Meet your privacy challenges head on with **IAPP TRAINING**

Data Is One Of Your Most Valuable Assets

Every day it is being accessed, shared, managed and transferred by people in your organization—in all departments and at all levels. Unless your employees have a solid understanding of the considerations and challenges involved in managing data, you risk a data breach, diminished customer trust and possible enforcement action.

IAPP training can provide your staff with the knowledge they need to help you meet your privacy program goals of reduced risk, improved compliance, enhanced brand loyalty and more. The IAPP offers privacy and data protection training programs specifically designed to extend that knowledge to those on your team requiring a solid understanding of privacy principles and practices.

In order to help you drive privacy knowledge across your organization, our comprehensive and flexible programs can be suited to your specific needs and availability.

U.S. Private-Sector Privacy covers U.S. privacy laws and regulations at federal and state levels, including breach notification and limits on various private sectors. You'll leave with an understanding of the legal requirements for the responsible handling and transfer of personal data within industry and workplaces, including government access to private-sector data.

The training is based on the body of knowledge for the IAPP's ANSI-accredited **Certified Information Privacy Professional/ U.S. (CIPP/US) certification program.**

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

U.S. PRIVATE-SECTOR PRIVACY

This training is a robust opportunity to learn about critical privacy concepts that are also integral to the CIPP/US exam. While not purely a "test prep" course, this training is appropriate for professionals who plan to certify, as well for those who want to deepen their privacy knowledge. Both the training and the exam are based on the same body of knowledge.

ONLINE TRAINING

MODULES:

Module 1: Introduction to privacy
Discusses the modern history of privacy, an introduction to personal information, an overview of data protection roles, and a summary of modern privacy frameworks

Module 2: Structure of U.S. law
Reviews the structure and sources of U.S. law and relevant terms and introduces governmental bodies that have privacy and information security authority

Module 3: General Data Protection Regulation overview (GDPR)
Presents a high-level overview of the GDPR, discusses the significance of the GDPR to U.S. organizations, and summarizes the roles and responsibilities outlined in the law

Module 4: California Consumer Privacy Act of 2018 (CCPA)
Presents a high-level overview of the newly passed California Consumer Privacy Act of 2018, including scope, consumer rights, business obligations and enforcement

Module 5: Enforcement of U.S. privacy and security laws
Distinguishes between criminal and civil liability, compares federal and state authority, presents theories of legal liability, and describes the enforcement powers and responsibilities of government bodies, such as the FTC and state attorneys general

Module 6: Information management from a U.S. perspective
Explores the development of a privacy program, reviews the role of privacy professionals and accountability, discusses employee training, user preferences, vendor management, and examines data classification

Module 7: Healthcare
Describes privacy laws in healthcare, including the major components of HIPAA and the development of HITECH, and outlines privacy protections mandated by other significant healthcare laws

Module 8: Financial privacy
Outlines the goals of financial privacy laws, highlights key concepts of FCRA, FACTA and GLBA, and discusses the Red Flags Rule, Dodd-Frank and consumer protection laws

Module 9: Education
Outlines the privacy rights and protections under FERPA, as well as recent amendments provided by PPRA and NCLBA

Module 10: Telecommunications and marketing
Explores rules and regulations of telecommunications entities, reviews laws that govern marketing and briefly discusses how privacy is addressed in the digital advertising realm

Module 11: Law enforcement, civil litigation and privacy
Relates the Fourth Amendment with expectations of privacy; outlines laws that ensure rights to financial privacy; describes laws around accessing and intercepting communication, including how the telecommunications industry must cooperate with law enforcement; and discusses privacy issues related to litigation, including electronic discovery, redaction and protective orders

Module 12: National security and privacy
Further explores rules and regulations on intercepting communication, including how the laws have evolved and how government agencies and private companies work collaboratively to improve cybersecurity

Module 13: Workplace privacy
Describes federal and state laws that regulate and protect employee privacy, as well as federal laws that prohibit discrimination; examines the lifecycle of employee privacy, including background screening, employee monitoring, investigating misconduct and termination

Module 14: State data security and breach notification laws
Identifies state laws that impact data security, reviews Social Security number use regulation, and discusses laws governing data destruction; summarizes the scope of state data breach notification law, highlights the nine elements of state data breach notification laws and notes major differences in state laws