Avantwerk | LEGAL AI

FREE RESOURCE · FOR SOLICITORS

Local or cloud AI: compare the actual information flows

For solicitors and small firms in England and Wales. Use this educational worksheet to compare two defined configurations for the same task. It does not cover Scotland or Northern Ireland and does not certify either option. “Local” and “cloud” describe parts of an arrangement; neither label establishes confidentiality, privilege or data-protection compliance.

Task: [complete]. **Information categories:** [complete]. **Option A and exact configuration:** [complete]. **Option B and exact configuration:** [complete]. **Reviewer and date:** [complete]. Use fictional material for tests. Record both observed behaviour and contractual assurances, distinguishing one from the other.

1. Draw the complete journey

For each option trace: source document → input preparation → prompt or upload → model or other processing → output → review → retained record → deletion or exit. Add side paths for search, retrieval, logs, diagnostics, backups, support and integrations. Identify the person or organisation controlling each step and who can access it.

A local document store can still send a prompt to an external model. A browser interface does not tell you where inference takes place. A cloud service may have configurable controls that need to be assessed individually. Check the selected plan and enabled features rather than another service from the same supplier.

2. Complete a side-by-side evidence table

For each row enter **A: answer and evidence / B: answer and evidence / unresolved issue / owner**.

QUESTION	RECORD FOR BOTH CONFIGURATIONS
Where is the authoritative matter record?	Host, controller, access and recovery arrangements
What leaves the firm?	Exact data categories, attachments, retrieved passages and identifiers

QUESTION	RECORD FOR BOTH CONFIGURATIONS
Where does processing occur?	Model provider, service, recipients and relevant locations
Who else can see it?	Staff, support, administrators, further processors and integrations
What is retained or reused?	Prompts, outputs, logs, backups, human review and training settings
What controls access?	Identity, permissions, matter separation and removal of access
What evidence supports security?	Assessed technical measures, configuration and test limits
How does the firm recover or leave?	Restore, readable export, deletion and residual copies

Do not fill missing answers with “none”. Use “unknown”, state what would resolve it and identify the affected use. Record dates and versions; a screenshot without the service or account context may prove little.

3. Test the operational differences

Run the same fictional task through each option. Observe which destinations receive information using evidence available to the firm and supplier documentation. Ask the supplier to account for unobservable routes. Record which functions fail without a network connection; offline behaviour alone does not establish what happens when the connection returns.

Test a revoked user, an attempted cross-matter search, an export and a restore. Check what remains in browser history, downloads, temporary files and ordinary system backups. These tests are practical prompts, not a complete security assessment. An encryption statement needs context: what is encrypted, who holds access and which operations require readable information?

4. Make the legal assessments separately

Para. 6.3 of the SRA Code governs client confidentiality. The responsible solicitor should record the permitted disclosure and assess legal professional privilege separately; architecture alone does not settle waiver or preservation. The SRA AI warning addresses contractual, technical and organisational safeguards.

Where a party processes personal data on the firm’s behalf, examine art. 28 UK GDPR arrangements. Record the applicable data-protection risk assessment, including whether art. 35

requires a DPIA. Overseas access and further recipients require analysis of their actual arrangements; storage location alone is insufficient evidence.

5. Record a use-specific decision

Preferred configuration and reasons: [evidence, limitations and operational needs]. **Approved task, users and information:** [complete]. **Conditions before affected live use:** [issue, owner and closure evidence]. **Residual risks and responsible decision-maker:** [complete]. **Review triggers:** [changed service, model, support, terms, integration or incident].

Retain the comparison in the existing procurement file. A reasoned decision may approve different configurations for different tasks. Avoid turning the comparison into a universal claim that one architecture is safe for every matter.

Edition 1.0.0. Law and guidance checked and native content reviewed: 9 November 2026. Next planned content review: 9 February 2027. Check for a newer edition; changes may require earlier review.