Ekselens

EKSELENS360

EKSELENS INSIGHT · DATA & SOVEREIGNTY

Data sovereignty and sovereign AI: why where your data lives now shapes supplier choice

Where data is held, processed and governed has become a board-level supplier question. Treat sovereignty as a design requirement, not a procurement afterthought.

THE EIGHT-PHASE METHOD



Ekselens Consulting

ekselens.com · info@ekselens.com

Changing how transformation is done

The EKSELENS360 family

DATA & SOVEREIGNTY · 12 NOVEMBER 2026 · 4 MIN READ

For years, data location was a technical detail settled late in a procurement. That has changed. Geopolitical uncertainty, the spread of AI, and new rules on data access and cloud switching have made the question of where data lives — and who can reach it — a board-level concern that shapes which suppliers an organisation can safely choose.

What "sovereignty" actually means

Sovereignty is often reduced to "keep the data in the UK". In practice it has three layers, and suppliers can meet one without meeting the others:

- **Data residency:** where the data is physically stored and processed.
- **Operational control:** who can administer the systems, including the supplier's own staff and sub-processors, and from where.
- **Legal jurisdiction:** which laws can compel access to the data, regardless of where it is stored.

A service hosted in a UK data centre but operated by a provider subject to foreign access laws may satisfy residency but not jurisdiction. Clear requirements start with being explicit about which layer matters for which data.

Why AI raises the stakes

AI multiplies the places data travels. Prompts, documents, embeddings, logs and fine-tuned models can all contain sensitive information, and each may be held in a different location by a different party. Common blind spots include:

- prompts and outputs retained by a model provider for monitoring or improvement;
- AI features switched on inside existing SaaS platforms, routing data to new sub-processors;
- vector databases and search indexes created outside the main data governance process;
- models fine-tuned on organisational data with unclear ownership.

The result is that an organisation can have strong data residency for its core systems and weak control over the AI layer built on top of them.

The regulatory backdrop

Several regimes now bear on these decisions. UK GDPR continues to govern international transfers. The Data (Use and Access) Act 2025 updates parts of the UK data protection framework. For organisations operating in the EU, the EU Data Act — applicable since September 2025 — introduces cloud-switching rights, with switching charges due to be removed by January 2027. Sector regulators in financial services, health and the public sector add their own expectations on outsourcing, resilience and concentration risk.

None of these requires every workload to be sovereign. Together they require organisations to know where their data is, justify where it goes and be able to move it.

Make sovereignty a design requirement

Treat sovereignty as a requirement set at the start of a programme, not a clause negotiated at the end. A practical approach:

Classify data by sovereignty need

Not all data needs the same protection. Group data into tiers — for example, public, internal, sensitive and restricted — and set residency, operational control and jurisdiction requirements for each tier.

Map the AI data flows

For each AI use case, trace where prompts, documents, outputs and logs go, which sub-processors handle them and how long they are kept. Update the map whenever a supplier switches on a new AI feature.

Build portability into contracts

Secure rights to export data, outputs and any custom models in usable formats. Use the switching rights now available in the EU where relevant, and require documented exit support everywhere.

Avoid concentration you cannot unwind

Relying on a single provider for infrastructure, platforms and AI models increases both resilience and sovereignty risk. Decide deliberately where concentration is acceptable and where it is not.

Questions to ask every supplier

- Where will our data, prompts and outputs be stored and processed?
- Who can access them operationally, and from which countries?
- Which laws could compel you to disclose our data, and how would you respond?
- Which sub-processors are involved, and how will we be told of changes?
- How would we exit, and in what format would our data and models be returned?

Suppliers that answer clearly and in writing are easier to trust. Those that cannot are telling you something important.

The leadership decision

Sovereignty is a trade-off between control, cost and capability, and the right balance differs by organisation and by data tier. What leaders should not accept is a position they have not chosen. Knowing where your data lives, who can reach it and how you would move it is now part of basic governance — and a growing factor in which suppliers you can safely pick.

Want to talk this through?

Book a 45-minute discovery conversation. Bring one challenge, leave with three prioritised next steps — written up within 24 hours.

ekselens.com/contact
info@ekselens.com
+44 (0) 20 7874 7217

© Ekselens Consulting. All rights reserved.