02. Data protection for AI apps

> **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

An app that holds personal data is covered by UK GDPR, however it was built. You must know what you hold, why, where it is kept and who can see it. An AI feature adds one more question: what is sent to the AI supplier, and what do they do with it?

Who it covers

Every app, database, spreadsheet and AI tool [Business name] uses to hold or process personal data.

The rules

1. **Keep a record of what you hold.** Fill in the data map below for every app. Update it when the app changes.
2. **Have a reason for each kind of data.** Write the lawful basis (contract, consent, legal obligation or legitimate interests) next to each. If you cannot name one, do not collect it.
3. **Collect less.** Ask only for what the app needs. Do not send a whole customer record to an AI model when a first name would do.
4. **Know where it lives.** Record the supplier and the country for each store of data, backups and AI suppliers included. Data held outside the UK needs a safeguard: an adequacy decision, or the UK International Data Transfer Agreement or Addendum in the supplier's contract.
5. **No training on customer data without a decision.** Use AI suppliers whose terms say they do not train their models on your data, or switch that off. Using customer data to train or fine-tune a model needs its own risk assessment (document 09).
6. **Tell people.** The privacy notice says what is collected, why, who receives it (AI suppliers named by category at least), how long it is kept and how to ask for a copy or deletion.
7. **Answer requests within one month.** A person may ask for a copy of their data, a correction or deletion. Log each request and the date it was answered (document 10 covers deletion).
8. **Protect it.** Encrypt data in transit and at rest, limit who can read it (document 03) and keep it out of logs and test systems (document 11).

9. **Special care for sensitive data.** Health, ethnicity, religion, biometrics, sexual life, trade union membership, criminal records and children's data need a second lawful condition and a risk assessment before any AI use.
10. **Register and pay the ICO fee** if the business processes personal data and no exemption applies.

Data map

App or tool	Personal data held	Why (lawful basis)	Where (supplier, country)	Sent to an AI supplier?	Kept for
[App name]	[Names, emails, order history]	[Contract]	[Supplier, UK]	[Yes: first name and message text to Supplier]	[6 years after last order]
[Tool name]	[ ]	[ ]	[ ]	[ ]	[ ]

Checklist

- ☐ The data map covers every app and was reviewed in the last 12 months.
- ☐ Each AI supplier's terms forbid training on our data, or the setting is off.
- ☐ Every transfer outside the UK has a named safeguard.
- ☐ The privacy notice matches the data map.
- ☐ Requests from individuals are logged with the date received and the date answered.
- ☐ The ICO registration is current. Reference: [number].

References

- ICO, *UK GDPR guidance and resources* and *Guidance on AI and data protection*.
- ICO, *International transfers*.

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.pugliseweb.com/ai-policy-kit