All about Data localisation in India

Ravi Singhania
Managing Partner
E: ravi@singhania.in

American Express and Diners Club were prohibited from accepting new clients for six months beginning in May 2021 after the Reserve Bank of India (the "RBI") imposed the first fines relating to localization of payments data in April 2021. In July 2021, it prohibited Mastercard from bringing on board new domestic clients for an indeterminate period of time. Given that Mastercard controls around a third of India's total cards network market, the prohibition is likely to have a considerable effect.

These limits may be viewed as being excessive considering that the RBI exercises regulatory authority in a generally restrained manner and rarely imposes such extensive fines.

What Is Data Localisation?

- The act of storing data on any device that is physically located inside the boundaries of the nation where the data is generated is known as "data localization." The majority of this data are currently kept on a cloud outside of India.
- Companies must keep and process sensitive customer data within national borders as a requirement of localization.

The following is a summary of India's primary data localization laws:

1. The (Indian) Companies Act 2013 and the Companies (Accounts) Rules 2014:

- Section 94 of the Companies Act, read with Sections 88 and 92, require covered organizations to store financial information at the registered office of the company.

2. The RBI ordered all payment companies to keep all information relating to payment systems on servers in India in April 2018. The RBI granted businesses a six-month window in which to abide by this instruction. Payment system providers were required to store all data in systems that were under India's territorial control, according to a circular titled "Storage of Payment System Data."

3. The IRDAI (Maintenance of Insurance Records) Regulation, 2015:

- Section 3(9) requires covered organizations to store insurance data within India.

The RBI clarified the what kinds of information that must be kept in India such as :

- end-to-end transaction information.
- any details relating to payments or settlements that are sent, gathered, or processed as part of a payment message or instruction.
- customer information like name.
- Permanent Account Numbers (PAN)
- Aadhar card numbers.
- payment sensitive information like beneficiary and customer account information,
- login credentials like one-time passwords and pin numbers,
- and transaction information are crucial details that must be protected in accordance with RBI guidelines.

Applicability of the RBI circular:

- The directions are applicable to all Payment System providers authorised / approved by the Reserve Bank of India (RBI) to set up and operate a payment system in India under the Payment and Settlement Systems Act, 2007.
- Banks function as operators of a payment system or as participant in a payment system. They are participants in (i) payment systems operated by RBI viz., RTGS and NEFT, (ii) systems operated by CCIL and NPCI, and (iii) in card schemes. The directions are, therefore, applicable to all banks operating in India.
- The directions are also applicable in respect of the transactions through system participants, service providers, intermediaries, payment gateways, third party vendors and other entities (by whatever name referred to) in the payments ecosystem, who are retained or engaged by the authorised / approved entities for providing payment services.
- The responsibility to ensure compliance with the provisions of these directions would be on the authorised / approved PSOs to ensure that such data is stored only in India as required under the above directions.

RBI also provided clarifications on implementation difficulties related to the "Storage of Payment System Data" regulations that were raised by Payment System Operators (PSOs).

It was explained that payment information could be handled outside of India, but that it had to be erased afterward and transported back to India for storage within a business day or 24 hours, whichever came first.

This action has drawn criticism because:

- It is challenging to determine whether data has been destroyed or is still being stored on foreign land.
- The laws in the countries where data is moved apply to it. As a result, the law passed in India cannot dictate how data is used in other countries.

It can be seen, then, that the pace of data localisation requirements has increased in the recent past, particularly in 2018 and 2019.