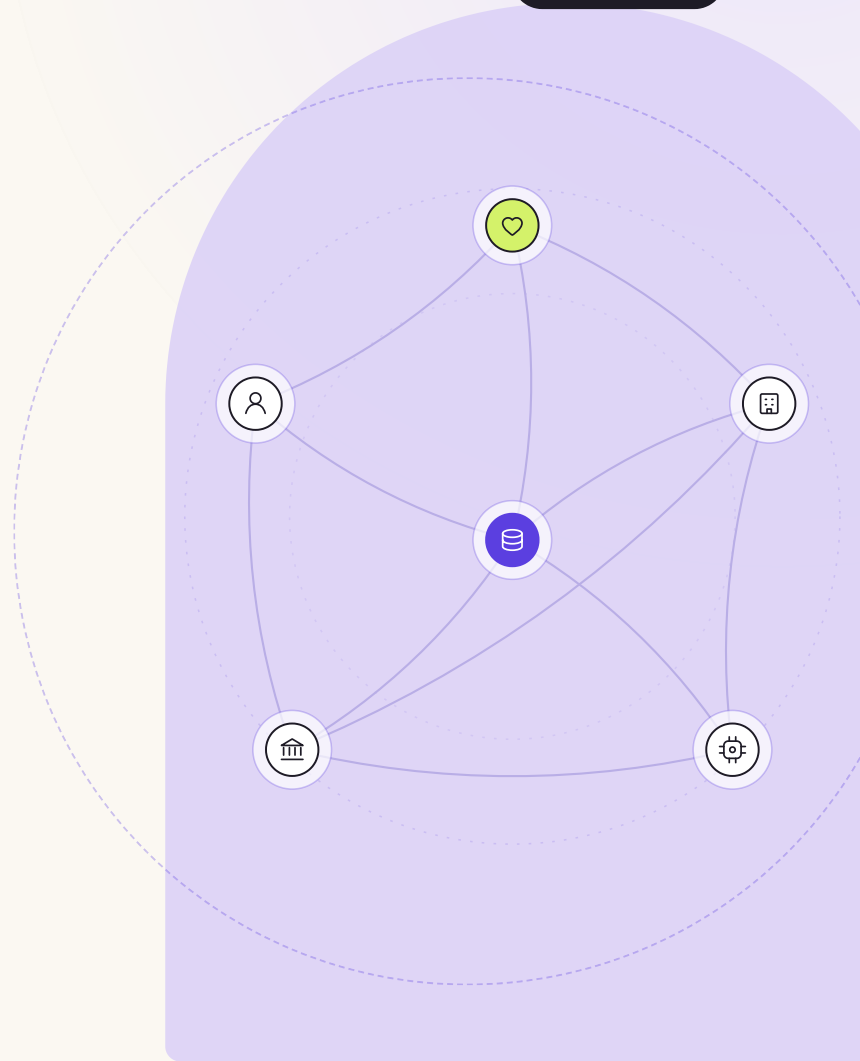




CHECKLIST · PRIVACY & DATA PROTECTION

Collection notice checklist

The ten matters APP 5 asks you to tell people when you collect their personal information, when to tell them, how layered notices work, and the mistakes to look for.

APP 5 requires an organisation that collects personal information to take reasonable steps to notify the individual of certain matters, or to make sure they are aware of them. A collection notice is different from a privacy policy. The privacy policy (APP 1) describes your general information handling. A collection notice is specific to a particular collection: a sign-up form, a job application, a phone enquiry, a CCTV camera, a customer survey.

Use this checklist for each point where your organisation collects personal information.

Start with a list of collection points

- ☐ List every place you collect personal information: website forms, apps, phone, email, in person, events, recruitment, CCTV, and information you receive from third parties.
- ☐ Note who owns each collection point, so someone is responsible for its notice.
- ☐ Include collection by suppliers or agents acting for you. The OAIC says you can require a third party collector, by contract, to give notice on your behalf.

The APP 5.2 matters

For each collection point, check whether the notice covers the following, as they relate to that collection:

- ☐ **(a)** Your organisation's identity and contact details.
- ☐ **(b)** If you collect from someone other than the individual, or the individual may not know you are collecting, the fact and circumstances of the collection.
- ☐ **(c)** If an Australian law or a court or tribunal order requires or authorises the collection, that fact and which law or order.
- ☐ **(d)** The purposes for which you collect the information.
- ☐ **(e)** The main consequences for the individual if some or all of the information is not collected.
- ☐ **(f)** Any other organisations, or kinds of organisations, to which you usually disclose this kind of information.

- ☐ **(g)** That your privacy policy explains how the individual can access and seek correction of their information.
- ☐ **(h)** That your privacy policy explains how to complain about a breach of the APPs and how you will deal with a complaint.
- ☐ **(i)** Whether you are likely to disclose the information to overseas recipients.
- ☐ **(j)** If so, the countries where those recipients are likely to be located, if practicable to specify them.

Timing

APP 5 requires the steps to be taken at or before the time of collection or, if that is not practicable, as soon as practicable afterwards.

- ☐ Is the notice in front of the person before they submit their information, not only in a confirmation email afterwards?
- ☐ Where notice is given after collection, can you explain why earlier notice was not practicable? The OAIC expects you to be able to justify any delay.
- ☐ For phone collection, is the notice given at the start of the call, or followed up in writing if that is not possible?

Layered notices

The OAIC's guidance supports layered notices. A short notice at the point of collection, such as a few lines on a form or a sign, can link to a fuller notice online or in print.

- ☐ Does the short layer say who you are, why you are collecting, and where to find the rest?
- ☐ Is the link to the fuller notice working, and does the fuller notice cover the matters relevant to this collection?
- ☐ If you rely on your privacy policy for some matters, have you checked that the policy actually covers this specific collection? The OAIC cautions that a policy may describe only general practices.

When not notifying may be reasonable

The OAIC recognises some circumstances where taking no steps may be reasonable, for example where the individual already knows the matters, or where notice would jeopardise someone's life, health or safety. You must be able to justify this.

- ☐ Where you give no notice, is the reason documented?
- ☐ For recurring collections, have you considered whether notice needs refreshing after a long gap or a change in how information is collected?

Common mistakes

The table below draws on pitfalls described in the OAIC's APP 5 guidance.

Mistake	What to check
Relying on the privacy policy alone	Whether the policy actually covers this particular collection
Listing every possible consequence of not providing information	Only the main consequences need describing
Listing disclosures that happen only in exceptional circumstances	Only usual disclosures need describing
Naming every recipient	Describing kinds of recipients may be enough
Treating routing data through overseas servers as a disclosure	The OAIC says this is usually a use, not a disclosure
Notices left unchanged after a change of purpose or system	Whether each notice still matches current practice

- ☐ Do your notices use the same descriptions of purposes, recipients and overseas locations as your privacy policy?
- ☐ Is someone reviewing notices whenever a form, system, supplier or purpose changes?

Next step

Lexora offers a fixed-scope privacy compliance review that checks your collection notices and privacy policy against what your organisation actually does. If you would like to discuss your situation 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 5 (APP 5, notification of the collection of personal information)
<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information>
2. 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>



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.