Google Cloud Whitepaper
February 2023

Google Cloud RBI Digital Lending Guidelines Whitepaper

Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of February 2023 and represents the status quo as of the time it was written. Google Cloud's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

As the digital lending ecosystem in India continues to evolve and shift to online platforms, regulators, including the Reserve Bank of India (RBI), have issued further guidance on customer protection and business conduct. In particular, in January 2022, RBI formed a Working Group (WG) and published guidelines on digital lending[1]. The Digital Lending Guidelines set out to accomplish a number of critical objectives. These include:

- Controlling engagement with third parties
- Addressing mis-selling
- Minimizing data privacy breaches
- Addressing unfair business conduct
- Eliminating charging of excessive interest rates
- Reducing unethical recovery practices

The regulatory framework focuses on the digital lending ecosystem of Regulated Entities (REs) and Lending Service Providers (LSPs) that REs engage with to extend their permissible credit facilitation services. Please see the section on Definitions below. In the context of this guideline, Google Cloud is not a LSP but may be a cloud service provider to Regulated Entities or Lending Service Providers. For example, a Lending Service Provider or a Regulated Entity, may use our services to host a Digital Lending App.

This whitepaper provides Google Cloud customers who come under the scope of the RBI guideline with information on how Google Cloud can support them with the requirements listed in **Section B. - Annexure I on Technology and Data Requirements**. This paper consolidates relevant information about Google Cloud's privacy and security posture, policies, and controls. We also provide details about how we protect **customer data** throughout its lifecycle and provide customers with transparency and control over their data. Documentation, protection, and control enable our customers to address the RBI Digital Lending Guidelines.

Definitions

Notably, the following two definitions can be found in the Digital Lending Guidelines and help further clarify the scope of the requirement.

Digital Lending Apps (DLA): Mobile and web-based applications with user interfaces that facilitate digital lending services. DLAs will include apps of the Regulated Entities (REs) as well as those operated by Lending Service Providers (LSPs) engaged by REs for extending any credit facilitation services in conformity with extant outsourcing guidelines issued by the Reserve Bank.

Lending Service Providers (LSP): An agent of a Regulated Entity who carries out one or more of lender's functions or part thereof in customer acquisition, underwriting support, pricing support,

[1] Guidelines on digital lending vide RBI/2022-23/111, DOR.CRE.REC.66/21.07.001/2022-23

servicing, monitoring, recovery of specific loan or loan portfolio on behalf of REs in conformity with extant outsourcing guidelines issued by the Reserve Bank.

Key Requirements

A Lending Service Provider or a Regulated Entity, may use Google Cloud products and services to host a Digital Lending App. Therefore, we'll focus on Section **B. of Annexure I** of the guidelines, which details the **Technology and Data Requirements** and how Google Cloud as a **Cloud service provider** can help REs and LSPs to meet the Technology and Data Requirements of this guideline. The guidelines also contain several requirements that deal with other aspects of the digital lending process. These are not relevant to the services that Google Cloud provides and are out of scope for this paper.

Several of the critical requirements are below.

Collection, usage, and sharing of data with third parties: Regulated Entities (RE) are required to ensure that any collection of data by their Digital Lending Apps (DLA) and Lending Service Providers (LSP) is need-based and with the prior and explicit consent of the borrower. It is the responsibility of the RE to ensure that explicit consent of the borrower is taken before sharing personal information with any third party, except for cases where such sharing is required as per statutory or regulatory requirements.

Storage of data: REs should ensure that LSPs and DLAs engaged by them don't store borrowers' personal information except for some basic minimal data (e.g., name, address, contact details of the customer) that may be required to carry out their operations. REs must put in place clear policy guidelines regarding the storage of customer data. Policy requirements include:

- The type of data that can be stored
- The length of time for which data can be stored
- Restrictions on the use of data
- Data destruction protocol
- Standards for handling security breach

Additionally, all borrower data must be stored in servers located within India, while ensuring compliance with statutory obligations/ regulatory instructions.

Comprehensive privacy policy: The guidelines also outline that REs should ensure that their DLAs and LSPs have a comprehensive privacy policy compliant with applicable laws, associated regulations, and RBI guidelines. The privacy policy should also disclose details of third parties (where applicable) allowed to collect personal information through the DLA.

Technology standards: REs are also responsible for ensuring that they comply with technology standards and cybersecurity requirements stipulated by RBI and other agencies, or that may be specified, for undertaking digital lending. It is also the REs responsibility to ensure the LSPs they engage with meet the same standards.

