AUSTRALIAN PRIVACY PRINCIPLES: WHAT YOUR BUSINESS NEEDS TO DO

The most common privacy compliance gaps aren't hard to fix. They are just easy to overlook until an access request or OAIC complaint makes them impossible to ignore. This checklist covers what your business is required to have in place under the Privacy Act 1988 (Cth) and the changes introduced by the Privacy and Other Legislation Amendment Act 2024.

PUBLISH A PRIVACY POLICY

Your privacy policy must cover:

- what personal information is collected and why
- how it is handled and stored
- whether it is disclosed overseas
- how individuals can access, correct or complain about their information

It must be current and easy to find on your website. It should be reviewed annually to make sure it is up to date with your business practices. For example, many businesses have now started using AI, which should be disclosed.

COLLECTION MUST BE LAWFUL AND DISCLOSED

You can only collect personal information that is reasonably necessary for your business. At the point of collection, individuals must be told who is collecting their information, why, and what it will be used for.

Analytics platforms, advertising pixels and audience targeting tools all trigger this obligation. If they're active on your site, collection is already occurring.

SECONDARY USE REQUIRES A SEPARATE BASIS

Information collected for one purpose can't be used for another without a valid basis. It usually needs to be related to the purpose you collected it for, or you may need consent to otherwise handle it. Using a contact form submission to add someone to a marketing list, without a separate basis, is a common gap.

CONSENT AND OPT OUR REQUIREMENTS

To send marketing emails, you need consent - which can be express or inferred in certain circumstances. Marketing communications must include a clear opt-out. Once someone opts out, you must stop promptly.

DATA QUALITY AND RETENTION

Personal information must be kept accurate and destroyed or de-identified when no longer needed. Your privacy policy should explain how you handle retention. A separate data retention policy is also worth having to manage this in practice.

OVERSEAS DISCLOSURE MUST BE DOCUMENTED

If personal information is processed by overseas tools or platforms (US-based SaaS, cloud storage, third-party software), your privacy policy must say so. You generally remain accountable for how thar data is handled offshore.

LEGALVISION®

AUSTRALIAN PRIVACY PRINCIPLES: WHAT YOUR BUSINESS NEEDS TO DO

ACCESS AND CORRECTION RIGHTS

Individuals can request access to their personal information. You have 30 days to respond. They can also request corrections, and you need a real process to handle both. These are the provisions most commonly tested by complaints.

ENFORCEMENT

The following penalties came into effect from 10 December 2024:

- Infringement notices of up to $330,000 for administrative breaches
- Mid-tier civil penalties of up to $3.3 million for serious contraventions
- Individuals can now sue directly for serious invasions of privacy

PRIVACY POLICIES

Most privacy policies fall short in the following areas:

- No functioning complaints process
- Out of date and not reflecting current business practices
- Undisclosed overseas data transfers
- Access and correction provisions that don't reflect actual practice
- A single access request or complaint will surface these.

COMPLAINTS HANDLING

Your privacy policy must set out how individuals can complain and how you'll respond. This is one of the first things the OAIC checks. A generic contact address without a described process doesn't satisfy the requirement.

LOOKING FORWARD

Automated decision-making transparency commences 10 December 2026.

If your business uses automated processes to make or significantly influence decisions about individuals (pricing, credit, hiring, access to services), you'll need to disclose this in your privacy policy. Build it into any privacy policy refresh now.

CONTACT US

visit our website | legalvision.com.au
email us | info@legalvision.com.au
call us | 1300 544 755

LEGALVISION®