SmartSuite

Framework / Privacy / Global Privacy Regulations

Privacy Act 1988 (Cth) – Australian Privacy Principles (APPs)

The Privacy Act 1988 and its 13 Australian Privacy Principles govern how Australian Government agencies and organizations with turnover above $3 million handle personal information.



What it is

The Privacy Act 1988 (Cth) is Australia's federal privacy law. Its 13 Australian Privacy Principles (APPs) set the standards for how Australian Government agencies and organizations with an annual turnover of more than $3 million, and some other organizations, collect, use, disclose, secure, and give access to personal information. These bodies are called APP entities. Parliament passed the Act at the end of 1988, it commenced in 1989, and the APPs have applied since 12 March 2014. The Office of the Australian Information Commissioner (OAIC) regulates it.

A breach of an APP is an interference with the privacy of an individual and can lead to regulatory action and penalties. The Act also regulates the privacy component of consumer credit reporting, tax file numbers, and health and medical research. Since 2018 the Notifiable Data Breaches scheme has required APP entities to notify affected individuals and the OAIC of a data breach that is likely to result in serious harm. The Privacy and Other Legislation Amendment Act 2024 made further changes, most of them commencing on 11 December 2024.

At a glance

PUBLISHER Australian Parliament (Privacy Act 1988); regulated by the Office of the Australian Information Commissioner (OAIC)	TYPE Framework	VERSION Privacy Act 1988 (current consolidated version with amendments)
EFFECTIVE 12 March 2014 (Australian Privacy Principles); Act commenced 1989	DOMAIN Privacy	FAMILY Global Privacy Regulations
REGION Australia	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY Medium

Source: oaic.gov.au/privacy/privacy-legislation/the-privacy-act

Why it matters

- **One structure for any sector** The 13 APPs cover collection, use and disclosure, governance and accountability, integrity and correction, and access, so one program covers most personal information handling.
- **A reasonable-steps standard** APP 10 and APP 11 require reasonable steps to keep information accurate, up to date, and protected from misuse, interference, loss, and unauthorized access, modification, or disclosure.
- **Higher standards for sensitive information** APP 3 applies higher standards to the collection of sensitive information, so teams know where to concentrate controls.
- **Accountability for overseas disclosure** APP 8 sets the steps an APP entity must take to protect personal information before it is disclosed overseas.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports Privacy Act 1988 (APPs)

APP-to-control library

Map each of the 13 APPs to policies, controls, and owners, including the APP privacy policy review date.

Personal information inventory

Record what personal information is collected, why, where it is held, and who receives it, including overseas recipients, using Privacy Management data inventories.

Collection notices and marketing

Track collection notices, sensitive information handling, and direct marketing opt-outs for each channel.

Access and correction requests

Run APP 12 access and APP 13 correction requests as tracked tasks with owners and dates, using Privacy Management requests.

Breach assessment and notification

Run the assessment of whether a breach is likely to result in serious harm, and the notices to individuals and the OAIC, with Workflow Orchestration.

Privacy program reporting

Use Enterprise Reporting to show open requests, incidents, and control status for privacy leadership.

Common framework mappings

APEC PF | CCPA/CPRA | GDPR | ISO 27001:2022 | ISO 27701 | NIST Privacy Framework v1.0

Official resources

Privacy Act 1988

Defines the national data protection framework including the 13 Australian Privacy Principles.

oaic.gov.au/privacy/privacy-legislation/the-privacy-act

Australian Privacy Principles (APPs) Guidelines

Provides detailed guidance on the application of the Australian Privacy Principles.

oaic.gov.au/privacy/australian-privacy-principles-guidelines

Notifiable Data Breaches Scheme

Outlines requirements for notifying affected individuals and the OAIC about eligible data breaches.

oaic.gov.au/privacy/notifiable-data-breaches

OAIC Regulatory Action Policy

Describes the OAIC's approach to using its regulatory powers under the Privacy Act.

oaic.gov.au/about-the-OAIC/our-regulatory-approach/privacy-regulatory-action-policy

Frequently asked questions

Which organizations must comply with the Privacy Act 1988?

Australian Government agencies and organizations with an annual turnover of more than $3 million, plus some smaller operators such as private health service providers, businesses that sell or purchase personal information, credit reporting bodies, and contracted service providers for an Australian Government contract. These are known as APP entities.

What are the 13 Australian Privacy Principles?

They cover open and transparent management, anonymity and pseudonymity, collection of solicited information, unsolicited information, notification of collection, use or disclosure, direct marketing, cross-border disclosure, government related identifiers, quality, security, access, and correction of personal information (APPs 1 to 13).

Does the Privacy Act apply to small businesses?

Generally not for businesses with an annual turnover of $3 million or less, unless an exception applies. Exceptions include private health service providers, businesses that sell or purchase personal information, credit reporting bodies, contracted service providers for an Australian Government contract, and businesses that have opted in.

When must a data breach be notified?

If the Privacy Act covers the organization or agency, it must notify affected individuals and the OAIC when a data breach involving personal information is likely to result in serious harm. This is the Notifiable Data Breaches scheme, in place since 2018.

 © 2026 SmartSuite Inc. All rights reserved.

What does APP 8 require for overseas disclosure?

APP 8 sets the steps an APP entity must take to protect personal information before it is disclosed overseas. Teams usually keep a register of overseas recipients and the safeguards in place for each.

License included / downloadable: Yes The Privacy Act 1988 is Australian national legislation and is publicly available through official government sources.

Full framework page and mappings: smartsuite.com/frameworks/australia-privacy-act-1988-australian-privacy-principles

© 2026 SmartSuite Inc. All rights reserved.