Certified Information Privacy Professional and Manager prep course

Duration: 4 Days   Course Code: CIPPE-CIPM

Overview:

This course is designed to provide the Data Protection Officer with a full range of competencies to deliver their organisations GDPR compliance.
In the CIPP/E elements, you will gain foundational knowledge on both broad and global concepts of privacy and data protection laws and practice. You will learn common principles and approaches to privacy as well as understand the major privacy models employed around the globe. An introduction to information security concepts and information security management and governance will be covered including frameworks, controls, and identity and access management. You will also learn about online privacy as it relates to using personal information on websites and other internet-related technologies.

This course delves into the context of European data protection law: origins, institutions and legislative framework; data protection concepts, principles and application, including processing criteria, obligations, data subject rights, confidentiality and security, notification requirements, international data transfers, and supervision and enforcement; and European data protection practices related to employment, surveillance, direct marketing and outsourcing.

In the CIPM elements, you will learn how to create a privacy programme at an organizational level, develop and implement a framework, and establish metrics to measure programme effectiveness. In an interactive format applying practices to a real-world scenario, you will review privacy programme practices through the privacy life cycle: assess, protect, sustain and respond.

The CIPP/E and CIPM designations are accredited under the internationally recognized ANSI/ISO standard 17024:2012, an acknowledgement of the quality and integrity of the programme.

This four-day programme covers the principals of information privacy and privacy management for the EU GDPR

CIPPE/CIPM course includes:
Exam voucher
Textbooks: European Data Protection: Law and Practice & Privacy Program Management: Tools for Managing Privacy Within Your Organization
Participant Guide
Sample Questions
1 Year IAPP Membership

Target Audience:

Individuals who need a foundational understanding of information privacy and data protection and privacy management. Those individuals interested in pursuing CIPP/E and CIPM certifications.
Data Protection Officers
Data Protection Managers
Auditors
Legal Compliance Officers
Security Manager
Information Managers
Anyone involved with data protection processes and programmes

Testing and Certification

Content:

Days 1 ; 2 are broken into 11 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 or 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.

Days 3 ; 4 are broken into ten modules:

Module 1: Introduction to privacy program management

Identifies privacy program management responsibilities, and describes the role of accountability in privacy program management.

Module 2: 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.

Module 3: Applicable laws and regulations

Module 4: 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.

Module 5: Policies

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

Module 6: 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.

Module 7: Training and awareness

Outlines strategies for developing and implementing privacy training and awareness programs.

Module 8: Protecting personal information

■ Examines a holistic approach to protecting personal information through privacy by design.

Module 9: Data breach incident plans

Provides guidance on planning for and responding to a data security incident or breach.

Module 10: Measuring, monitoring and auditing program performance

Relates common practices for monitoring, measuring, analyzing and auditing privacy program performance.

Discusses the regulatory environment, common elements across jurisdictions and strategies for aligning compliance with organizational strategy.

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.com/en-qa/

Global Knowledge, Qatar Financial Center, Burj Doha,Level 21, P.O.Box 27110, West Bay, Doha, Qatar