

AI Vendor Security Checklist

Eight questions to send any AI vendor, in one email, before the demo. A vendor should answer all eight in writing within a week; the speed and format of the answers are findings too.

1. Where does the data physically live?

Ask for jurisdiction and infrastructure provider, not "the cloud". If clients require North American servers, confirm before signature.

Answer received: ☐ in writing ☐ verbal only ☐ none Date: _____

2. Is it dedicated hardware or shared infrastructure?

Shared cloud with logical separation is reasonable; what matters is that the vendor says so plainly.

Answer received: ☐ in writing ☐ verbal only ☐ none Date: _____

3. What happens to the data before it reaches a model?

What is removed or masked before content is sent for processing, and what is not.

Answer received: ☐ in writing ☐ verbal only ☐ none Date: _____

4. Does your agreement with the model provider differ from consumer terms?

Ask for the substance of the commercial agreement, in writing.

Answer received: ☐ in writing ☐ verbal only ☐ none Date: _____

5. Is our data used for training?

Two questions: the vendor's own models, and any third party's. A single denial usually covers only the first.

Answer received: ☐ in writing ☐ verbal only ☐ none Date: _____

6. What are the retention and deletion terms?

What is kept, for how long, what deletion removes, and whether it reaches backups. Check against your own record-retention obligations.

Answer received: ☐ in writing ☐ verbal only ☐ none Date: _____

7. What happens if the vendor disappears?

Fire, outage, acquisition, insolvency: can you export every document in a usable format without the vendor's cooperation?

Answer received: ☐ in writing ☐ verbal only ☐ none Date: _____

8. Who at the vendor can see our content?

The internal access model: limited, logged, and disclosed is the reasonable answer.

Answer received: ☐ in writing ☐ verbal only ☐ none Date: _____

Keep the answers on file. If a client asks where their data has travelled, the reply should come from a document you hold.

tenerapro.com/reports/blog/what-your-it-should-ask-an-ai-vendor