Google Cloud

How GCP addresses Data Localization for payment data per RBI Guidelines

March 2022

Disclaimer

This document does not create any warranties, representations, contractual commitments, conditions or assurances from Google and customers should not rely on this document for a customer's decision to purchase GCP services. The responsibilities and liabilities of Google to its customers are controlled by Google agreements, and this document is not part of, nor does it modify, any agreement between Google and its customers. This document does not constitute legal advice.

Google Cloud

Executive Summary

At Google Cloud, the privacy and security of customer data are primary design criteria that underpin all the services we offer. Entities regulated by RBI's Directive on Storage of Payment System Data can use GCP Regions in India (Mumbai and Delhi) for local storage. GCP provides controls that customers can use to restrict where their data is stored. This helps regulated customers to ensure compliance with the payment system data localisation requirement. Google Cloud contractually provides for audit rights to regulated customers and their regulators. Our products regularly undergo independent verification of their security, privacy, and compliance controls, achieving certifications, attestations, and audit reports to demonstrate compliance; details of which are available in our Compliance resource center.

RBI Directive on Storage of Payment System Data

The RBI guidelines on data localization is specific to storage of payments systems data. The key stated drivers for this directive is around assuring the safety and security of payment systems data by adoption of the best global standards and their continuous monitoring and surveillance to reduce the risks from data breaches while maintaining a healthy pace of growth in digital payments and have supervisory access to such data by RBI.

- As per the RBI directive on Storage of Payment System Data - *RBI/2017-18/153 DPSS.CO.OD No.2785/06.08.005/2017-2018*

  *"… All system providers shall ensure that the entire data relating to **payment systems** operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required."*

  "... it is important to have unfettered supervisory access to data stored with these system providers as also with their service providers / intermediaries/ third party vendors and other entities in the payment ecosystem…"

- The RBI has also issued clarification on the specific types of data that this directive applies to. *Storage of Payment System Data*.

> *"… 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.)."*

- Additionally, it is also important to note that the localization directives do not prohibit processing of payment data as noted from the above clarification issued by the RBI*;*

  > *"…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…."*

Detailed Brief

Firstly; Google Cloud Platform (GCP) offers customers the ability to control where your data is stored.

Customers may configure the services listed at Google Cloud Platform Services with Data Residency to store **payment data as listed out in the RBI directive** in Mumbai (asia-south1) or Delhi (asia-south2) and Google will store that customer data at rest only in the selected Region/Multi-Region in accordance with our Service Specific Terms. When coupled with Cloud IAM configuration, which helps one to define fine-grained access policies and precisely control access to Google Cloud hosted data, customers can prevent your employees from accidentally storing customer data in the wrong Google Cloud region.

To assist customers in enforcing these controls, Google Cloud offers Organization Policy constraints, which can be applied at the organization, folder, or project level. You can limit the physical location of a new resource with the Organization Policy Service resource locations constraint.

Google Cloud also offers VPC Service Controls that provides an extra layer of security defense for Google Cloud services that is independent of Identity and Access Management (IAM). While IAM enables granular *identity-based access control*, VPC Service Controls enables broader *context-based perimeter security*, including controlling data egress across the perimeter. Using VPC Service Controls, you create a service perimeter which defines the virtual boundaries from which a service can be accessed, preventing data from being moved outside those boundaries. It also helps

mitigate data exfiltration risks such as the misconfiguration of employee access controls or attackers taking advantage of compromised accounts.

In addition to the above controls, *data is automatically encrypted while in transit when it is being transferred from/to a location outside of Google's network and while at rest*, and can only be accessed by roles and services that have authorization, with audited access to the encryption keys. By default, data at rest is encrypted using encryption keys managed by Google. When protecting sensitive data, such as customer financial information, credit card numbers and other personal identifiers, banks and FIs can choose to instead manage their keys in Google Cloud using Cloud Key Management Service (KMS).

Secondly; customers may access their data on the services at any time and regulated entities may provide their supervisory authority with the same access. In addition, Google grants audit, access and information rights to regulated entities, their supervisory authorities and both their appointees. This includes the regulated entity's internal audit department or a third party auditor appointed by the regulated entity. Google will fully cooperate with regulated entities and supervisory authorities exercising their audit, information and access rights regardless of the service location. Google Cloud aligns to RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks and the mapping document can be reviewed here.

Thirdly; GCP is empanelled by MeitY. Google Cloud undergoes at least an annual third-party audit to certify individual products against the PCI DSS. This means that these services provide an infrastructure upon which customers may build their own services or applications which store, process, or transmit cardholder data.

Conclusion

Google Cloud comprehensively addresses the RBI Directive on storage of payment system data by offering multiple layers of preventive technical controls for a defense in depth approach. Using GCP data residency controls outlined in this document, customers can ensure storage of the relevant payment data within India. Further, Google Cloud contractually provides for access and audit rights to regulated customers and their regulators.