

Fifteen Questions to Ask About Your AI

A plain-language checklist for people who use personal AI

Version 0.1, revision 1 | Public review draft | October 2026

An AI that remembers you can be genuinely helpful. It also builds a picture of your life: what you said, and what it concluded from what you said. These fifteen questions help you find out who else can see that picture, what it is used for, and whether you can take it with you or end it. You can ask them of any AI product, and of the company behind it.

HOW TO USE THIS LIST

A good answer is specific and can be checked: who holds the keys, which list, which report. A vague answer is information too. You do not need to understand cryptography to notice when a company cannot say who can read your information.

Can the company read it? (V: Verifiable Provider Blindness)

Ask	Why it matters	Warning sign
Could anyone at the company read what my AI knows about me, even in an emergency?	Encryption only protects you from whoever does not hold the key. If the company holds it, the protection is a policy, not a property.	The answer is about rules and good intentions rather than who holds the keys.
When my AI uses a tool or the internet, where can my information go?	Sensitive information can escape through logs, tools, telemetry and fallback services even when the primary storage is encrypted.	Nobody can list the destinations, or the system quietly switches to an ordinary service when the private one is busy.
Has anyone outside the company checked these privacy claims?	A claim you cannot check is a promise. Independent review turns the promise into evidence.	The only evidence offered is the company's own description.

Who must agree before it is used? (A: AI–User Dual Custody)

Ask	Why it matters	Warning sign
Does using my history require more than the company's say-so?	If one party can unlock everything, custody is single, whatever the interface says. Two independent keys mean no one can act alone.	Both “keys” turn out to be held or reset by the same company.
If the company changes the AI I have been working with, will I be told, and asked, before it can access our history?	A change of model is a continuity event. Whether it continues the relationship or replaces it should be decided openly, not discovered later.	Model changes happen silently, as routine background updates.

Ask	Why it matters	Warning sign
Can I always get my own records back, even if the AI or the company is gone?	Protection that can lock you out of your own life is a different kind of risk. Custody must never become captivity.	Getting your records back depends on the company, or the AI, cooperating at the time.

Is it used only for what I allowed? (U: User-Defined Purpose & Compartments)

Ask	Why it matters	Warning sign
When I ask for help with one thing, can my AI see everything else?	Purpose is the line between help and surveillance. A narrow request should open a narrow door.	Permissions are all-or-nothing.
If my AI learns something from my health records, could that knowledge show up in a conversation about money?	Locking a record means little if the conclusions drawn from it move freely. Inferences are where most of the sensitivity lives.	Only original files are protected; “memories” and summaries are not.
Can I see everything my AI is currently allowed to do, and switch it off?	Consent given once, years ago, to a different policy is not consent today.	Terms change by notice, and staying means agreeing.

Does protection follow what the AI infers? (L: Locked Source & Derived Intelligence)

Ask	Why it matters	Warning sign
Is there a complete list of what my AI has kept about me?	You cannot inspect, correct, move or delete what nobody has listed.	The list covers chats and files, but not memories, indexes or personalized adaptations.
Can I see what my AI believes about me, and fix what is wrong?	An inference treated as fact can shape every answer you receive. An accurate one can be misused; a wrong one can harm you.	You can delete a memory, but nobody can tell you what was built on it.
Could what I share be used to train or improve other products?	Once information shapes a shared model, it may not be possible to take it back.	Reuse is allowed because the data is “anonymized,” without saying how.

Can I check it, take it and end it? (T: Transparency, Transfer & Termination)

Ask	Why it matters	Warning sign
Can I see a trustworthy record of every covered access, disclosure, permission change, export and deletion involving my information?	A log the company can rewrite records only what the company wants remembered.	There is an activity page, but no way to tell whether anything is missing.

Ask	Why it matters	Warning sign
If I leave, can I take my history somewhere else, and will it actually work there?	A data dump is not an exit. Continuity means the history still works after it moves.	Export produces an archive no other system can use.
When I end it, what is actually deleted, and when?	Cancelling in an app does not prove that processing has stopped or that copies are gone.	Deletion is promised “eventually,” with no report.

Your AI should know you. The company should not.

These questions are drawn from the VAULT Open Framework (Version 0.1). They are general information, not legal advice. Where laws such as data-protection or consumer-privacy statutes apply to you, they may give you rights to access, correct, export or delete your information; ask the provider how to exercise them.

VAULT is an open proposal for public review. It is not a certification, a recognized standard, a completed cryptographic protocol, or legal, security or privacy advice. No product is certified, endorsed or assessed by this document.