rubrik

SOVEREIGNTY 101

DOES YOUR DATA HAVE A PASSPORT PROBLEM?

Most organisations have achieved **data residency**, but few have achieved **data sovereignty**. If you don't control the recovery path, you don't own the data.

THE SHIFTING LANDSCAPE

Geopatriation Rising

61%

of Western European CIOs are shifting to local cloud providers*

Regulatory Pressure

NIS2 & DORA

now require systems that work even when global vendors are cut off

The Autonomy Problem

53%

of IT leaders say geopolitics will limit their use of global cloud platforms*

*Gartner Survey

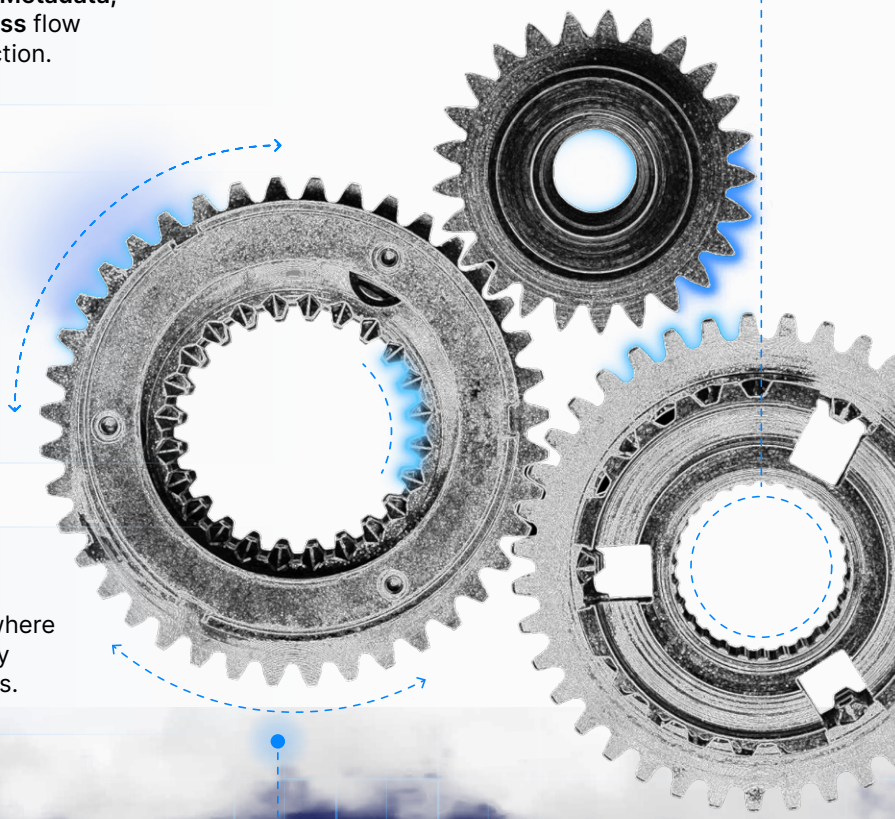
THE RESIDENCY ILLUSION VS. THE SOVEREIGNTY REALITY

The Residency Illusion

Your data may be stored locally, but your **Metadata**, **Encryption Keys**, and **Global Admin Access** flow through a vendor's HQ in a foreign jurisdiction.

The Sovereignty Gap

If your recovery path is foreign-owned, storing data locally is not enough. Foreign legal mandates (like the U.S. CLOUD Act) can force a vendor to cut off your management access, making it technically impossible to restore your data during a crisis.



The Sovereignty Reality

The goal is to create a technical airlock, where data, metadata, and the control plane stay entirely within your designated boundaries.

But full digital sovereignty is expensive and hard to maintain.

THE SOLUTION

Define
Minimum Viable Sovereignty
what level of control is "good enough" for each data type?

DEFINING MINIMUM VIABLE SOVEREIGNTY (MVS)

MVS is the baseline level of control required to guarantee business continuity regardless of external jurisdictional interference. To achieve it, you must audit these four pillars:

Backup and recovery infrastructure

- Can you restore operations without relying on vendor support teams in jurisdictions subject to sanctions or lockout orders?
- If your vendor's headquarters or primary operations are restricted, do you have alternative recovery paths?

Key management

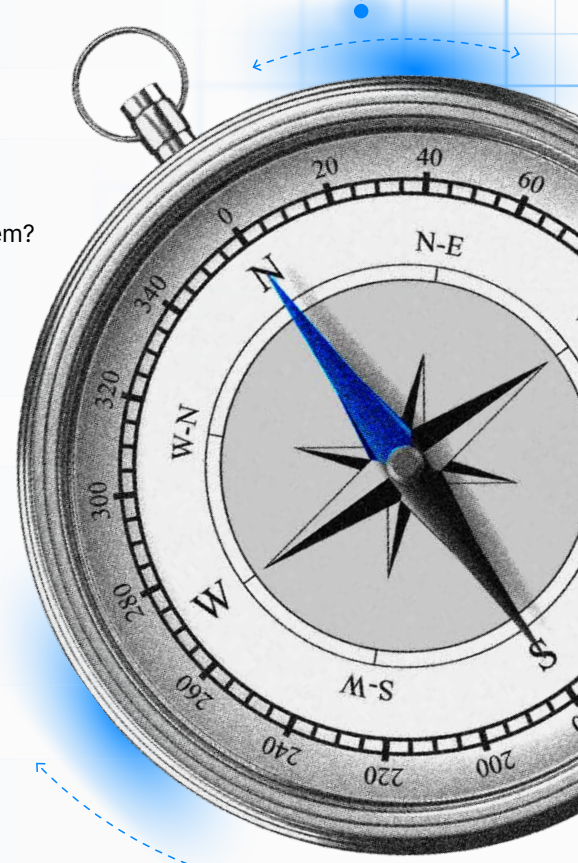
- Where are your encryption keys stored? Who controls access to them?
- If your vendor's jurisdiction is sanctioned, can you still decrypt and access your data?
- Do you need bring-your-own-key (BYOK) or hold-your-own-key (HYOK) capabilities for your most sensitive workloads?

Identity and authentication resilience

- Can your identity infrastructure function if your primary vendor's APIs are geoblocked or restricted?
- Do you have failover identity providers in alternative jurisdictions?

Failover independence

- Can you fail over to secondary sites without vendor intervention or cross-border dependencies?
- Are your secondary sites truly independent, or do they rely on the same vendor operations teams?



Stop guessing. Start governing. Learn how to bridge the Sovereignty Gap and achieve true operational resilience in a fragmented world.