JULY 2021 | Lindsey R. Sheppard, Erol Yayboke, Carolina G. Ramos

THE SHIFT TOWARD DATA LOCALIZATION

The most common and widely accepted definition of "data localization" is policies or mandates requiring certain data related to citizens or residents of a country—whether personal, health, business, or financial—to be physically stored on infrastructure within that country's borders. Additionally, policies may establish **different categories of data**, as in the distinction between "personal data," "sensitive personal data," and "critical personal data," and apply different levels of restrictions or permissions to each.

In practice, data localization mandates come in a variety of forms and manifestations. However, most approaches can be generally classified as:

- hard localization,
- mirroring or soft localization,
- hybrid localization, or
- de facto localization.

Further, one or more of the above approaches may be applied to different categories of data within a country's overall data governance framework.

Under hard localization mandates, data may only be processed and stored within the issuing country's borders. In other words, data may not be transferred outside the jurisdiction. Hard localization affects major data flows and digital platforms. International data transfers necessary for delivery of even mundane services **like email** may require transfer, storage, and processing that may be inconsistent with hard localization mandates. For example, China's 2017 **Cybersecurity Law** and 2020 draft **Personal Information Protection Law** require that various forms of data, including personal data, be stored in China and undergo a government "security review" before transfer.

Mirroring or soft localization mandates allow data to be transferred outside the jurisdiction for processing and storage, but a copy of the data must be retained within the issuing nation's borders. An example of this form of localization is found within **India's draft Personal Data Protection Bill** (see **chapter 8** of bill text) and **Pakistan's draft Personal Data Protection Bill** (see **section 15** of bill text). Soft localization requires providers to retain a copy of the data within the country. However, the India and Pakistan bills add additional requirements to the mirroring approach, allowing for the transfer of broadly defined "sensitive personal data" outside of the issuing country, subject to certain preconditions.

Hybrid localization mandates are a form of hard localization that adopts the permissiveness of soft localization. While data can only be stored in the jurisdiction where it is created, it can temporarily be processed outside of the jurisdiction to facilitate related transactions. Through a **2018 directive** issued by the Reserve Bank of India, India has implemented hybrid localization requirements related to payments data. Within this "Storage of Payment System Data" mandate, there are no restrictions on processing payments outside the country, but once the processing is complete, the data must be stored only in India. If stored (even temporarily) outside of the jurisdiction, it must be deleted within 24 hours or one business day. However, the data can be accessed when needed for all activities related to processing.

De facto data localization results when a nation or governing body has no express data localization requirements but does enact laws or mandates that permit data to be transferred outside of the jurisdiction only if certain conditions are met. These can include threat of fines, bureaucratic roadblocks, or other excessive requirements that make regular cross-border data transfers risky, costly, or even impossible in practice. For example, **many concerns** have been raised that de facto localization will be the outcome of the European Union's General Data Protection Regulation (GDPR), in accordance with the ruling by the **Court of Justice** of the European Union in the Schrems II case—even though the GDPR does not have explicit data localization clauses.

CSIS | INTERNATIONAL SECURITY PROGRAM