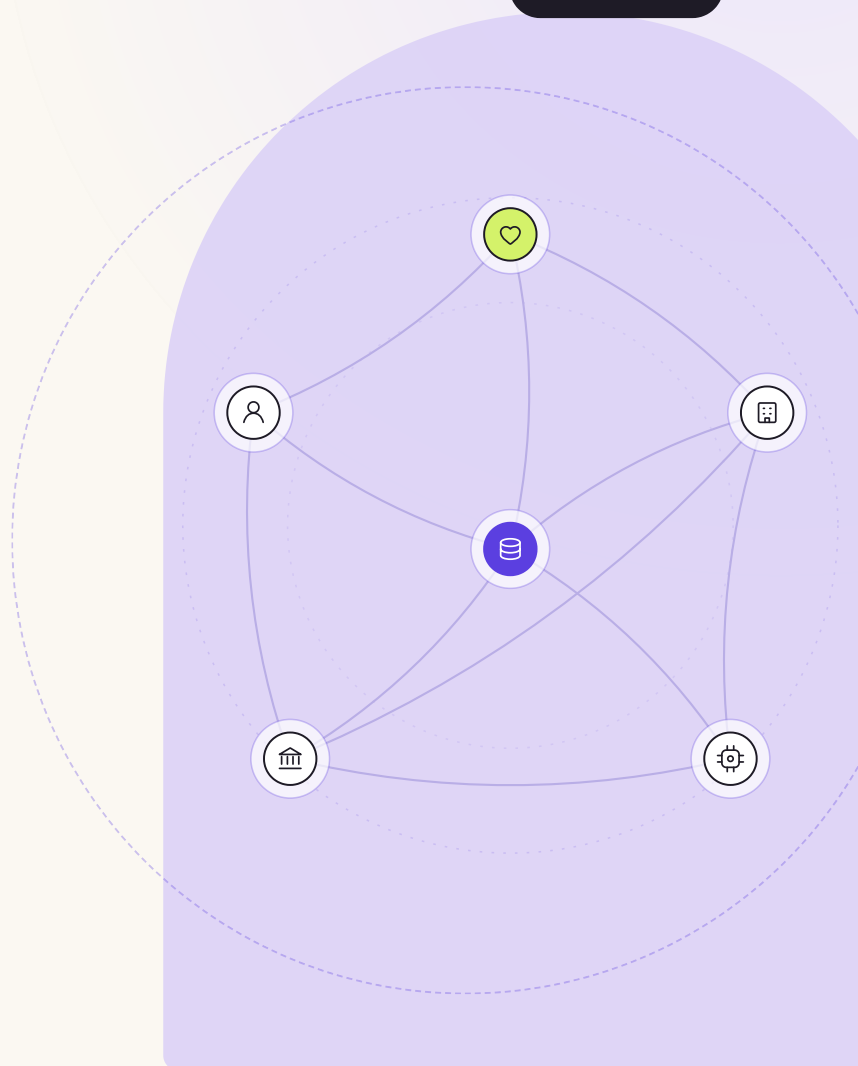




FREE GUIDE



GUIDE · PRIVACY & DATA PROTECTION

Data retention and destruction guide

What APP 11.2 requires once you no longer need personal information, how to find what you hold, how to think about retention periods, the basics of de-identification, and why suppliers and backups matter.

Personal information you no longer need is risk without benefit. If it is breached, it can harm the people it is about, and it adds to the scale of any incident you have to assess and report. The Privacy Act addresses this directly in APP 11.2.

What APP 11.2 requires

Under APP 11.2, an organisation must take reasonable steps to destroy personal information, or to ensure it is de-identified, once it no longer needs the information for any purpose for which it may be used or disclosed under the APPs. The obligation does not apply where:

- the information is contained in a Commonwealth record, or
- an Australian law, or a court or tribunal order, requires the organisation to keep it.

Two points follow. First, “we might need it one day” is not a permitted purpose. Second, the obligation is triggered by need, so you cannot meet it without knowing why you hold each category of information.

Since 11 December 2024, APP 11.3 has made clear that reasonable steps include technical and organisational measures. The OAIC gives examples such as staff training, standard operating procedures, and policies for deciding what to retain or destroy.

Finding what you hold

You cannot destroy what you cannot find. Most organisations hold personal information in more places than they expect.

