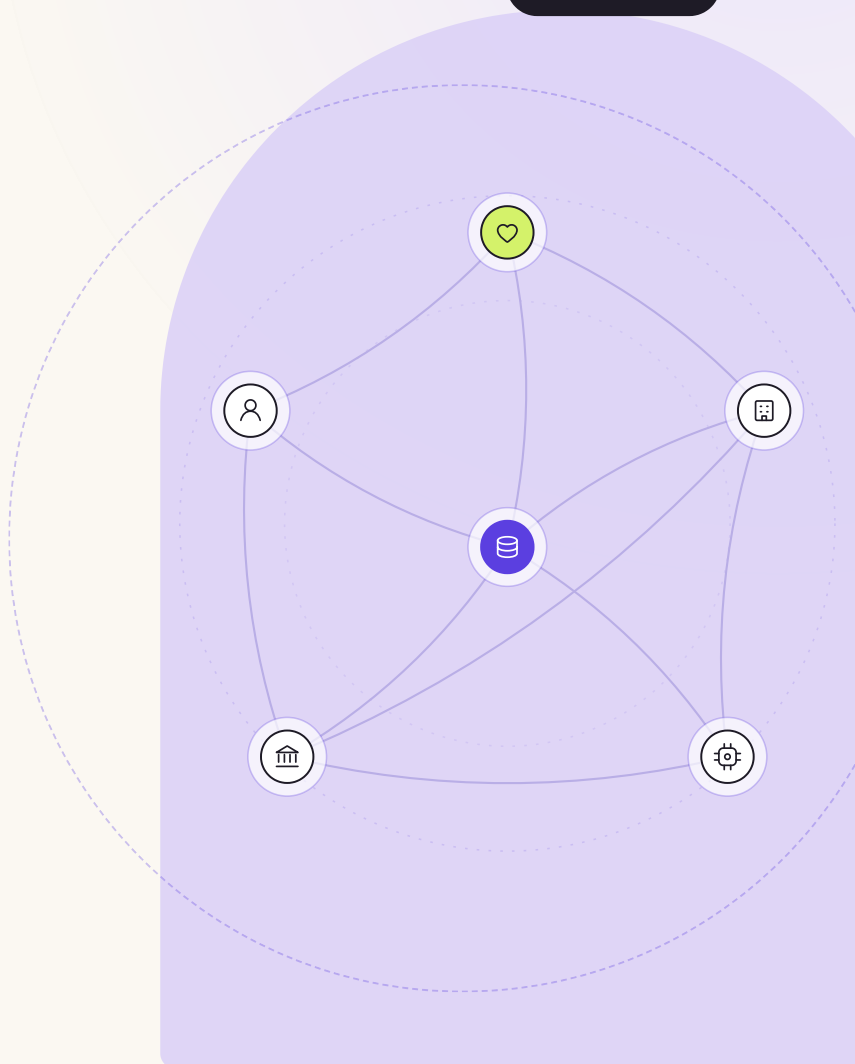




FREE GUIDE



SELF-ASSESSMENT · PRIVACY & DATA PROTECTION

Privacy policy health check

A self-assessment to see whether your APP privacy policy covers what APP 1 requires, reads clearly, matches what you actually do, and is ready for the automated decision-making content due from 10 December 2026.

Updated 17 October 2026

Law in force

lexoraai.com.au

Every organisation covered by the Privacy Act must have a clearly expressed and up-to-date privacy policy about how it manages personal information. This is APP 1. The policy is often the first document a regulator, a customer or a journalist reads when something goes wrong, so a policy that is vague, out of date or inconsistent with practice is a real exposure, not a formality.

Use the questions below to see where your policy stands today. Answer each one honestly: yes, no or not sure. A “not sure” is useful information in itself.

Part 1. The required content (APP 1.4)

APP 1.4 lists matters the policy must contain. The list is a minimum, not the whole of what a good policy covers.

APP 1.4	The policy must state
(a)	The kinds of personal information you collect and hold
(b)	How you collect and hold it
(c)	The purposes for which you collect, hold, use and disclose it
(d)	How individuals can access their information and seek correction
(e)	How individuals can complain about a breach of the APPs, or a binding registered APP code, and how you will deal with complaints
(f)	Whether you are likely to disclose personal information to overseas recipients
(g)	If so, the countries where those recipients are likely to be located, if practicable to specify them

☐ Does the policy address every item in the table, in words specific to your organisation?

