

Questions for an AI vendor

Ask in writing before you approve a tool, and keep the answers, dated, with its line in the register. These are questions only: the answers are the vendor's to give, and they change.

YOUR INFORMATION

- ☐ Where is our information processed and stored?
- ☐ Is anything we put in used to train or improve your models?
Can we switch that off for the whole organisation?
- ☐ How long do you keep prompts, files, outputs and logs? Can we delete them, and how quickly?
- ☐ Who at your company can see our information, and when?
- ☐ Which other companies process it for you, and where is that list?

ACCOUNTS AND CONTROL

- ☐ Do we get work accounts the organisation controls, with an admin console?
- ☐ Can we use single sign-on and two-step sign-in?
- ☐ Can we see who has access, and remove someone on their last day?

CONNECTIONS AND ACTIONS

- ☐ Which apps can it connect to? Can each connection be set to read only?
- ☐ Can it act on its own: send, pay, delete, book or change files?
Where is the approval setting, and can an admin lock it?
- ☐ Can it run tasks on a schedule, or when something happens?
Who can see and stop them?
- ☐ Does it keep a log of what it did that we can read?

MEMORY

- ☐ What does it remember between chats or tasks? What is the setting on our plan, and can an admin set it for everyone?
- ☐ If we disconnect an app, is what it already learned from that app deleted?

SECURITY AND PROBLEMS

- ☐ Which independent security audits or certifications do you have, and can we see the reports?
- ☐ How, and how fast, do you tell customers about a security incident?
- ☐ What do you do to reduce the risk of prompt injection?

CONTRACT AND EXIT

- ☐ What does our plan include, and what would change what we pay?
- ☐ Can we export our information if we leave, and is it deleted afterwards?
- ☐ How will you tell us before you change features, terms or how you use our information?

RECORD THE ANSWERS

Vendor and tool

Asked on

Answers kept with

Add the date and where the answers are kept to the tool's line in the register, and ask again at its review date.

Ask your adviser about

Topics to raise with your legal, HR, data protection or IT security adviser before you approve the policy. Take the filled-in policy and the register with you.



01

Data protection

Which personal data may our AI tools touch, and what must we do before they do?

02

Staff monitoring

Do any of our tools watch, score or record what staff do, and what does that mean for us?

03

Who owns AI output

Who owns what our AI tools make, and what do our client contracts say about it?

04

Sector rules

Do rules for our sector, or our clients' sectors, limit how we may use AI?

05

Recordings

What consent and keeping rules should apply when AI records, transcribes or summarises calls and meetings?

06

Telling customers

When must we, or should we, tell customers and the public that AI was used?

Also worth raising: the caution page on AI in hiring and staff decisions, and the note on Article 4 in the training record.

OUR ADVISER _____

DATE WE SPOKE _____