- ☐ Core systems: customer, client, patient, member or student records.
- ☐ Human resources and payroll records, including unsuccessful job applications.
- ☐ Email accounts, shared drives, collaboration tools and personal folders.
- ☐ Marketing lists, analytics platforms and event registrations.
- ☐ Spreadsheets and exports created for a one-off project and never deleted.
- ☐ Paper files, archive boxes and offsite storage.
- ☐ Copies held by suppliers, including cloud services, outsourced call centres and IT providers.
- ☐ Backups and archives.

For each, it helps to record what kinds of personal information are held, why, who owns it, and where it is.

Setting retention periods

A retention period answers the question: how long do we need this, and why? Two kinds of reason usually apply.

Minimum periods set by other laws. Some laws require you to keep certain records for a set time, and APP 11.2 does not override them. Two common examples:

- The Australian Taxation Office says businesses need to keep most tax records for 5 years. The start of that period depends on the record, and some records must be kept longer.
- The Fair Work Ombudsman says employers have to keep time and wages records for 7 years.

Your industry may have others, for example in health, financial services or education. Check the requirements that apply to you with your legal adviser rather than assuming.

Your own business need. Beyond legal minimums, the question is whether you still need the information for the purpose you collected it for, or for a permitted secondary purpose. A legal minimum is a floor, not a reason to keep everything for that long or longer.

Questions to ask for each category:

- ☐ Is there a law or order that requires us to keep it, and for how long?
- ☐ Do we still need it for the purpose it was collected for?
- ☐ What would actually go wrong if we no longer had it?
- ☐ Who has authority to approve the retention period and any exceptions?
- ☐ How will we know when the period has ended for a given record?

Destruction

The OAIC's APP 11 guidance says information is destroyed when it can no longer be retrieved. Putting hard copy in ordinary garbage or recycling is not enough unless it has first been shredded, pulped or otherwise destroyed. Where you instruct a third party to destroy information, the OAIC says you should take steps to verify that it has done so.

Where irretrievable destruction is not possible, the OAIC describes putting information "beyond use", which requires that you will not use or disclose it, cannot give anyone else access to it, keep

appropriate security around it, and commit to destroy it once that becomes possible. The OAIC expects this to be needed only in limited cases.

De-identification basics

De-identification is an alternative to destruction where the data still has value, for example for research or analysis. The OAIC's guidance says information is de-identified when there is no reasonable likelihood of re-identification in the context in which it is held or released. That usually means removing direct identifiers, such as names and addresses, and then altering other identifying details, applying controls on who can access the data and how, or both.

Some cautions from the OAIC:

- De-identification is context-dependent. Data that is de-identified in one setting can become personal information again if it is released publicly, breached or combined with other data.
- Re-identification risk has to be actively assessed and managed. If it cannot be reduced enough, destruction should be considered instead.

The OAIC and CSIRO's Data61 published the De-identification Decision-Making Framework in 2017 as a practical guide for organisations considering sharing or releasing data. The OAIC notes that some of its content may now be outdated, so read it alongside the OAIC's current guidance.

Suppliers and backups

The OAIC says APP 11 applies to information you "hold", which includes information you have the right or power to deal with, even if a third party stores it. Outsourcing storage does not outsource the obligation. The OAIC also says reasonable steps extend to all copies you hold, including archived copies and backups.

☐ Do your supplier contracts say what happens to personal information at the end of the engagement?

☐ Can you get confirmation that a supplier has deleted or returned information?

☐ Do you know how long your backups are kept, and whether deleted records persist in them?

☐ Is someone responsible for checking that destruction actually happens on schedule?

Next step

Lexora offers a fixed-scope data protection review covering what you hold, how long you keep it and how it is secured and disposed of. 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. Retention requirements vary by industry, so confirm the periods that apply to you with a qualified legal adviser.

Sources

1. OAIC, APP Guidelines, Chapter 11 (APP 11, security of personal information)
<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information>
2. OAIC, De-identification and the Privacy Act
<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-and-the-privacy-act>
3. OAIC and CSIRO's Data61, De-identification Decision-Making Framework
<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-decision-making-framework>
4. Australian Taxation Office, Overview of record-keeping rules for business
<https://www.ato.gov.au/businesses-and-organisations/preparing-lodging-and-paying/record-keeping-for-business/overview-of-record-keeping-rules-for-business>
5. Fair Work Ombudsman, Record-keeping
<https://www.fairwork.gov.au/pay-and-wages/paying-wages/record-keeping>



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.