GOVERNANCE, PRIVACY AND SECURITY // QUESTIONS TO ASK

Five questions to ask before AI goes near your customer data

Written for owners without an IT or legal team. You don't need to be a security expert, just to ask the right questions of any AI tool or provider before the data moves.

Travis's short version: most data problems with AI come from not asking, rather than from anything exotic. These five questions work for any tool, any vendor and any consultant, including us.

Ask them in writing

Put these to the provider before you sign up or switch a feature on, and keep the answers. A good provider answers plainly and in writing. A vague answer is information too. You don't need a technical or legal background, and if a provider can't explain something in plain English, that tells you something.

1. Where does our data go, and who can see it?

Know the journey before the data takes it.

Why it matters. Information typed into an AI tool is usually sent to servers run by the vendor or its partners, sometimes overseas. You are still responsible for the customer and business information you hand over. In a small business, a common risk is a well-meaning staff member pasting a customer list or a contract into a free chatbot.

A good answer. A clear description of what is sent, where it is processed and stored, which subcontractors are involved, and which of their staff can access it.

A warning sign. "Don't worry, it's secure" with no detail.

2. Will our data be used to train the AI?

Check the default, because it differs between products and plans.

Why it matters. Some products may use what you enter to improve their models unless you switch that off. Business plans often handle this differently from free or consumer ones, so check the current terms for your exact product. Your customer lists, pricing and job history are the commercial heart of a small business, so it matters where they end up.

A good answer. A written statement that your inputs and outputs are not used for training, or a setting you can turn off and confirm.

A warning sign. Terms that are hard to find or that change without notice.

3. What happens to our data when we stop?

Plan the exit on day one.

Why it matters. Data can sit in logs, backups and connected tools long after you stop using a service. If you change your accounting or job software next year, you will want your data back in a usable form.

A good answer. A stated retention period, a way to export your data, and confirmation that it is deleted, including backups, when you leave.

A warning sign. No deletion process, or "we keep everything".

4. Who is accountable when it gets something wrong?

AI makes mistakes. Decide who catches them.

Why it matters. AI output can sound confident and still be wrong. Where a mistake would hurt a customer, a person should review the work before it goes out, and you should be able to see what was sent and why. Without an IT department, the owner is usually the one answering to the customer.

A good answer. A human check where it matters, a log of what the system did, and a named person on your side who owns the result.

A warning sign. “The AI decides” with no way to review or reverse it.

5. Does this fit our privacy obligations?

Know which rules apply to you before you start.

Why it matters. If your turnover is over $3 million, the Privacy Act applies to you. Under $3 million you may be exempt, but not if, for example, you provide health services or trade in personal information, and reforms are expected. Either way, your customers expect their details to be handled carefully.

What is changing. From **10 December 2026**, if the Privacy Act applies to you, your privacy policy must say what kinds of decisions are made by automated tools, including AI, when they significantly affect people and use their personal information.

A good answer. You know whether the Act applies to you, your privacy policy reflects how you use AI, and you only share the minimum personal information a task needs.

Simple habits that cost nothing

Do	Avoid
Use business accounts with the privacy settings checked.	Don’t paste customer or sensitive details into free public chatbots.
Share the minimum information a task needs.	Don’t give a tool more access than the task needs.
Keep a person checking anything that reaches a customer.	Don’t switch on a new AI feature without checking what it does with your data.

General information only, not legal advice. Check the current rules with the Office of the Australian Information Commissioner (oaic.gov.au) or your own adviser.

Want to talk this through for your business?

Book a free 15-minute call. We’ll look at your situation and give you a straight answer, with no jargon and no sales pitch.

Let’s Chat Opens the request form on our website. Free, no obligation.