



U.S. CLOUD Act & Data Sovereignty

Maintain Greater Control Over Where Your Data Lives—
and Who Can Access It



The U.S. CLOUD Act can require covered U.S. service providers to produce data within their possession, custody, or control—even when that data is stored outside the United States.

For global organizations, this highlights an important distinction: **data residency does not always equal data sovereignty.**

Why the CLOUD Act Matters



Data Location

Storing data within your country can support residency requirements, but location alone may not determine which laws apply to the provider managing it.



Foreign Jurisdiction

Organizations using U.S.-based cloud providers may need to consider whether their data could be subject to lawful U.S. government access requests.



Regulatory Requirements

Government agencies and regulated industries may require greater control over where sensitive information is stored, processed, and accessed.



Data Sovereignty

True sovereignty involves more than geography. It also includes control over infrastructure, access, governance, and legal jurisdiction.

Data Residency vs. Data Sovereignty

Data Residency	Data Sovereignty
Where data is physically stored	Who ultimately controls the data
Geographic storage requirements	Applicable legal jurisdictions
Local or regional hosting	Control over access and infrastructure



Data can reside locally while still being subject to another jurisdiction.

Support Data Sovereignty with FileCloud

FileCloud gives organizations deployment flexibility and administrative control to align content collaboration with their sovereignty and compliance requirements.

Flexible Deployment



Deploy FileCloud on-premises, in a private cloud, or in infrastructure and regions selected by your organization.

Infrastructure Control



Self-hosted deployments enable organizations to maintain direct control over the systems used to store and manage sensitive content.

Granular Data Governance



Manage access with granular permissions, authentication controls, audit logs, retention policies, and administrative governance.

Security by Design



Protect sensitive information with encryption, Zero Trust security capabilities, DLP, DRM, and other enterprise security controls.

Why FileCloud for Data Sovereignty?

- ✓ **Control Where Data Lives:** Choose deployment infrastructure and geographic location based on organizational requirements.
- ✓ **Control Who Has Access:** Apply granular user, sharing, security, and administrative policies.
- ✓ **Control How Data Is Governed:** Support compliance, retention, auditing, and information governance from one platform.

Millions of users and thousands of global organizations trust FileCloud

Deloitte.

FUJIFILM



7Wise

