

Data Sovereignty

[Go up to Terms and Definitions](#)

Discussion

Data sovereignty addresses the legal, regulatory, policy, and governance authority that applies to data, metadata, data processing, data access, data movement, and data protection within or across jurisdictions.

Data sovereignty differs from [data_residency](#). Data residency focuses on the location, movement, and protection of data and metadata across geographies and jurisdictions. Data sovereignty focuses on the authority governing data and the controls that preserve that authority.

OMG and the Cloud Standards Customer Council describe data residency challenges as arising when laws and regulations dictate where data transfers, storage, sharing, and protection occur across geographic boundaries. Those same challenges raise data sovereignty concerns when jurisdictional authority, access rights, operational control, or legal obligations determine who governs the data and who gains access to it. :contentReference[oaicite:0]{index=0}

Data sovereignty also differs from data localisation. Data localisation focuses on retaining or storing data within a specified geographic or jurisdictional area. Data sovereignty focuses on governed control, jurisdictional authority, legal exposure, access control, operational control, evidence, and accountability.

Data sovereignty semantic content includes:

- Jurisdictional authority
- Legal authority
- Regulatory authority
- Governance authority
- Data access control
- Data processing control
- Data transfer control
- Metadata control
- Key custody
- Operational control
- Audit evidence
- Legal exposure
- Cross-border access risk
- Third-party provider risk
- Traceability to sovereignty rules and policies

Definition

governed authority over data, metadata, data processing, data access, data movement, and data

protection within or across jurisdictions

Source

DIDO Solutions usage, informed by OMG and Cloud Standards Customer Council data residency challenge material and specialised for use in the FX Demo Reference Architecture.

Note

Data sovereignty does not reduce to the physical location of data. A system can store data in an approved jurisdiction, while a foreign legal authority, cloud operator, administrator, support process, encryption key holder, or subcontractor still affects the risk of access, control, or disclosure.

Data residency identifies where data resides or moves. Data sovereignty identifies who governs the data and which authorities, controls, and obligations apply.

Example

An FX reporting node stores EU trade data in an EU data centre. The storage location satisfies a data residency constraint. Data sovereignty analysis also examines who operates the infrastructure, which legal authorities can compel access to it, who controls encryption keys, which administrators can access raw counterparty data, which support teams can inspect logs, and which audit evidence demonstrates compliance with the governing policy.

In this example, data residency concerns the location and movement of the data. Data sovereignty concerns the legal and operational authority over the data.

© 2026 Dido Solutions, Inc. and Jackrabbit Consulting, Inc.

From:
<https://wiki.didosolutions.com/> - Dido Solutions, Inc Wiki

Permanent link:
https://wiki.didosolutions.com/dido/99_annexes/annex-b-terms-and-definitions/d/data_sovereignty?rev=1783793672

Last update: **2026/07/11 11:14**

