08. Supplier and AI vendor checklist

> **Template.** Part of the open-source AI App Policy Kit, version 1.0. Replace everything in [square brackets], delete what does not apply, and have the person who runs the business approve it. A starting point, not legal advice.

Business	[Business name]
Document owner	[Name and role]
Approved by, and date	[Name], [date]
Next review	[Date, at most 12 months on]

Why this matters

Your app runs on other companies: a host, a database, an AI model, a payment provider, an app builder. Under UK GDPR you answer for what they do with your customers' data. Ten minutes of questions before you sign up is cheaper than moving later.

Who it covers

Any supplier that stores, processes or can reach [Business name]'s data or its customers' data, AI tools and AI model providers included.

The rules

1. **Check before you use.** Complete the checklist below for each supplier before any real data goes in. [Policy owner] approves.
2. **Have a contract.** A supplier that handles personal data for you needs a data processing agreement. Most publish one: read it, accept it and keep a copy.
3. **Keep the register** of suppliers up to date. It is also your list of who to call in an incident and who appears in the privacy notice.
4. **Review every 12 months,** and when a supplier changes its terms, has a breach or changes owner.
5. **Have a way out.** For each supplier the app depends on, know how you would export your data and what you would move to.

Checklist for one supplier

Supplier: [Name] **Used for:** [Purpose] **Checked by:** [Name] **Date:** [Date]

Data

- ☐ We know what data of ours they will hold, and it is in the data map (document 02).
- ☐ We know the country where it is stored and processed. If outside the UK, the contract has a transfer safeguard.
- ☐ A data processing agreement is in place.
- ☐ They list the other companies they pass data to (sub-processors).
- ☐ We can export our data in a usable format, and they delete it when we leave.

For AI suppliers

- ☐ Their terms say they do not train models on our data, or we have switched it off.
- ☐ We know how long they keep prompts and outputs, and who at the supplier can read them.
- ☐ We know which model and version we use, and how much notice they give before retiring it.
- ☐ We know who owns the output and whether they offer any protection against copyright claims.
- ☐ Usage limits and spend alerts are available and set (document 04).

Security

- ☐ They hold an independent certificate or report: ISO 27001, SOC 2 or Cyber Essentials Plus.
- ☐ Two-step sign-in is available and switched on for our account, with single sign-on if we use it.
- ☐ They commit to telling us about a breach, and how quickly.
- ☐ They have a public status page and a record of past incidents.

Business

- ☐ We know the price as use grows, and what happens at the limits.
- ☐ They publish an uptime commitment and what they pay if they miss it.
- ☐ We know how to reach support, and how fast they answer on our plan.
- ☐ We have a plan if they close or triple the price.

Decision: [Approved / approved with conditions / refused]. **Conditions:** [ ]

Supplier register

Supplier	Used for	Personal data?	Country	Agreement in place	Trains on our data?	Checked on	Next review
[Name]	[Hosting]	[Yes]	[UK]	[Yes, link]	[No]	[Date]	[Date]
[Name]	[AI model]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

References

- ICO, *Contracts and liabilities between controllers and processors*.
- NCSC, *Supply chain security guidance* and *Cloud security guidance*.

AI App Policy Kit, version 1.0. © 2026 PugliseWeb LTD, licensed under CC BY 4.0: use it, change it and share it, with credit. The whole kit, and a free Software Health Check of your app against it: https://www.puglieseweb.com/ai-policy-kit