Date : Jun 26, 2019

Storage of Payment System Data

The Reserve Bank of India issued a directive vide circular DPSS.CO.OD.No 2785/06.08.005/2017-18 dated April 06, 2018 on 'Storage of Payment System Data' advising all system providers to ensure that, within a period of six months, the entire data relating to payment systems operated by them is stored in a system only in India.

Payment System Operators (PSOs) have sought clarification on certain implementation issues, from time to time, from Reserve Bank. The FAQs are intended to provide clarity on those issues to facilitate and ensure expeditious compliance by all PSOs.

1. Applicability of the direction

- 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.

2. Where should the payment data be stored?

The entire payment data shall be stored in systems located only in India, except in cases clarified herein.

3. Clarification regarding data that needs to be stored in India

The data should include end-to-end transaction details and information pertaining to payment or settlement transaction that is gathered / transmitted / processed as part of a payment message / instruction. This may, interalia, include - Customer data (Name, Mobile Number, email, Aadhaar Number, PAN number, etc. as applicable); Payment sensitive data (customer and beneficiary account details); Payment Credentials (OTP, PIN, Passwords, etc.); and, Transaction data (originating & destination system information, transaction reference, timestamp, amount, etc.).

4. Storage of data pertaining to cross-border transactions

For cross border transaction data, consisting of a foreign component and a domestic component, a copy of the domestic component may also be stored abroad, if required.

5. Processing of payment transactions

- There is no bar on processing of payment transactions outside India if so desired by the PSOs. However, the data shall be stored only in India after the processing. The complete end-to-end transaction details should be part of the data.
- In case the processing is done abroad, the data should be deleted from the systems abroad and brought back to India not later than the one business day or 24 hours from payment processing, whichever is earlier. The same should be stored only in India.
- However, any subsequent activity such as settlement processing after payment processing, if done outside India, shall also be undertaken / performed on a near real time basis. The data should be stored only in India.
- In case of any other related processing activity, such as chargeback, etc., the data can be accessed, at any time, from India where it is stored.

6. Can the data processed abroad be retained abroad till the window for customer dispute resolution / chargeback is available?

As indicated above, the payment data sent abroad for processing should be deleted abroad within the prescribed time line and stored only in India. The data stored in India can be accessed / fetched for handling customer disputes whenever required.

7. Can the payment system data be shared with overseas regulators?

The data may be shared with the overseas regulator, if so required, depending upon the nature / origin of transaction with due approval of RBI.

8. Scope and coverage of the System Audit Report (SAR)

The System Audit Report (SAR), from a CERT-In empanelled Auditor, should inter-alia include Data Storage, Maintenance of Database, Data

Backup Restoration, Data Security, etc.

9. Clarification in respect of entities earlier permitted to store banking data abroad?

In the case of banks, especially foreign banks, earlier specifically permitted to store the banking data abroad, they may continue to do so; however, in respect of domestic payment transactions, the data shall be stored only in India, whereas for cross border payment transactions, the data may also be stored abroad as indicated earlier.