

RBI – Directions on Storage of Payments Systems Data

Applicable

- a. To all Payment System Providers, Operators including Banks; Banks function as an operator of the Payment System
- b. All system participants, service providers, intermediaries, payment gateways, third party vendors in the overall payment ecosystem.

Key Pointers and Controls to be Implemented

1. The entire payment system data shall be stored only in India; End-to-End Transaction details, data relating to payment.
 2. Organizations should identify and classify data elements – as Payments and Non-Payments data
 3. A detailed transaction and data flow of payment process should be maintained by the participants.
 4. Sensitive data, Customer data should be encrypted at rest and in transit
 5. Backup and Recovery – Regular Backups of the payment systems data shall be taken and tested periodically for restoration and recovery.
 6. Access to the payment systems, applications shall be strictly controlled and monitored continuously.
 7. Systems should be patched regularly; anti-virus should be implemented and logs to be monitored for the payment systems managed by the participant.
 8. Maintain a detailed and a clear network and application architecture of the payment systems depicting the modules, applications, database with the locations.
- Note – Backups CANNOT be stored outside India. DR site, data for DR should be within India.

Cross Border Transactions and Processing Outside India

1. Storage of payment data elements for both foreign component and domestic component should be identified, classified and stored accordingly. A copy of domestic component can be stored abroad.
2. Data shall be stored in India after processing outside India.
3. Data shall be deleted from systems abroad and brought back to India within 24 hours of payment processing.
4. Post payment processing conducted outside India should have a Purging Policy and Process to store data back in India and delete data outside India jurisdiction.

System Audit Report (SAR) for Data Localization

1. At least annually to confirm adherence to the RBI direction of storing payment systems data in India.
2. Banks and Participants have to audit/confirm adherence of the service providers in their payment ecosystem to the RBI direction of data localization.
3. Banks to submit a compliance certificate at half-yearly intervals for period ending March 31st and September 30th.