The WG has adopted a principles-based approach in its report The guidelines reflect this by advocating for high-level, broadly stated rules, objectives, and principles. This approach sets the standards that entities conduct business and safeguard **borrower and customer data**. RBI's guidelines on digital lending are directed to facilitate a secure, inclusive, and accessible digital lending ecosystem.

How Google Cloud helps

Our Trust Principles

At Google Cloud, we've set a high bar for what it means to host, serve, and protect our customers' data. Security and data protection are at the core of how we design and build our products. We start from the fundamental premise that Google Cloud customers own their data and control how it is used. The customer data stored and managed on Google Cloud is processed per your instructions in accordance with the Cloud Data Processing Addendum (CDPA) and for no other purpose. Our Google Cloud Trust Principles summarize our commitment to protecting the privacy of data stored by customers in Google Cloud.

1. You control your data

Customer data is your data, not Google's. We only process your data according to your agreement(s).

2. We never use your data for ads targeting

We do not process your customer data to create ads profiles or improve Google Ads products.

3. We are transparent about data collection and use

We're committed to transparency, compliance with regulations like the GDPR, and privacy best practices.

4. We never sell customer data or service data

We never sell customer data or service data to third parties.

5. Security and privacy are primary design criteria for all of our products

Prioritizing the privacy of our customers means protecting the data you trust us with. We build the strongest security technologies into our products.

We also know that privacy plays a critical role in earning and maintaining customer trust. That's why Google Cloud has developed industry-leading product capabilities that give you—our customers—control over your data and provide visibility into when and how your data is accessed. See how Google Cloud helps you comply with the privacy requirements of the guidelines by referring to Common Privacy Principles and Relevant Products.

Our trust principles guide the work that we do across Google Cloud and enable us to help our customers meet their requirements outlined under the RBI Digital Lending Guidelines.

Data localization

Google Cloud offers customers the ability to control where your data is stored.

Physical storage of data

Customers may configure the services listed at Google Cloud Platform Services with Data Residency to store customer data, which is the focus of the guideline in Mumbai (asia-south1) or Delhi (asia-south2), and Google Cloud will store that customer data at rest only in the selected Region/Multi-Region in accordance with our Service Specific Terms.

Cloud IAM configuration helps define access policies and precise access control to Google Cloud hosted data. With Cloud IAM, customers can prevent employees from accidentally storing 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. Customers can limit the physical location of a new resource with the Organization Policy Service resource locations constraint.

Location-based access

Google Cloud customers can use VPC Service Controls to restrict the network locations from which their users can access data, defining a service perimeter outside which customer data cannot be accessed. This functionality allows customers to limit user access by IP address filtering, even if the user is otherwise authorized. Cloud Armor also allows customers to restrict locations from which traffic is allowed to their external load balancer.

Securing your data

Security of Google Cloud's infrastructure

Google Cloud manages our infrastructure's security, including the hardware, software, networking, and facilities that support our services. Google Cloud provides detailed information to customers about our security practices, so they can understand and consider these practices as part of their risk analysis.

Security by default

You define the security of your data and applications in the cloud, which refers to the security measures you choose to implement and operate when using our services. The security of your data is paramount to Google Cloud, and we take the following proactive steps to assist you.

Encryption at rest - Google Cloud encrypts customer data stored at rest by default, with no additional action required from you.

Encryption in transit - Google Cloud encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google Cloud or on behalf of Google Cloud.

Security products

In addition to the other tools and practices available to you outside Google Cloud, you can choose to use tools we provide to enhance and monitor the security of your data. Information on Google Cloud's security products is available on our Cloud Security Products page and Security best practices and Security use cases.

More information about how we secure your data is available:

- On our Infrastructure security, infrastructure security design overview, and security resources pages.
- In our Google security overview whitepaper
- In our cloud-native security whitepaper

Safeguarding access to your data

At Google Cloud, protecting the sensitive data that customers and enterprises trust us with is a top priority. Our zero trust-based architecture and least privilege principles include the industry's strongest authentication protocols, are highly resistant to data exfiltration, and deploy 24/7 advanced monitoring and analytics to restrict the misuse of credentials, detect abnormal employee activity, and automatically respond to new or evolving threats.

With a team of security and privacy experts and inventive software design, we built our least-privilege framework from the ground up, guided by the principles of:

- Strong authentication and role-based, non-unilateral access restrictions
- End-to-end workload protection
- Continuous logging and auditing
- Transparency and Customer Control

Google Cloud's global technical infrastructure, designed to provide security through the entire information processing life cycle, provides secure deployment of services, storage of data with end-user privacy safeguards, communication between services, and secure and private communication with customers over the internet. To learn more, please refer to Google infrastructure security design overview.

