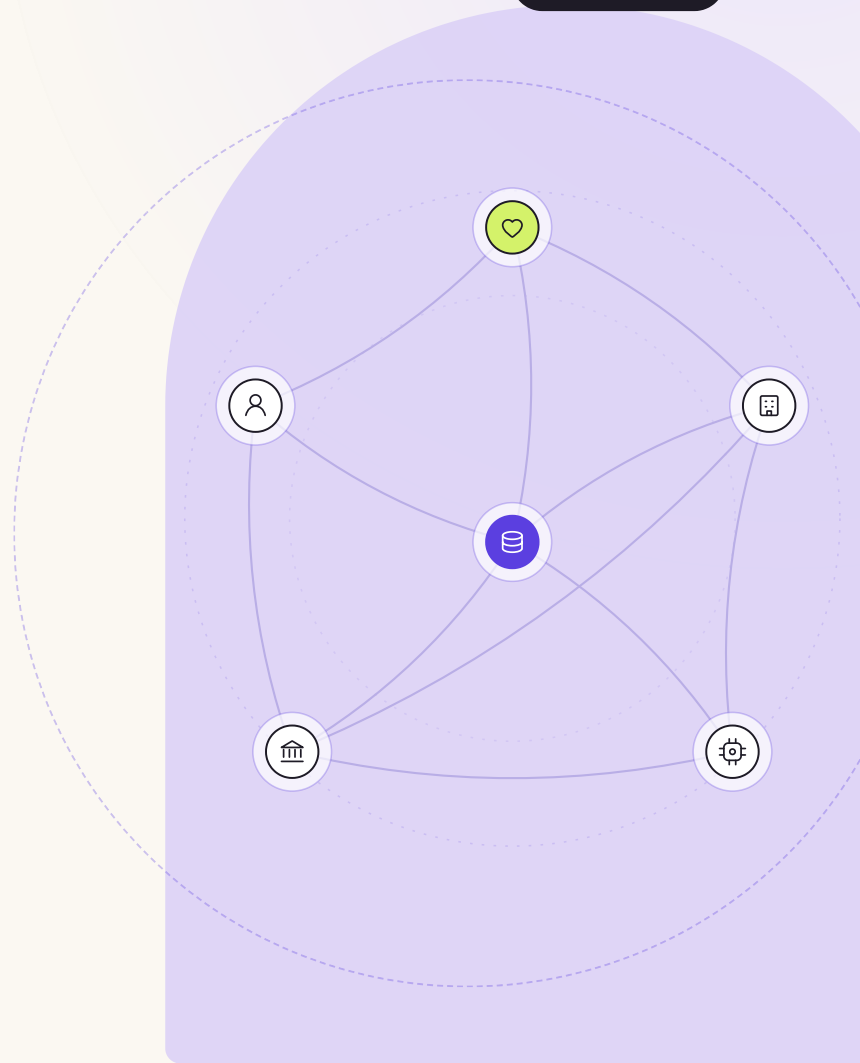




FREE GUIDE



QUESTION SET · PRIVACY & DATA PROTECTION

Supplier privacy due diligence questions

Eighteen questions to ask any supplier that will handle personal information for you, covering data location, security, breaches, sub-processors, deletion and AI.

Updated 17 October 2026

Law in force

lexoraai.com.au

When a supplier stores, processes or accesses personal information for you, your obligations under the Privacy Act do not transfer to them. Your organisation still has to take reasonable steps to protect that information, and in some cases you remain accountable for what the supplier does with it. Asking the right questions before you sign, and at renewal, is one of the simplest ways to show those reasonable steps.

Use these questions to start the conversation. The answers tell you where the risks are; they do not replace a contract review or a proper assessment of the supplier.

