



Planning Your AI Data Capacity Needs and Data Sovereignty Risk

The questions leaders need to ask

As companies adopt AI models, planning data capacity mounts. But where the capacity comes from, and therefore where the data is housed, is becoming a global and political issue, and understanding the risks is something every boardroom needs to prioritise.

Our blog 'AI models, sovereignty and what your business can do today' provides an outline of why in detail, but fundamentally, the reasons fall into four categories:

- Ownership and legal reach
- Data residency and control
- AI inference and workloads
- Risk and accountability

Every business is different, so there is no single solution. However, there are certainly questions leaders need to ask which will shape the plan.

We've listed them here and intend them to be a go-to list for ensuring every aspect is discussed. Asking these questions will unlock the answers needed to help identify the options businesses have for managing risk whilst taking advantage of the opportunities AI presents.

OWNERSHIP AND LEGAL REACH

1

Who is the ultimate parent company, and under which country's laws is it incorporated?

The operating entity in your country may answer to a US or non-UK parent with its own legal obligations.

2

Could a foreign government compel your provider to hand over your data without notifying you?

The US CLOUD Act applies to US companies regardless of where data is physically stored.

3

Is the entity that holds your contract incorporated and regulated in the UK (or your operating country)?

A locally registered subsidiary is not the same as a company that answers only to local law.

DATA RESIDENCY AND CONTROL

4

Where exactly is your data stored, processed, and backed up, and is that guaranteed contractually?

A provider can commit to residency in the marketing materials and carve out exceptions in the small print.

5

Can your provider access your data for operational purposes, and who inside their business can see it?

Support staff, engineers, and automated systems may all have access. Ask for specifics, not a general privacy statement.

6

Does your data ever transit through infrastructure outside the UK, even temporarily?

Routing, CDN, and replication arrangements can move data across borders in ways residency clauses do not cover.

AI AND INFERENCE WORKLOADS

7 Where is AI inference being run, and does that infrastructure sit within your required legal boundary?

Many AI services route inference requests through infrastructure that does not match the residency of the data they process.

8 Is any of your data used to train or fine-tune AI models, and can you opt out of that contractually?

Training data use is sometimes buried in acceptable use policies rather than the main service agreement.

RISK AND ACCOUNTABILITY

9 What happens to your data if the provider is acquired, goes insolvent, or exits the market?

Acquisition by a non-UK entity can change your legal exposure overnight. This should be a specific clause, not a general reassurance.

10 Can you get your data back in a usable format if you decide to leave, and on what timeline?

Portability and exit rights are as important to sovereignty as residency. Control includes the ability to move.

We answer these questions every day with clients, designing strategic paths to follow that make sense for their business, their country of origin and operation.

Residency on its own isn't enough. What matters is whether the company holding your data answers to UK law, and whether you own and control the infrastructure it runs on. **We can say yes to both.**

We're UK-owned, we run our own Data Centre in Nottingham, and we answer only to UK law. That's the position we help clients work towards.

Reach us at info@cvwcs.co.uk or call us on 0800 1 777 000.