DATA LOCALIZATION

What Does Data Localization Mean?

Data localization is the act of storing data on any device that is physically present within the borders of a specific country where the data was generated. Free flow of digital data, especially data which could impact government operations or operations in a region, is restricted by some governments. Many attempt to protect and promote security across borders, and therefore encourage data localization.

Data localization or **data residency** law requires data about a nations' citizens or residents be collected, processed, and/or stored inside the country, often before being transferred internationally, and usually transferred only after meeting local privacy or data protection laws, such as giving the user notice of how the information will be used and obtaining their consent.

Data localization builds upon the concept of data sovereignty that regulates certain data types by the laws applicable to the data subject or processor. While data sovereignty may require that records about a nation's citizens or residents follow its personal or financial data processing laws, data localization goes a step further in requiring that initial collection, processing, and storage occur first within the national boundaries. In some cases, data about a nation's citizens or residents must also be deleted from foreign systems before being removed from systems in the data subject's nation.

Motivations and concerns

The push for data localization greatly increased after revelations by Edward Snowden regarding United States counter-terrorism surveillance programs in 2013. Since then, various governments in Europe and around the world have expressed the desire to be able to control the flow of residents' data through technology. Some governments are accused of and some openly admit to using data localization laws as a way to surveil their own populaces or to boost local economic activity.

Technology companies and multinational organizations often oppose data localization laws because they impact efficiencies gained by regional aggregation of data centers and unification of services across national boundaries. Some vendors, such as Microsoft, have used data storage locale controls as a differentiating feature in their cloud services.

While some arguments support data localization, some feel that misguided policies on data localization could cause serious harmful consequences to citizens and economies alike.

The requirements for data localization can be for different reasons, such as mandate by national laws that require certain data to be physically stored on servers within the country or the need to comply with data protection regulations. This is especially true when it comes to cross-border transfers in which case data storage within a country seems to be a cost effective and better solution, or in cases where enterprise customers of data storage technologies and public opinion favors in-country datastorage solutions and strategies. Data localization often requires better IT infrastructure and stringent security measures for data related to business operations.

Some favor data localization due to fear of losing private data to hackers in the case of foreign data storage solutions. Some oppose data localization, as it is seen as hindering the flexibility of the internet.