

AI rules, permits and data approval

Map jurisdiction, personal data and sector requirements before an AI pilot.

Updated October 29, 2026

Do not assume a software project needs a construction-style permit. Do not assume that the absence of such a permit removes legal duties. The applicable rules depend on the use, users, data and jurisdiction. Ask qualified local advisers to review the planned use.

Build an approval map

Write down where the business operates, where users are located and where providers process data. Name the business owner, privacy contact, security lead and legal reviewer. Record who can approve a pilot and who can approve production use. Keep sector requirements separate from general software procurement.

For UK personal data, start with the ICO's AI guidance. Review the purpose, lawful basis, fairness, transparency and data protection risks with your privacy team. The guide is a starting point, not a permit or approval certificate.

Make data use explicit

Inventory the data you plan to send. Record its source, access rights, sensitivity, retention and deletion process. Confirm whether the agency acts as a processor and what contracts are required. Check subprocessors and international transfers. A demonstration should use synthetic or approved data until access is cleared.

Control consequential actions

Hiring, lending, health and other consequential uses need careful sector review. Ask whether people can challenge an outcome. Define the human authority to stop or override the system. Do not let an agent send payments, change records or make commitments merely because a model produced plausible text.

Use the NIST framework to track unresolved risks and decisions. Use the NCSC guidance to review secure design, development, deployment and operation. Neither source is a universal legal compliance certificate. Recheck local law before launch and when the use changes.

Sources

- [ICO, Artificial intelligence guidance](#). Public page fetched 2026-10-29.
- [NIST, AI Risk Management Framework](#). Public page fetched 2026-10-29.
- [NCSC, Guidelines for secure AI system development](#). Public page fetched 2026-10-29.

Frequently asked questions

Is this a supplier recommendation?

No. Use this guide to prepare a brief and check the supplier evidence yourself.