

Certified Information Privacy Professional

Learn via: **Classroom/AFA**

Duration: **2 Day**

Overview

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. You'll gain an understanding of the European model for privacy enforcement, key privacy terminology and practical concepts governing the protection of personal data and trans-border data flows.

This course is designed for anyone whose work is related to the processing of personal data, particularly those in the public sector and from EU institutions, agencies and bodies, including:

- Data Protection Officers
- Data Protection Lawyers
- Compliance Officers
- Information Officers
- Record Managers
- Human Resources Officers
- Data Protection Professionals
- Anyone who uses, processes and maintains personal data

*Please note: that whilst exam costs are covered within the fee of this course, you will need to book your exam via the IAPP website. Delegates will be emailed their Kryterion exam voucher code by the IAPP directly after completion of the course. The voucher is valid for six months from point of receipt.

Prerequisites

There are no specific prerequisites for this course.

What You Will Learn

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.

Training Outline

The program is broken into eleven modules:

Module 1: Data Protection Laws

Introduces key European data protection laws and regulatory bodies, describing the evolution toward a Harmonised European 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 obligations controller and processor.

Module 7: Security or 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, 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, Decisions adequacy and appropriateness safeguards and derogations.

Module 10: Super Visions 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, employers-including processing employee data, surveillance, direct marketing, Internet technology and communications and outsourcing.