The above snapshot of Google Cloud’s security measures highlights our robust infrastructure and technology standards designed to help support our customers. Regulated Entities should review their third parties' security and technology standards as outlined under the RBI’s Digital Lending Guidelines.

Data deletion & retention

Google Cloud takes a principled approach to storing and deleting Customer Data (as defined under our Cloud Data Processing Addendum). Google Cloud is engineered to achieve a high degree of speed, availability, durability, and consistency, and the design of systems optimized for these performance attributes must be balanced carefully with the need to achieve timely data deletion.

When you delete your Customer Data, Google Cloud's deletion pipeline begins by confirming the deletion request and eliminating the data iteratively from application and storage layers, from both active and backup storage systems. We further define this process in our data deletion whitepaper.

The logical deletion occurs in phases, beginning with marking the data for deletion in active storage systems immediately and isolating the data from ordinary processing at the application layer. Successive compaction and mark-and-sweep deletion cycles in Google Cloud's storage layers serve to overwrite the deleted data over time. Cryptographic erasure is also used to render the deleted data unrecoverable. Finally, backup systems containing snapshots of Google Cloud's active systems are retired on a standard cycle.

Deletion from application and storage layers may occur immediately depending on how data storage has been configured and the timing of ongoing deletion cycles in the relevant storage layers and data centers. Deletion from active systems typically completes within about two months of the deletion request. Finally, Customer Data is removed from Google Cloud's long-term backup systems, which preserve snapshots of Google systems for up to six months (180 days) to guard against natural disasters and catastrophic events.

Notably, data deletion and retention standards is a requirement under the RBI guidelines as defined in the storage of data section within Section B. - Annexure I.

Security & compliance standards

Moving to the cloud means protecting sensitive workloads while achieving and maintaining compliance with complex regulatory requirements, frameworks, and guidelines. Google Cloud's industry-leading security, third-party audits, and certifications help support your compliance. Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google undergoes several independent third-party audits regularly to provide this assurance. Some of the key international standards we are audited against are:

- ISO 27001 (Information Security Management)
- ISO 27017 (Cloud Security)
- ISO 27018 (Cloud Privacy)
- ISO/IEC 27701 (Privacy - Data Processor)
- SOC 2 and SOC 3
- NIST 800-53

- PCI DSS
- CSA Star

Please visit our compliance resource center for a complete list of our compliance offerings. Our additional compliance offerings provide additional support, documentation, and transparency into Google Cloud's compliance approach beyond the RBI Digital Lending Guidelines.

Data Incident Response Process

Google's highest priority is to maintain a safe and secure environment for customer data. To help protect customer data, we run an industry-leading information security operation that combines stringent processes, an expert incident response team, and multi-layered information security and privacy infrastructure. Experts from these teams are engaged in a variety of ways. For example, incident commanders coordinate incident response and, when needed, the digital forensics team performs forensic investigations and tracks ongoing attacks. Product engineers work to limit the impact on customers and provide solutions to fix the affected products. Counsel works with members of the appropriate security and privacy team to implement Google's strategy on evidence collection, engage with law enforcement and government regulators, and advise on legal issues and requirements. Customer Care responds to customer inquiries and requests for additional information and assistance. This document explains our principled approach to managing and responding to data incidents in Google Cloud.

Conclusion

Protecting customer data is a primary design consideration for Google Cloud's infrastructure, applications, and personnel operations. Google Cloud's security practices are verified by independent third parties, assuring customers regarding our security controls and practices.

Google Cloud offers strong contractual commitments to ensure our customers maintain control over their data and its processing, including the commitment that we only process your customer data according to your instructions. Google Cloud is designed to meet stringent privacy and security standards based on industry best practices. Google has strong contractual commitments regarding data ownership, data use, security, transparency, and accountability. These commitments ensure you maintain control over your data and how it is processed, including the assurance that your data is not used for advertising or any purpose other than to deliver Google Cloud services. In addition, we give you the tools you need to help meet your compliance and reporting requirements.

Furthermore, because protecting data is core to Google Cloud, we invest extensively in security, resources, and expertise at a scale. Our investment frees you to focus on your business and innovation. Google Cloud's operations and collaboration with the security research community also enable us to address or prevent vulnerabilities quickly. For these reasons and more, organizations across the globe trust Google with their most valuable asset: their information. Google will continue to invest in Google Cloud to allow you to benefit from our services securely and transparently.