and regulations, as well as industry- standard best practices for corporate compliance. Those taking this course will gain an understanding of the European model for privacy enforcement, key privacy terminology and practical concepts concerning the protection of personal data and trans-border data flows. CIPM: Privacy Program Management is the how-to training on implementing a privacy program framework, managing the privacy program operational lifecycle and structuring a knowledgeable, high-performing privacy team. Those taking this course will learn the skills to manage privacy in an organization through process and technology - regardless of jurisdiction or industry.

Course Outline

1 - Data Protection Laws
- Introduces key European data protection laws and regulatory bodies, describing the evolution toward a harmonized legislative framework.

2 - Personal Data
- Defines and differentiates between types of data, including personal, anonymous, pseudo-anonymous and special categories.

3 - Controllers and Processors
- Describes the roles and relationships of controllers and processors.

4 - Processing Personal Data
- Defines data processing and GDPR processing principles, explains the application of the GDPR and outlines the legitimate bases for processing personal data.

5 - Information Provision
- Explains controller obligations for providing information about data processing activities to data subjects and supervisory authorities.

6 - Data Subjects' Rights
- Describes data subjects' rights, applications of rights and controller and processor obligations.

7 - Security of Processing
- Discusses considerations and duties of controllers and processors for ensuring security of personal data and providing notification of data breaches.

8 - Accountability
- Investigates accountability requirements, including data protection management systems, data protection impact assessments, privacy policies and the role of the data protection officer.

9 - Cross-Border Data Transfers
- Outlines options and obligations for transferring data outside the European Economic Area, including adequacy decisions and appropriate safeguards and derogations.

10 - Supervisions and Enforcement
- Describes the role, powers and procedures of supervisory authorities; the composition and tasks of the European Data Protection Board; the role of the European Data Protection Supervisor; and remedies, liabilities and penalties for non-compliance.

11 - Compliance
- Discusses the applications of European data protection law, legal bases and compliance requirements for processing personal data in practice, including employers processing employee data, surveillance, direct marketing, Internet technology and communications and outsourcing.

12 - Introduction to privacy program management
- Identifies privacy program management responsibilities, and describes the role of accountability in privacy program management.

13 - Privacy Governance
- Examines considerations for developing and implementing a privacy program, including the position of the privacy function within the organization, role of the DPO, program scope and charter, privacy strategy, support and ongoing involvement of key functions and privacy frameworks.

14 - Applicable Laws and Regulations
- Discusses the regulatory environment, common elements across jurisdictions and strategies for aligning compliance with organizational strategy.

15 - Data Assessments
- Relates practical processes for creating and using data inventories/maps, gap analyses, privacy assessments, privacy impact assessments, data protection impact assessments, and vendor assessments.

16 - Policies
- Describes common types of privacy-related policies, outlines components and offers strategies for implementation.

17 - Data Subject Rights
- Discusses operational considerations for communicating and ensuring data subject rights, including privacy notice, choice and consent, access and rectification, data portability, and erasure and the right to be forgotten.

18 - Training and Awareness
- Outlines strategies for developing and implementing privacy training and awareness programs.

19 - Protecting Personal Information
- Examines a holistic approach to protecting personal information through privacy by design.

20 - Data Breach Incident Plans
- Provides guidance on planning for and responding to a data security incident or breach.

21 - Measuring, Monitoring, and Auditing Program Performance
- Relates common practices for monitoring, measuring, analyzing and auditing privacy program performance.