AUSTRALIAN AI READINESS CHECKLIST

15 points to run before any team member touches an AI tool with company or client data.

By Ravijeet Dang — AI advisor, Melbourne. ravijeet.com

1. Data mapping (do this first)

1	List every place company or client data currently leaves the business (email, cloud tools, AI chats, third parties).	☐
2	Mark which flows contain personal information (names, emails, financials, health).	☐
3	Identify any AI tool staff use informally — including their own accounts.	☐

2. Privacy obligations

4	Confirm whether the Privacy Act / APP 11 applies to you (revenue or data volume thresholds).	☐
5	Decide what personal data is permitted into AI tools, and what is banned outright.	☐
6	Have a process to assess a notifiable breach if data does escape.	☐

3. Local-first fallback

7	For sensitive work, trial a local / on-prem model so data never leaves your infrastructure.	☐
8	Document which tasks are safe on public tools vs. which need local-first.	☐
9	Keep a vendor-independent fallback so a price/term change can't halt your workflow.	☐

4. Vendor & data residency

10	Record where each AI vendor stores and processes data (AU / US / EU / elsewhere).	☐
11	Check the contract: does the vendor train on your inputs? Push back if so.	☐
12	Confirm data-residency and deletion terms match your obligations.	☐

5. Accountability & audit

13	Name one person accountable for AI risk.	☐
14	Publish a short, readable AI usage policy and get acknowledgement.	☐
15	Be able, on demand, to show what data flows to which AI vendor.	☐

Most breaches aren't malicious — they're helpful people pasting data into the wrong tool. Map the flows first, then pick the model. If you want a 30-minute walkthrough of your real exposure, book a call at ravijeet.com/contact.html.