



Australian Privacy is a practical training focused on the Australian Privacy framework, including the Privacy Act; the Australian Privacy Principles; federal, state and territorial privacy obligations; regulatory enforcement; sector-specific considerations and emerging privacy issues. Those taking this course will build practical knowledge for navigating privacy obligations in Australia.

The training is based on the body of knowledge for the **Certified Information Privacy Professional/Australia** certification.

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 by people in your company or institution, 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 breach, diminished customer trust and possible enforcement action.

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

Our comprehensive and flexible offerings can be suited to your specific needs and availability to help you drive privacy knowledge across your enterprise.

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.

AUSTRALIAN PRIVACY

This training teaches privacy concepts integral to Australian federal data privacy and personal information protection legislation. It is appropriate for professionals who plan to certify, as well as those who want to deepen their jurisdictional knowledge. Both the training and exam are based on the same body of knowledge.

MODULES:

Module 1: Foundations of Australian privacy law

Establishes the Australian privacy landscape, including the federated legal framework; the Privacy Act's history, scope and 13 Australian Privacy Principles; the OAIC's enforcement powers and extraterritorial reach; and Australia's evolving approach to AI and automated decision-making regulation.

Module 2: Privacy across Australian jurisdictions

Covers the privacy obligations of Commonwealth agencies under the Australian Government Agencies Privacy Code, the foundational state and territory privacy statutes and their regulators, and how these regimes overlap with the Privacy Act.

Module 3: APPs, part one: Transparency and collection

Reviews the APPs relating to transparency and collection (1-5), privacy governance and policy requirements, anonymity and pseudonymity, solicited collection and sensitive information, plus unsolicited information and collection notices.

Module 4: APPs, part two: Use, disclosure and cross-border transfers

Reviews the APPs relating to post-collection handling (6-9), use and disclosure, direct marketing, cross-border disclosure and overseas accountability, and government-related identifiers.

Module 5: APPs, part three: Data integrity and individual rights

Reviews the APPs relating to data integrity and individual rights (10-13), information quality, security, retention and breach response, plus access and correction requests.

Module 6: Privacy enforcement in Australia

Discusses the OAIC's enforcement powers and escalation model, its regulatory priorities and jurisdictional overlap with other regulators, and the penalties, case law and statutory tort that follow serious privacy breaches.

Module 7: Health information privacy, financial privacy and children's privacy

Covers health information and emerging health technologies, financial information and the Consumer Data Right, and heightened protections for children's personal information.

Module 8: Workplaces, surveillance and emerging frontiers

Considers the employee records exemption and its limits, workplace surveillance and automated decision-making, Commonwealth surveillance powers, and evolving obligations around data breaches, the Digital ID system, open data and cybersecurity.