☐ Does it describe the kinds of information you actually hold, rather than a generic list copied from another business?

☐ Does it explain how people can access and correct their information, with a working contact point?

☐ Does it explain how to make a complaint and what happens next?

☐ Does it say whether information goes overseas and, where practicable, to which countries? Think about cloud services, offshore support teams and related companies.

Part 2. Readability and availability

The OAIC's APP Guidelines say a privacy policy should be easy to understand, avoid jargon and internal terms, be easy to navigate, and include only information relevant to how the entity handles personal information. A layered approach, with a short summary linking to the detail, can help.

- ☐ Could a customer with no legal background understand the policy on first reading?
- ☐ Have you removed internal system names, unexplained acronyms and legal boilerplate that does not apply to you?
- ☐ Is the policy easy to find on your website, free of charge and easy to download?
- ☐ Could you provide it in another form on request, such as a printed copy or an accessible format?
- ☐ Does it show when it was last updated?

Part 3. Accuracy against practice

This is where most policies fall down. A policy that describes what the organisation intended several years ago, rather than what it does now, can mislead the people relying on it.

- ☐ When did someone last compare the policy with what your teams, systems and suppliers actually do?
- ☐ Have you added new products, apps, marketing tools, analytics or AI tools since the policy was last reviewed?
- ☐ Have you changed key suppliers, hosting locations or offshore arrangements since then?
- ☐ Do your collection notices, forms and consent wording say the same thing as the policy?
- ☐ Does the policy describe any collection of sensitive information, such as health information, that your organisation in fact undertakes?
- ☐ Is a named person responsible for keeping the policy current, and is a review scheduled? The OAIC suggests reviewing it at least as part of annual planning.

Part 4. Automated decision-making content (from 10 December 2026)

The Privacy and Other Legislation Amendment Act 2024 inserted new APP 1.7 to 1.9. From **10 December 2026**, if you have arranged for a computer program to make, or do a thing substantially and directly related to making, a decision that could reasonably be expected to significantly affect an individual's rights or interests, and personal information is used in that process, your policy must describe:

- the kinds of personal information used in the operation of those programs
- the kinds of decisions made solely by the operation of those programs
- the kinds of decisions for which a thing substantially and directly related to making the decision is done by those programs.

The OAIC's guidance says "computer program" is read broadly and includes AI and machine learning, and that a decision includes refusing or failing to make one.

☐ Do you know which of your systems, including supplier software, make or substantially contribute to decisions about individuals?

☐ Have you considered whether any of those decisions could significantly affect someone's rights or interests, such as access to credit, employment, services, pricing or eligibility?

☐ Have you identified the kinds of personal information each relevant system uses?

☐ Is someone responsible for drafting the new content and having it reviewed before 10 December 2026?

Reading your results

If you answered "no" or "not sure" to several questions in any one part, that part needs attention. Gaps in Part 3 usually point to a wider issue: the policy cannot be accurate unless someone has a current picture of what personal information the organisation holds and where it goes. Gaps in Part 4 are time-sensitive because the obligation commences on 10 December 2026.

Next step

Lexora offers a fixed-scope privacy compliance review that tests your policy and notices against your actual practices and the APPs. If you would like to talk it through first, book a free 20-minute call.

General information, not legal advice. Lexora is not a law firm. For advice on your organisation's obligations, consult a qualified legal adviser.

Sources

1. OAIC, APP Guidelines, Chapter 1 (APP 1, open and transparent management of personal information)
<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information>
2. Privacy and Other Legislation Amendment Act 2024 (legislation.gov.au)
<https://www.legislation.gov.au/C2024A00128/asmade/text>



Better governance. *Greater confidence.*

Lexora is an Australian-first advisory business. We help organisations understand their privacy, data and AI obligations, assess risk, build governance frameworks and put practical controls in place.

OUR PRACTICES

Privacy & Data Protection

AI Governance & Responsible AI

Data Governance

Regulatory Readiness & Compliance

WAYS TO START

Privacy Health Check

AI Governance Readiness Assessment

Data Governance Review

Regulatory Readiness Consultation

DISCUSS YOUR GOVERNANCE NEEDS

lexoraai.com.au

info@lexoraai.com.au

More free guides: lexoraai.com.au/resources

This guide is general information, current at the date shown. It is not legal advice and does not take account of your circumstances. Lexora is not a law firm. Check the primary sources before relying on any date or requirement. © 2026 Lexora. You are welcome to share this guide unaltered, with this page attached.