



## International Association of Privacy Professionals (IAPP) CIPP

### Course Length:

2 days

### Overview

Founded in 2000, the IAPP is the world's largest and most comprehensive privacy resource with a mission to define, support and improve the Privacy profession globally. Every day, we access, share, manage and transfer data across companies, continents and the globe. Knowing the ins and outs of data protection requirements gives you the information you need to stay ahead of breaches—and help you advance your career.

The Principles of Data Protection in Europe training covers the essential pan-European and national data protection laws, as well as industry-standard best practices for compliance with these laws.

The General Data Protection Regulation (GDPR) takes effect in 2018 and CIPP/E gives you comprehensive GDPR knowledge, perspective and understanding to ensure compliance and data protection success in Europe.

### Course Objectives

Principles of Data Protection in Europe covers the essential pan-European and national data protection laws, as well as industry-standard best practices for corporate compliance with these laws. 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. The training is based on the body of knowledge for the IAPP's ANSI accredited Certified Information Privacy Professional/Europe (CIPP/E) certification program.

### Target Student

- Those involved in:
- Data Protection Officers
- Data Protection Lawyers
- Records Managers
- Information Officers
- Compliance Officers
- Human Resource Officers
- Anyone who uses, processes and maintains personal data

**Prerequisites:** None

## Course Content

**Module 1: Data Protection Laws:** Introduces key European data protection laws and regulatory bodies, describing the evolution toward a harmonised legislative framework.

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

**Module 3: Controllers and Processors:** Describes the roles and relationships of controllers and processors.

**Module 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.

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

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

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

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

**Module 9: International Data Transfers:** Outlines options and obligations for transferring data outside the European Economic Area, including adequacy decisions and appropriate safeguards and derogations.

**Module 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.

**Module 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.