# 4.6.2 Data Localization

| International Considerations | **Provide Feedback** |
|---|---|

Data localization is about jurisdictions adopting policies with an aim to protect the jurisdictions' sovereignty over the data generated from within its geographic boundaries or from its residents. The policies are intended to help protect the jurisdiction and its residents from external entities (private or public).

Figure 1 shows the increase in **Data Localization** measures globally from 1960-2015. This increase indicates that this is a problem that will only get bigger as time goes by. The CBDC needs to understand and recognize it as a growing international trend.

Figure 1: Increase in data localization measures globally (1960 - 2015)[1)]

The need for **Data Localization** is justified for different reasons, such as the protection of data from:

- Hackers engaged in nefarious activities.
- Personal Identifiable Information (PII)
- Regulators wanting to access the information on participants in cross-border transactions
- External jurisdictions trying to identify individuals engaged in activities it finds illegal or offensive, but that are not considered that way locally
- Unwanted or desired commercial mining
- Public opinion favoring in-country data storage solutions and strategies

This usually takes the form of a mandate and/or a set of laws or regulations that require certain data to be physically stored on servers within the country of origin.

Data Localization policies tend to fall into three categories[2)]:

Table 1: Data Localization Policies. See: [3)]

| Localization Category | Description | Law or Regulation Examples |
|---|---|---|
| **Local-only Storing, Transmission, and Processing** | **This generally means an obligation to locally manage data or a prohibition of international data transfers. This is the strictest type of localization policy and is more likely to be descriptive of nations seeking broader control over citizen activities.** | **Russia**<br>Under Russia's Federal Law No. 242-FZ, operators must ensure the recording, systematization, accumulation, storage, adjustment (update, alteration), and retrieval of personal data of citizens of the Russian Federation will be performed through database servers located in the territory of the Russian Federation. Substantial fines are imposed on organizations and individuals that fail to comply with data localization requirements.<br>**China**<br>Article 37 of the Cybersecurity Law of the People's Republic of China ('CSL') requires critical information infrastructure operators ('CIIOs') to store personal information and important data generated from critical information infrastructure in China. These requirements are likely to be expanded by the Personal Information Protection Law, the draft of which was released in October 2020. |
| **Local Copy Required** | **Companies are required to keep a copy of data in local servers or data centers. This allows for easier access to this data for regulation and law enforcement purposes, i.e., it is generally easier for local law enforcement agencies to access data stored locally than it is for them to access data stored in another jurisdiction.** | **India**<br>Under India's Personal Data Protection Bill, sensitive personal data (which includes financial information) must be stored in India, but a copy of the data can be transferred internationally if certain requirements are met. These include:<br>1. The data principal provides explicit consent, the transfer is made pursuant to a contract or intra-group scheme approved by the Data Protection Authority<br>2. The government has deemed a country to provide adequate protection<br>3. The Data Protection Authority has specifically authorized the transfer |

| Localization Category | Description | Law or Regulation Examples |
|---|---|---|
| **Narrower, conditional restrictions** | **Transfers of data outside the country are only permitted if certain conditions are met by the transferee and/or by the recipient country.** | **European Union**<br>Under the EU's GDPR, the transfer of personal data outside the European Economic Area is permitted only where:<br>1. The recipient is in a territory considered by the European Commission to offer an adequate level of protection for personal data<br>2. Safeguards are in place, such as binding corporate rules approved by Data Protection Authorities<br>3. A legal exemption applies, such as where data subjects provide explicit consent, the transfer is necessary to fulfill a contract or there is a public interest founded in EU or member state law<br>**Brazil**<br>Under the General Personal Data Protection Law (LGPD) international data transfers are only permitted in certain situations, including when recipient countries ensure an adequate level of data protection, when approved legal mechanisms (such as model contract clauses) are employed or when data subjects have provided their consent. |

1) 2) 3)
, , ,

Emily Wu, Harvard Kennedy School - Belfer Center - For Science and International Affairs, Sovereignty and Data Localization, July 2021, Accessed: 9 April 2022, https://www.belfercenter.org/publication/sovereignty-and-data-localization