iapp

Chinese Personal Information Protection training covers data governance, personal information protection, and legal and regulatory requirements. Through training, professionals will be able to oversee the implementation of Chinese privacy laws (most significantly, the Personal Information Protection Law of the People's Republic of China), fulfill data subject requests, and implement privacy governance programs in daily operations.

Training is the foundation of preparation for IAPP certification, the global standard for data protection credentials. Passing the exam earns you the CIPP/CN certification, which will improve your standing in a competitive job market.

Meet your privacy challenges head-on with IAPP training

Data is one of your most valuable assets. Every day, employees at every level of your enterprise access, share, transfer and manage it. Unless they have a solid understanding of data management, you are at risk for data breaches, diminished customer trust and enforcement actions.

IAPP training provides your staff with the knowledge they need to reduce your privacy risk, improve compliance, enhance brand loyalty and more. The IAPP offers privacy and data protection training specifically designed to extend that knowledge to anyone on your team who needs a solid understanding of privacy principles and practices.

The IAPP can also tailor training to your needs and availability.

By investing in your staff, you will give them the knowledge to make better decisions in their everyday work, which is fundamental to the success of your privacy program.

CHINESE PERSONAL INFORMATION PROTECTION TRAINING

This training teaches critical privacy concepts integral to the CIPP/CN exam and is excellent exam preparation. The training and exam are based on the same body of knowledge.

MODULES:

Module 1: Legal and regulatory framework
Introduces the Chinese legal system, including legislation related to data security and privacy protection.

Module 2: Supervisory authorities
Provides an overview of the Chinese political system, as well as a description of the roles and responsibilities of China's law enforcement, industry regulators and judiciary bodies in protecting privacy in China.

Module 3: Principles for personal information-handling activities and personal information protection concepts
Describes how the PIPL introduces the principles and handling methods that should be followed for personal information protection. Reflects the concept of people-centered legislation, and establishes a personal information protection system at the national level.

Module 4: Scope of application and legal bases for personal information handling
Clarifies the legal basis and scope of application for personal information handling to enable learners to fully understand the circumstances in which the PIPL has jurisdiction.

Module 5: Rights of personal information subjects
Discusses how the PIPL expands the scope of personal information protection, and reinforces the protection obligations of personal information handlers. Describes the various legal rights of individuals in information handling.

Module 6: Cross-border data transfers
Outlines the rules the PIPL establishes for the cross-border flow of personal information, and articulates the basic conditions and qualifications that a personal information handler should have to transfer personal information outside the country.

Module 7: Accountability
Discusses how accountability in the PIPL implementation will help guide and encourage personal information handlers to develop personal information protection measures that go beyond their legal obligations.

Module 8: Law enforcement and automated decision-making and algorithms
Reviews how the PIPL regulations impact personal information handler use for automated decision-making. Includes a summary of the potential legal liability for illegal handling of personal information.

Module 9: Sectoral regulatory authorities and PIPL compliance
Specifies the rules for the protection of personal information in: the handling of criminal records, internet applications and electronic monitoring, the protection of children and minors, banks and financial institutions, internet platforms, automotive industry, employment, health and human genetic resources, and governance of emerging technologies.