

4.6.3 Data Sovereignty

[Return to Top](#)

Data Sovereignty is concerned with any jurisdictions' laws and regulations covering any data collection or processing done within that jurisdiction, governing the data. **Data Sovereignty** differs from **Data Residency** in that Data Residency reflects a business decision on where to store and process data, often based on **Data Sovereignty** Laws and Regulations applicable to a particular jurisdiction.

Much of the current interest in **Data Sovereignty** by jurisdictions (i.e., Countries) around the world is traceable to the revelations made public of U.S. activities of surveillance and collecting data globally on people (i.e., internally and externally to the U.S.) ¹⁾. The simplest way to look at **Data Sovereignty** is to consider national [Privacy Considerations](#) and preventing data stored in a foreign country from subpoenas by the host country's government.

A globally accepted U.S. CBDC needs to take the Data Sovereignty issues seriously if there is any hope of *"Preserving the dominant international role of the U.S. dollar (B0036)"*

A theoretical example of how complicated a globally accepted U.S. CBDC would be:

- Assume U.S. CBDC transactions that occur in the E.U. are stored and processed in the U.K.
- A U.S. CBDC transaction occurs in Italy and would be subject to the **Data Sovereignty** laws and regulations of Italy and the EU.
- However, since the data is stored and processed in the U.K., the data would be subject to the data sovereignty rights of the U.K. as Italy and the E.U.
- To further complicate matters, U.S. CBDC transactions made and stored in the U.K. are backed up on servers in Ireland, making the CBDC transaction also subject to the data **Sovereignty Rights** of Ireland too.

A real-world example of **Data Sovereignty** issues is [Microsoft's Data Privacy Case vs. the DoJ](#) ²⁾:

Microsoft's case against the US Department of Justice (DoJ) was also a high-profile event that further highlighted the importance of data sovereignty.

After the DoJ ordered the tech company to grant access to emails stored in Ireland-based servers related to a narcotics investigation in 2013, Microsoft had refused to comply with the Department of Justice's request.

Despite that Microsoft stated that complying with the request would break the data privacy laws of the European Union, the initial ruling ordered the company to fulfill the DoJ's request.

However, later on, after Microsoft won the appeal and the DoJ changed its data-related policies.

The adoption of U.S. CBDC could break traditional geopolitical barriers more than ever before, especially depending on the [Currency Model](#) selected. Depending on the perception of privacy protection of the

CBDC, many countries may amend existing laws and regulations or greatly restrict the use of a U.S. CBDC.

The U.S. CBDC needs to be completely honest and open about where data:

- Servers are hosted (i.e., [Data-At-Rest](#))
- Flows over networks (i.e., [Data-In-Motion](#))
- Is processed (i.e., [Data-In-Use](#))

1)

Ewen MacAskill and Gabriel Dance, The Guardian, [NSA Files: Decided - What the revelations mean for you](#), 1 November 2013, Accessed: 9 April 2022, <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>

2)

Benjamin Vitaris, Permission.io, [What Is Data Sovereignty? Everything You Need to Know](#), 11 August 2020, Accessed: 9 April 2022, <https://permission.io/blog/data-sovereignty/>

From:
<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:
https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc_omg:04_doc:15_common:50_international:30_overn&rev=1652739085

Last update: **2022/05/16 18:11**

