

The AI Vendor Vetting Card

From the COO Seat — The Free Vault · Vault 003 · Version 1.0 · August 2026

Ten questions before you sign. Thirty minutes of asking beats a year of finding out.

The card

1. **Where does our data go — processing, storage, and who else touches it?**
2. **Is our data used to train your models? Anyone's models? How do we opt out?**
3. **What happens to our data if we leave? Format, timing, and cost.**
4. **What do you log, how long do you keep it, and who at your company can see it?**
5. **What happens to our workflow when the underlying model changes or disappears?**
6. **What's your uptime and incident history — specifically for the AI features, not the whole product?**
7. **Where does liability sit when an AI output causes damage — wrong answer, bad decision, leaked data?**
8. **What EU / state privacy regimes do you support, and which are on us?**
9. **What did your last two security reviews find, and what changed because of them?**
10. **Who owns AI compliance at your company, and will you put me in touch?**

Answers that should make you walk

- “We can't share that” on data handling (Q1-2). If they can't tell you where your data goes, they've told you.
- “Retention is at our discretion” (Q4). That's forever, in a trench coat.
- “Liability is addressed in the terms of service” (Q7) — with no stated cap or coverage. Read the TOS. If their liability floor is a month of fees, that's the real price of the tool.
- “We don't have a compliance owner” (Q10). Someone always does, even if the title is made up. If they can't name them, the role is nobody's.

The email that sends the card

Subject: [Product] — security & AI questions before we proceed

Hi [NAME] — we're close to a decision on [PRODUCT]. Before we sign, our process requires written answers to ten questions on data handling, model changes, and liability (attached). Public documentation links are perfectly fine answers where they exist. Could we have these by [DATE — give them a week]?

How to read the replies

Green: specific, dated, names a person. Amber: general but honest (“we don't support that yet — here's the roadmap”). Red: vague, salesy, or silent. Two reds, and you have your answer — whatever the demo looked like.

*Free vault item. Provided as-is. Nothing here is legal or procurement advice — it's an operator's card.
Full terms: same rules, no price. Our total liability is \$0.00.*