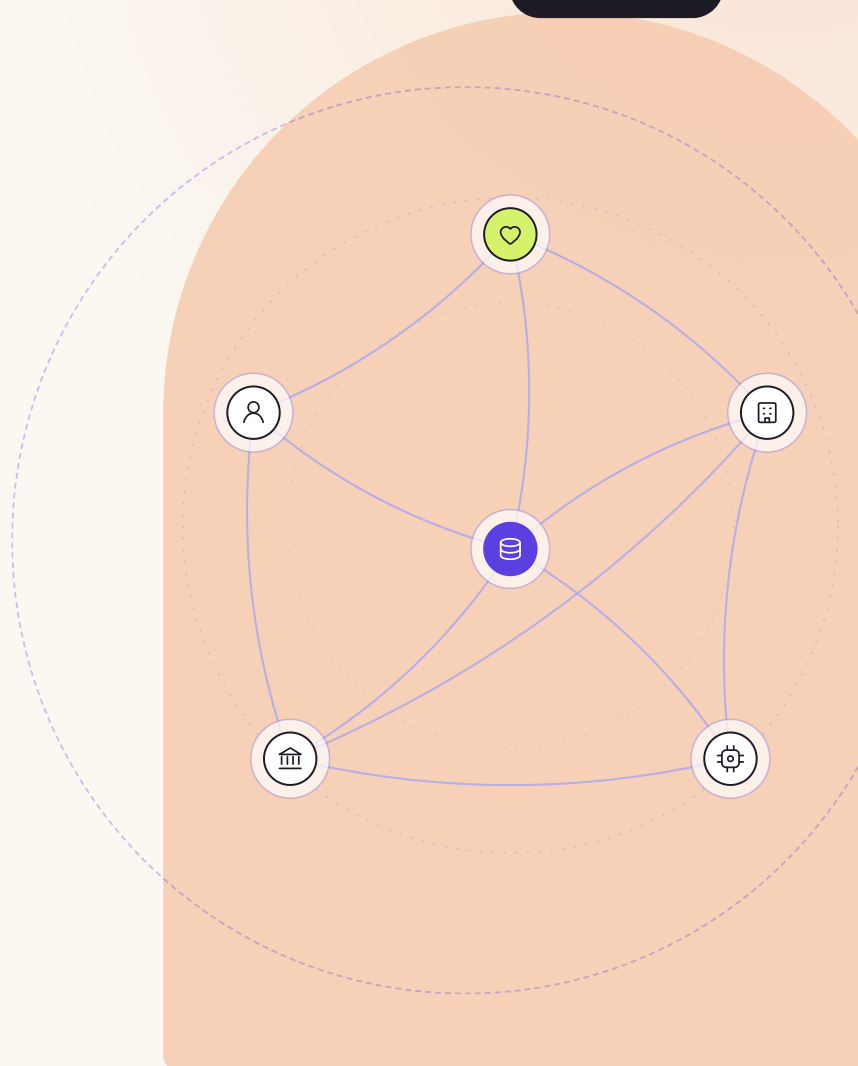




QUESTION SET · REGULATORY BRIEFINGS

Questions boards should ask about privacy, data and AI

Twelve questions directors can put to management on privacy, data and AI, with a line on why each one matters.

Privacy, data and AI now sit squarely within board oversight. The Australian Institute of Company Directors (AICD), in the June 2026 update of its Director's Guide to AI Governance prepared with the Human Technology Institute at UTS, says board oversight of AI and AI-related risk forms part of directors' existing duties under the Corporations Act 2001, including acting with care and diligence. The same logic applies to privacy and data more broadly.

Directors do not need to be technical specialists. They do need to ask the right questions and expect clear, evidence-based answers. The questions below are a starting point for a board or risk committee discussion.

Accountability

1. Who in management is accountable for privacy, for data governance and for AI, and how do they report to the board? Why it matters: without named owners and a reporting line, issues surface late or not at all.

2. What does the board receive, how often, and does it show where risk is rising? Why it matters: the AICD guide recommends reporting that shows where AI is used, how it performs and where risks are increasing, in plain language.

Personal information

3. Do we know what personal information we hold, where it is, and why we keep it? Why it matters: you cannot protect, disclose accurately or delete information you have not identified.

4. When did we last review our privacy policy and collection notices against what we actually do? Why it matters: these documents are public statements, and they must match practice.

5. Are we ready for the automated decision-making disclosures that apply from 10 December 2026? Why it matters: amendments made by the Privacy and Other Legislation Amendment Act 2024 require privacy policies to describe certain uses of personal information in computer programs that make, or help make, decisions significantly affecting individuals.

6. Has management considered our exposure to the statutory tort for serious invasions of privacy? Why it matters: since 10 June 2025, individuals can sue for serious invasions of privacy that were intentional or reckless, and the tort is not limited to entities covered by the Australian Privacy Principles.

Data breaches and security

7. If we discovered a data breach tomorrow, who would lead the response, and when was the plan last tested? Why it matters: under the Notifiable Data Breaches scheme, eligible breaches must be notified to affected individuals and the OAIC, and an untested plan tends to fail under pressure.

8. Which suppliers hold or can access our personal information, and what do our contracts require of them? Why it matters: information held or accessed by suppliers can still expose your organisation, and customers will look to the organisation they dealt with.

AI

9. Do we have a current register of the AI systems in use, including AI features inside existing software? Why it matters: the AICD guide recommends an AI register that tracks approved systems and is updated regularly.

10. What is our risk appetite for AI, and does it differ by use case? Why it matters: a drafting assistant and a system that screens job applicants carry very different risks and need different levels of oversight.

11. Where is AI used in decisions about customers, staff or the public, and who reviews those outputs? Why it matters: accuracy, fairness and transparency risks are highest where AI influences decisions about people.

Assurance

12. How do we know our controls work, and when were they last independently reviewed? Why it matters: policies show intent; testing and review show whether the organisation is actually doing what it says.

Using the questions well

- Ask for evidence, such as a register, a test report or a review date, not just assurance.
- Revisit the questions at least annually, and after a major incident, acquisition or new technology rollout.
- Note the AICD's caution that directors should not rely on AI-generated summaries in place of their own review of board papers.

Next step

Good answers to these questions take regular, informed input. Lexora's ongoing advisory service supports boards and management with briefings on privacy, data and AI as the rules change.

General information, not legal advice. It does not address the specific duties of any director or organisation, and directors should obtain their own legal advice.

Sources

1. AICD and Human Technology Institute (UTS), A Director's Guide to AI Governance, Version 2 (June 2026)
<https://www.aicd.com.au/news-media/research-and-reports/a-directors-guide-to-ai-governance>
2. AICD, A Director's Guide to AI Governance (PDF)
<https://www.aicd.com.au/content/dam/aicd/pdf/news-media/research/2026/director-guide-to-ai-governance.pdf>
3. OAIC, Notifiable Data Breaches scheme
<https://www.oaic.gov.au/privacy/notifiable-data-breaches>
4. Privacy and Other Legislation Amendment Act 2024 (Cth)
<https://www.legislation.gov.au/C2024A00128/asmade/text>
5. OAIC, Statutory tort for serious invasions of privacy
<https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/statutory-tort-for-serious-invasions-of-privacy>



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.