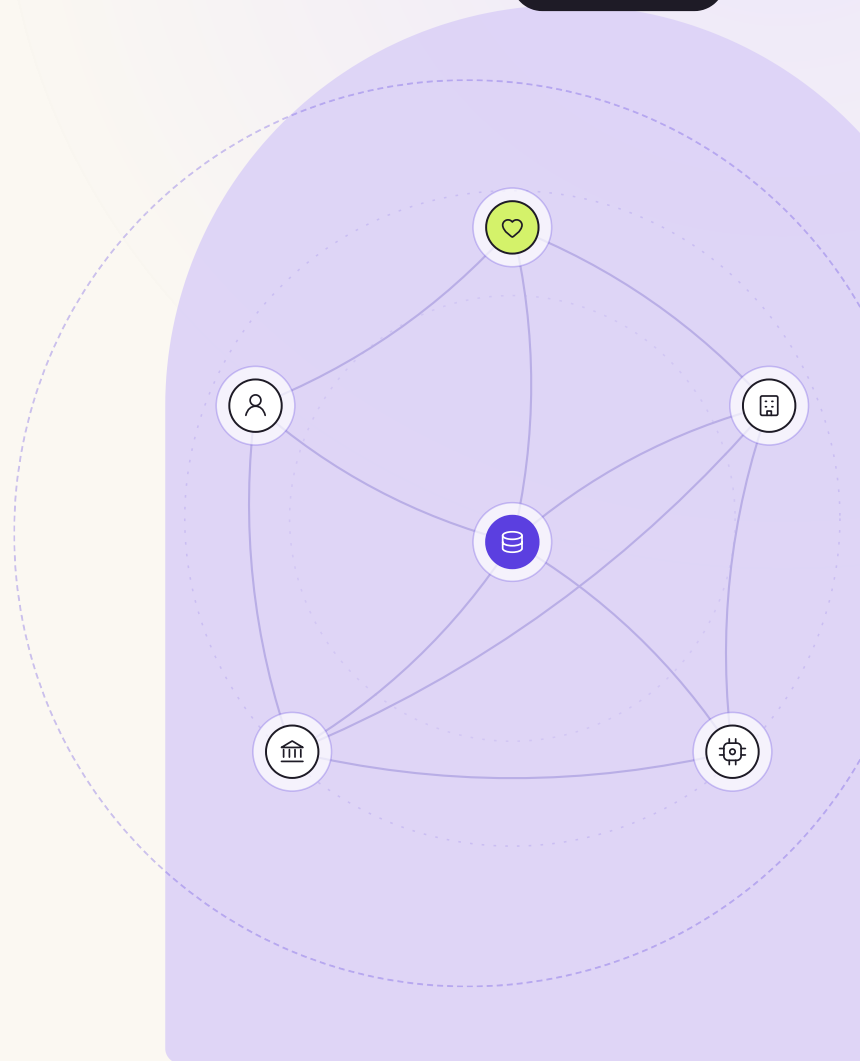




FREE GUIDE



QUESTION SET · PRIVACY & DATA PROTECTION

Privacy impact assessment screening questions

Eighteen screening questions to help decide whether a new project, system or change needs a privacy impact assessment, grouped by theme.

A privacy impact assessment (PIA) is a systematic assessment of a project that identifies its impact on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact. The OAIC says that to be effective, a PIA should be an integral part of project planning, not an afterthought. It is far cheaper to change a design than to fix a live system after a complaint or a breach.

Is a PIA required?

It depends on who you are.

- **Australian Government agencies** covered by the Privacy Act must conduct a PIA for high privacy risk projects. This is required by section 12 of the Privacy (Australian Government Agencies – Governance) APP Code 2017. The OAIC explains that a project may be a high privacy risk project if the agency reasonably considers it involves new or changed ways of handling personal information that are likely to have a significant impact on individuals' privacy.
 - **Private sector organisations** are not required by the Privacy Act to conduct PIAs. The OAIC encourages them to do so, and a PIA is one of the most practical ways to show that privacy has been considered from the start of a project.
-

Start with a threshold assessment

The OAIC's Guide to undertaking privacy impact assessments recommends a threshold assessment for every project. The first question is simply whether personal information will be collected, stored, used or disclosed at all. If it will, the guide suggests recording a short description of the project, what personal information is involved and how sensitive it is, any changes to how existing information is handled, and whether a full PIA will proceed.

The questions below are a way to structure that threshold step. They are not a scoring tool. A "yes" to any one of them is a reason to look more closely, and several "yes" answers usually point towards a full PIA.

The information involved

1. Will the project collect, use, store or disclose personal information, including information that could identify someone when combined with other data?
2. Will it involve sensitive information, such as health, biometric, racial or ethnic origin, or criminal record information?
3. Will it involve a large quantity of personal information, or information about a large number of people?

- 4. Will it involve information about children or other people who may be vulnerable?
 - 5. Is this an entirely new collection, or a new use or disclosure of information you already hold?
-

How it will be handled

- 6. Will the project combine, match or link datasets that were previously kept separate?
 - 7. Will it use new technology, or use existing technology in a new way, such as AI, biometrics, tracking or location data?
 - 8. Will a computer program make, or substantially contribute to, decisions that could significantly affect individuals?
 - 9. Will it involve monitoring or surveillance of customers, staff or the public?
 - 10. Will individuals be required to provide information, with no real choice?
-

Who else is involved

- 1. Will a supplier, contractor or cloud provider handle the personal information for you?
 - 2. Will information be shared with other organisations, or across sectors or government?
 - 3. Will personal information be stored or accessed outside Australia?
-

Impact on people

- 4. Could the project affect key aspects of someone's life, such as their livelihood, housing, health, reputation, or access to services or entitlements?
 - 5. Could a mistake, misuse or breach cause serious harm to the people involved?
 - 6. Would the people affected be surprised by how their information is being used?
 - 7. Is the project likely to attract significant community or media interest?
-

Changes to what already exists

- 8. Is the project a significant change to an existing system, process or purpose that already handles personal information?

What the answers tell you

The OAIC's guide notes that the need for a full PIA grows with a project's complexity and privacy scope. It lists factors such as large quantities of personal information, sensitive information, outsourcing, new technology, data matching, compulsory collection, and impacts on key aspects of people's lives. These map directly to the questions above.

If you decide not to proceed to a full PIA, record the threshold assessment and the reasons. If the project changes, run the questions again. The OAIC also notes that projects using de-identified data may still warrant a PIA, to show how re-identification will be prevented.

Next step

Lexora helps organisations build a privacy governance framework, including when and how PIAs are triggered and who signs them off. If you would like to discuss a specific project first, book a free 20-minute call.

General information, not legal advice. Lexora is not a law firm. For advice on whether a PIA is required in your circumstances, consult a qualified legal adviser.

Sources

1. OAIC, Guide to undertaking privacy impact assessments
<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments>
2. OAIC, When do agencies need to conduct a privacy impact assessment?
<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/government-agencies/australian-government-agencies-privacy-code/when-do-agencies-need-to-conduct-a-privacy-impact-assessment>



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.