Data location and cross-border disclosure (APP 8)

Before disclosing personal information to an overseas recipient, an organisation must generally take reasonable steps to ensure the recipient does not breach the Australian Privacy Principles. Under section 16C, the disclosing organisation can be accountable for the overseas recipient's acts that would breach the APPs. The OAIC's guidance explains that giving information to a cloud provider purely for storage may be a use rather than a disclosure, but only where a binding contract limits the provider, subcontractors are bound, and you keep effective control.

1. In which countries will our data be stored, processed or accessed, including for support, backups and disaster recovery?
2. Can you commit contractually to keeping data in a specified location, and will you tell us before that changes?
3. Will your staff or affiliates overseas be able to view our data, and in what circumstances?
4. Does the contract limit you to handling our data only on our instructions, and let us access, retrieve and delete it at any time?

Security (APP 11)

APP 11 requires reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. Since 11 December 2024, APP 11.3 confirms that those steps include technical and organisational measures. The OAIC lists third party providers, including cloud computing, as an area where reasonable steps are needed.

5. What independent security assessments or certifications do you hold, and can we see the current report or summary?
6. How is our data encrypted in storage and in transit, and who manages the keys?
7. How do you control and log staff access to customer data, and how often is access reviewed?
8. Is our data logically separated from other customers' data?

Breach notification and cooperation (NDB scheme)

Where information is held by more than one entity, an eligible data breach of one is generally a breach of each. The Privacy Act allows one entity's assessment and notification to satisfy the obligations of the others (sections 26WJ and 26WM), but if nobody notifies, each may be in breach. The OAIC suggests the entity with the most direct relationship with affected individuals should usually notify them. You will usually need a supplier's facts quickly to complete your own assessment within 30 days.

- 9. How quickly will you tell us about a suspected incident affecting our data, and through which contact?
- 10. What information will you give us, and will you support our assessment of whether it is an eligible data breach?
- 11. Who will notify affected individuals and the OAIC if a breach occurs in your systems, and is that agreed in writing?

Sub-processors

- 12. Which sub-processors or subcontractors will handle our data, where are they, and what do they do?
- 13. Are they bound by obligations at least as protective as yours, and will you tell us before adding or changing one?

Retention, return and destruction

APP 11.2 requires reasonable steps to destroy or de-identify personal information once it is no longer needed for a permitted purpose. The OAIC notes this extends to backups and archived copies, and that for cloud data you should instruct the provider and take steps to verify destruction.

- 14. How long do you keep our data, including backups and logs, during and after the contract?
- 15. On termination, how will you return our data, in what format, and how quickly?
- 16. How will you destroy remaining copies, and what confirmation will you give us?

AI use of your data

The OAIC's guidance on commercially available AI products recommends checking service terms and settings to see whether a developer can access input or generated data, including for training, and warns that secondary uses such as model training are hard to justify as reasonably expected by individuals.

- .7. Do you use our data, or data generated from it, to train or improve AI models, yours or a third party's? Can that be switched off by contract?
- .8. Which features of your service use AI on our data, which third-party AI providers are involved, and where is that processing done?

Reading the answers

- ☐ Vague answers on location or sub-processors are a reason to ask again, not a reason to proceed.
- ☐ Anything promised in a sales conversation should appear in the contract.
- ☐ Record the answers and the date. They are part of your evidence of reasonable steps.
- ☐ Revisit the questions at renewal and when the supplier changes its service.

Next step

If several suppliers hold your most sensitive personal information, a structured review of those arrangements is usually more efficient than one-off questionnaires. Lexora's data protection review looks at supplier arrangements alongside your other privacy controls.

General information, not legal advice. Supplier contracts and cross-border arrangements should be reviewed by your legal adviser.

Sources

1. OAIC, APP guidelines Chapter 8 (APP 8 cross-border disclosure of personal information)
<https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information/>
2. OAIC, APP 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>
3. OAIC, Data breach preparation and response, Part 4 Notifiable Data Breach (NDB) scheme
<https://www.oaic.gov.au/privacy/notifiable-data-breaches/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme>
4. OAIC, Guidance on privacy and the use of commercially available AI products
<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products>



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.