U.S. Private-Sector Privacy training covers state and federal laws and regulations. Topics include breach regulation, workplace privacy, limits on private-sector data collection, and government access to private-sector data. You will come away understanding the legal requirements for responsibly handling and transferring personal data in industry and workplaces.

The training is based on the body of knowledge for the IAPP's ANAB-accredited **Certified Information Privacy Professional/US** certification.

iapp

Meet your privacy challenges head on with IAPP TRAINING

Data is one of your most valuable assets. Every day it is accessed, shared, managed and transferred at all levels of your institution. Unless your employees have a solid understanding of the considerations and challenges of managing data, you risk breaches, diminished customer trust and possible enforcement action.

IAPP training can provide your staff with the knowledge they need to help you reduce 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.

To help you drive privacy knowledge across your enterprise, our comprehensive and flexible training options can be tailored to your specific needs and availability.

By investing in IAPP training, you will give your staff the knowledge to make better decisions in their everyday work and operations.

U.S. PRIVATE-SECTOR PRIVACY

This training is an 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 and for those who want to deepen their privacy knowledge. Both the training and the exam are based on the same body of knowledge.

MODULES:

Module 1: Foundations of privacy and data protection
Discusses the modern history of privacy and data protection, introduces fair information practices and types of personal information, and gives an overview of data protection roles and privacy protection models.

Module 2: Comprehensive privacy and data protection laws
Provides an overview of both international and state comprehensive privacy laws with extraterritorial scope and explores options for international data transfers.

Module 3: U.S. legal framework
Reviews the structure and sources of U.S. law and relevant legal terms and introduces governmental bodies that have privacy and information security authority in the U.S.

Module 4: Enforcement of U.S. privacy and security laws
Distinguishes between criminal and civil liability; presents theories of legal liability; and describes the enforcement powers, responsibilities, and evolving priorities of government bodies such as the Federal Trade Commission and state attorneys general.

Module 5: Information management from a U.S. perspective
Examines data classification and data flow management and explores the role of the privacy professional within organizations, including the development of a privacy program, accountability, employee training, privacy policies and notices, management of user preferences and requests and third-party vendors, and the mitigation of online privacy risks.

Module 6: Government and court access to private-sector information
Explores rules and regulations on intercepting communications, including how the laws have evolved and how government agencies and private companies work collaboratively with law enforcement to improve cybersecurity.
The training also outlines laws that ensure rights to financial privacy; discusses privacy issues related to litigation, including electronic discovery, redaction and protective orders; and briefly compares U.S. discovery rules to foreign laws.

Module 7: State data privacy and security laws
Compares federal and state authority; identifies state laws that impact privacy and data security, data subject rights, and privacy notice requirements; discusses state cookie and online tracking regulations; the use of artificial intelligence technologies and biometric information and laws governing data retention and destruction; outlines the scope of state data breach notification laws; and highlights key elements and major differences in state laws.

Module 8: Telecommunications and marketing
Explores rules and regulations of telecommunications entities, reviews laws that govern telecommunications and marketing, and briefly discusses how privacy is addressed in the digital advertising realm.

Module 9: Health care
Describes privacy laws in health care, including the major components of HIPAA and the development of the Genetic Information Non-Discrimination and Health Information Technology for Economic and Clinical Health acts, and outlines privacy protections mandated by other significant health care laws.

Module 10: Children's privacy
Discusses the Children's Online Privacy Protection Act and state statutes that regulate children's privacy outlines privacy rights and protections under the Family Education Rights and Privacy Act, and describes recent amendments provided by the Protection of Pupil Rights Amendment and Every Student Succeeds Act. Also explores education technology and privacy.

Module 11: Financial privacy
Outlines the goals of financial privacy laws; highlights key concepts of Fair Credit Reporting, Fair and Accurate Credit Transactions, and Gramm-Leach-Bliley acts; and discusses the Red Flags Rule, the Disposal Rule, Dodd-Frank, online and mobile banking, and anti-money laundering laws.

Module 12: Privacy in the workplace
Describes federal laws that regulate and protect employee privacy and prohibit discrimination; examines the life cycle of employee privacy, including background screening, employee monitoring, investigating misconduct and termination; and outlines antidiscrimination laws.