DATA SOVEREIGNTY HAS AN OWNERSHIP PROBLEM

Straight-talking insight from Miso

Contact
0121 232 8000

Website
www.misoportal.com

E-mail
info@misoportal.com

DATA SOVEREIGNTY HAS AN OWNERSHIP PROBLEM

Data sovereignty has always been framed as a control problem. Where is the data, who can access it, and which legal systems can compel disclosure. Questions that can be answered mostly with architecture.

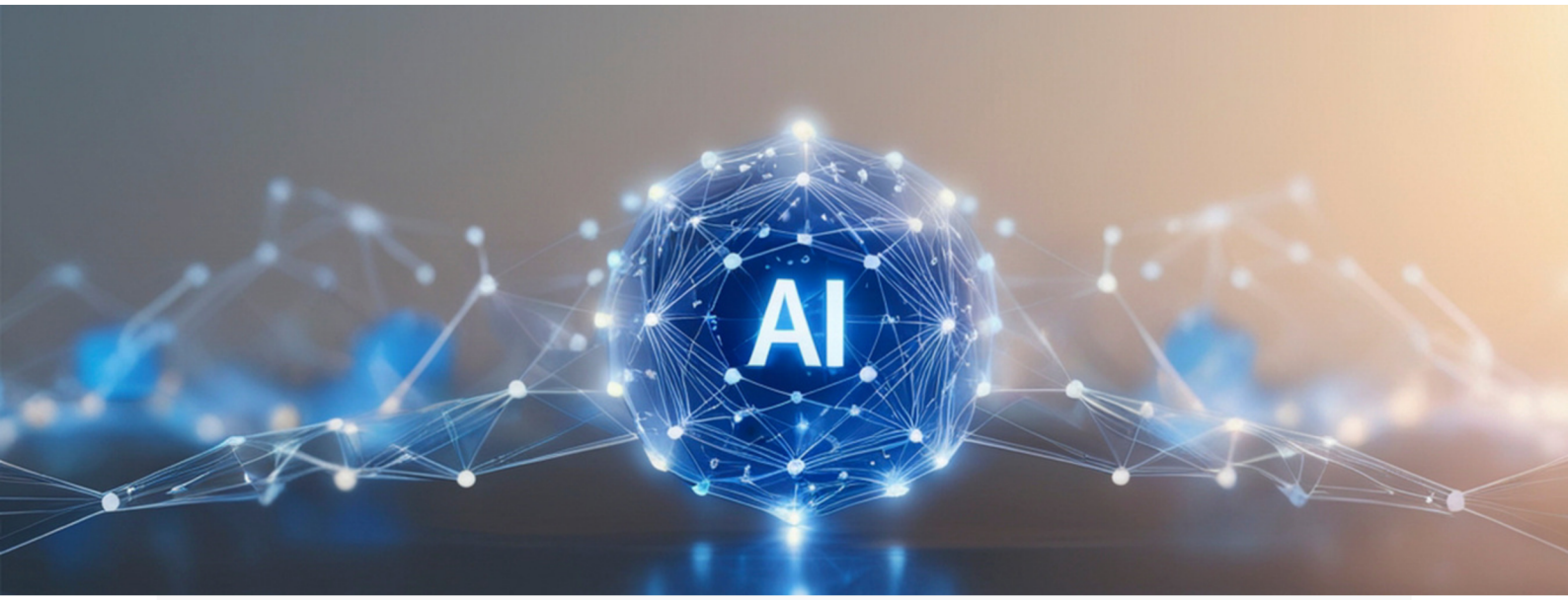
However, data sovereignty actually has two pillars: control and **ownership**. We've focused heavily on control, and in doing so, we're starting to lose sight of the ownership of our data.

CONTROL WAS THE MAIN CONCERN

For a long time, sovereignty was a fence problem. On-premises environments were about keeping the wrong people out, encrypting what mattered, and putting everything behind a firewall. If you controlled the environment, you controlled the data.

As data moved onto laptops and remote devices, the same principle applied. The data was more distributed, but organisations still owned the devices and could enforce policy.

Cloud introduced more complexity, but the core challenge remained the same. Questions about where data was stored, who could access it, and which regulators had jurisdiction became more nuanced but ultimately were still about control.



THE OWNERSHIP CRISIS

We're entering a period where ownership is becoming the more important issue, and it is far easier to lose than most organisations realise.

Many platforms and services operate on terms that allow them to use, transform, and build on the data you provide. For example, something as simple as putting a pin on a Google Map gives Google "…a worldwide, royalty-free licence to transform and create derivative works".

AI has accelerated this shift. What happens to data after it has been processed by a model you do not own? It may be retained for training, cached in infrastructure you cannot inspect, or used to improve outputs for other users. You may still control access to your original data, but you have no ownership of what it becomes.

BALANCING OWNERSHIP, CONTROL AND RISK

Most already have strong approaches to managing data risk, but the challenge is that those approaches were built around control, not ownership. They now need to evolve in 3 ways…

- **Classification:** Classification needs to capture ownership and exposure as well as sensitivity. In practice, this is where metadata and lineage tracking become critical, which is a big part of why platforms like Databricks have gained traction.

- **Process:** Organisations need to understand what service providers are allowed to do with that data. That means properly evaluating terms of service.

- **Architecture:** The starting point should be identifying the data you cannot afford to lose ownership of. That data probably belongs on-prem, or in infrastructure you control directly. For everything else, understand the ownership risk of each service before you connect it.

DATA SOVEREIGNTY IS A MIX OF OWNERSHIP AND CONTROL

Data sovereignty is no longer just about control. It is about balancing ownership, control and risk. If any one of those is not properly understood, it creates a gap. And those gaps are where organisations become exposed.

www.misoportal.com