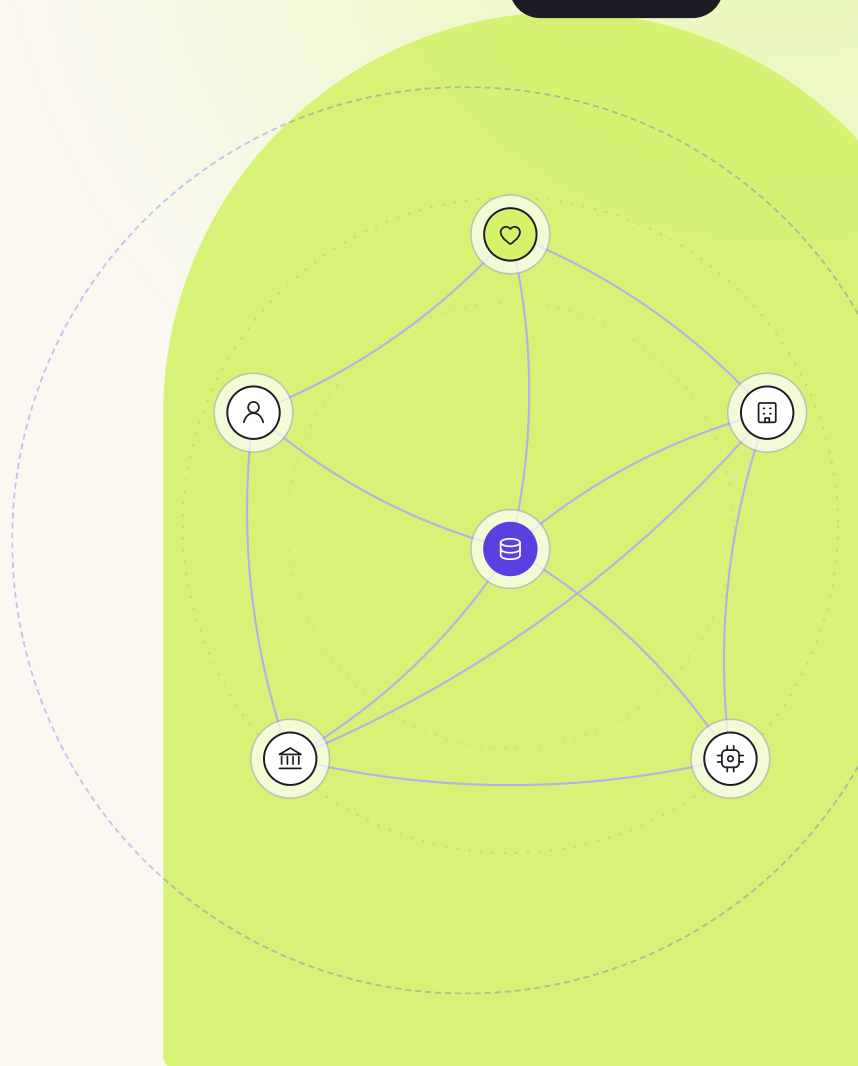




FREE GUIDE



ONE-PAGER · DATA GOVERNANCE

Data governance roles on one page

Data owner, data steward, data custodian and data user. What each role decides and does, and six signs your roles are unclear.

Updated 17 October 2026

lexoraai.com.au

Most data problems are not technology problems. They are accountability problems: nobody is sure who can approve a new use of a dataset, who fixes a quality issue, or who decides when records can be deleted. Clear roles answer those questions before they become incidents.

The titles below are common industry conventions, not terms defined in the Privacy Act. Organisations use different names, and that is fine. The Department of Finance’s Australian Government Data Governance Framework (September 2025), written for Australian Government agencies, makes the same point: agencies may use their own role titles, because what matters is the roles and their responsibilities. That framework sets minimum roles for agencies, including a Chief Data Officer with overall accountability and a responsible officer with day-to-day authority over specific data assets. Private sector organisations are not bound by it, but the principle carries across.

The four roles

Role	Usually held by	What they decide	What they do
Data owner	A senior business leader accountable for a data domain, such as customer, employee or finance data	Who may access the data and for what purposes; acceptable risk; classification; retention; approval of new uses and sharing	Signs off on access and sharing requests, accepts or escalates risk, answers for the data to executives and the board
Data steward	A subject matter expert in the business, often reporting to the owner	Definitions, quality rules and standards for the data within the owner’s settings	Maintains definitions and metadata, monitors quality, resolves data issues, advises users on correct use
Data custodian	IT, a platform team or an external provider that runs the system	How the owner’s requirements are implemented technically	Operates storage, access controls, backups, logging, security measures and secure deletion as directed
Data user	Any staff member, contractor or system that works with the data	Nothing about the rules; they decide only how to do their task within them	Uses data for approved purposes only, follows handling rules, reports errors, misuse and suspected breaches

Two points are easy to miss. First, a custodian is not the owner. The IT team or a cloud provider may hold the data, but it should not decide who gets access or how long records are kept. Second, accountability stays with the organisation even when a supplier is the custodian. The OAIC’s APP 11

guidance notes that an entity can still hold personal information stored by a third party, and lists third party providers, including cloud computing, as an area where reasonable security steps are needed.

Why this matters for privacy obligations

Under APP 11, organisations covered by the Privacy Act must take reasonable steps to protect personal information and to destroy or de-identify it when it is no longer needed. Since 11 December 2024, APP 11.3 makes clear that those reasonable steps include technical and organisational measures. The OAIC gives staff training and written procedures as examples of organisational measures. The law does not prescribe data governance roles, but it is hard to show organisational measures are working if nobody is accountable for a dataset.

Six signs your roles are unclear

- ☐ **Access requests go to IT and IT decides.** If the custodian approves access by default, the business is not making the risk decision.
- ☐ **Nobody can name the owner of your most sensitive dataset.** Try it for customer records, HR files or health information. Hesitation is the answer.
- ☐ **The same term means different things in different reports.** “Active customer” or “employee” counts that do not reconcile point to missing stewardship.
- ☐ **Data is never deleted.** If no one has authority to approve disposal, records accumulate, and so does breach exposure.
- ☐ **New uses are approved informally.** A dataset is used for analytics, AI or sharing with a partner because someone asked, not because an owner considered it.
- ☐ **During an incident, the first hour is spent finding the right person.** If your breach response depends on working out who owns the affected data, the roles are not settled.

If two or more of these apply, it is usually a sign that roles exist on paper, or not at all, rather than in daily practice.

Questions to ask internally

- Who is the owner of each of our three to five most important datasets, by name or position?
- Do our stewards and custodians know which decisions are theirs and which they must escalate?

- Are supplier custodians bound by contract to follow our instructions on access, security and deletion?
 - Does our breach response plan refer to data owners, so decisions can be made quickly?
-

Next step

A short conversation about where accountability for your key datasets currently sits is often enough to see whether the gaps are minor or structural. Lexora's data governance framework work helps organisations define roles that fit their size and existing teams.

General information, not legal advice. Role titles and responsibilities should be tailored to your organisation, and you should seek advice on your specific obligations.

Sources

1. Department of Finance, Australian Government Data Governance Framework (September 2025)
<https://www.finance.gov.au/sites/default/files/2025-09/Data-Governance-Framework.pdf>
2. OAIC, Australian Privacy Principles guidelines, Chapter 11 (APP 11 security of personal information)
<https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-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.