Questions to ask before you buy an AI agent

A UK supplier checklist · AI Agents UK · aiagents.org.uk

Before you let an AI agent near customer or staff data, ask the supplier ten questions in writing. If they score under 10 out of 20, or fail on training, the DPA or the off switch, walk away or keep personal data out of it.

Use it whenever an AI tool will read, store or act on personal data (customer emails, CVs, invoices, patient or client records), or will act in your systems, such as sending emails, changing records or making payments. Under UK GDPR, if the supplier processes personal data for you, it's your processor and you must use only processors that give "sufficient guarantees" (Article 28).

The ten questions

Data and privacy

1. Where is our data stored, and where is it processed?

- **Good:** names regions ("stored in UK South; model inference in the EU; web search in the US") and puts it in the contract.
- **Bad:** "Our cloud is secure", or "Europe" with no detail.
- **Why:** transfers outside the UK need cover under UK GDPR.

2. Do you train or improve models on our data?

- **Good:** "No, not by default, and it's in the data processing agreement."
- **Bad:** "Only anonymised data", with no definition, or an opt-out buried in settings.

3. Who else processes our data?

- **Good:** a published sub-processor list, including any model provider (OpenAI, Anthropic, Google and so on), with notice of changes.
- **Bad:** no list, or "we use leading AI partners".

4. Will you sign a data processing agreement that covers UK GDPR?

- **Good:** a DPA naming them as processor, with the UK Addendum or IDTA for transfers.
- **Bad:** "Our terms of service cover it."

Security and control

5. What can the agent access, and can we limit it?

- **Good:** per-tool permissions, read-only options, approval before anything irreversible (sending, paying, deleting).
- **Bad:** one "connect everything" button.
- **Why:** NCSC and DSIT guidance both stress least privilege.

6. Is there a log of everything the agent did?

- **Good:** an exportable action log with timestamps and the data touched.
- **Bad:** chat history only.

7. How do we switch it off, fast?

- **Good:** a kill switch or admin revoke that stops all actions at once, plus a named incident contact and breach notice time in the contract.
- **Bad:** "Raise a support ticket."

Contract, cost and exit

8. What does it cost when usage spikes?

- **Good:** a price in pounds (or the dollar price with VAT treatment stated), clear usage limits, and a hard spending cap.
- **Bad:** "credits" with no cap, or overage billed after the fact.

9. How do we get our data back and deleted if we leave?

- **Good:** export in a standard format, deletion within a stated number of days, and written confirmation.
- **Bad:** no exit clause.

10. What happens to us if you change model, owner or terms?

- **Good:** notice period for material changes and a right to leave without penalty.
- **Bad:** "We may update these terms at any time."

How to score the answers

Score each answer 2 (clear, in writing, in the contract), 1 (clear but only on a web page or in an email) or 0 (missing, vague or bad).

Total out of 20	What it means
16-20	Reasonable to proceed with personal data, subject to your DPIA
10-15	Pilot with test or low-risk data only; chase the gaps
Under 10, or a 0 on question 2, 4 or 7	Walk away, or use it with no personal data at all

Keep the completed sheet with your DPIA.

Scoring sheet

Supplier: _____ Tool: _____ Date: _____

#	Answer received (summarised)	Score (0, 1 or 2)
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
	Total	**/ 20**

Red flags that end the conversation

- They can't say which model provider they use.
- Training on your data is on by default, with no business plan that turns it off.
- No DPA, or a DPA that only mentions EU GDPR and not UK GDPR.
- The agent can send, pay or delete without any approval step.
- Pricing only in "credits", with no cap and no pound figure.

Sources

- UK GDPR Article 28 (processors), legislation.gov.uk
- ICO, guidance on AI and data protection and draft guidance on automated decision-making (31 March 2026)
- NCSC, Guidelines for secure AI system development (ncsc.gov.uk)
- DSIT, AI Cyber Security Code of Practice (gov.uk)

Full guide, with a worked example: aiagents.org.uk/ai-supplier-due-diligence-checklist

This checklist explains UK law and regulator guidance in plain English. It is general information, not legal advice. For a contract that matters, ask a data protection professional or solicitor to review it. Free to download and reuse with credit to AI Agents UK.