



CUSTOMER DATA STORAGE, RETENTION, ARCHIVAL AND DESTRUCTION POLICY

**DOCUMENT CONTROL:**

Policy / Document Title	Customer Data Storage, Retention, Archival and Destruction Policy
Applicable To	Mufin Green Finance Limited (“MGFL” / “the Company”)
Current Version	V.01
Current Status	Final
Current Effective Date	02 nd September, 2026
Next Review Date	01 st September, 2027
Document Owner	Mr. Manoj Taneja

VERSION & APPROVAL HISTORY:

Version	Created / Revised By	Reviewed By	Approved By	Approval Date	Effective Date	Change Description
V.01	Mr. Deepak Bansal	Mr. Manoj Taneja and Mr. Prakash Pogaku	Board of Directors (on the recommendation of IT Strategy Committee)	02 nd September, 2026	02 nd September, 2026	Initial version – Adopted pursuant to RBI (Non- Banking Financial Companies – Credit Facilities) Directions, 2025, RBI (Non-Banking Financial Companies - Managing Risks in Outsourcing) Directions, 2025, DPDP Act, 2023 and rules made thereunder.



Table of Contents

1. Introduction and Purpose	4
1.1 Objectives.....	4
2. Scope and Applicability	4
2.1 In Scope.....	4
2.2 Out of Scope.....	4
3. Definitions and Abbreviations	4
4. Regulatory and Reference Framework	5
5. Data Governance Principles.....	5
6. Customer Data Categories	6
7. Data Storage, Security and Localisation	6
7.1 Storage Standards.....	6
7.2 Security Controls.....	6
7.3 Data Localisation and Residency	6
7.4 Data Masking	6
8. Access Control	7
9. Customer Data Retention	7
10. Data Archival	7
11. Legal Hold and Preservation.....	8
12. Data Sharing, Third-Party and Outsourcing	8
13. Data Destruction and Secure Disposal.....	8
14. Data-Principal Rights and Privacy	8
15. Roles and Responsibilities	8
16. Audit, Monitoring and Metrics	9
17. Policy Exceptions and Enforcement	9
18. Regulatory Compliance and Precedence.....	9
19. Review, Maintenance and Board Approval	9
Annexure A – Data Destruction Register (Template).....	10



1. Introduction and Purpose

Mufin Green Finance Ltd. (“MGFL” or the “Company”), a Non-Banking Financial Company registered with the Reserve Bank of India (RBI), recognises that customer information is a critical business and regulated asset. The Company is committed to protecting the confidentiality, integrity, availability, and privacy of customer data across its entire lifecycle – from collection and storage through retention, archival, sharing, and secure destruction.

The purpose of this Policy is to establish a consistent, risk-based, and compliant framework governing how customer information is stored, retained, archived, and destroyed, so that the Company meets its obligations under applicable RBI directions, data-protection law, and other statutory and contractual requirements while avoiding over-retention of personal data.

1.1 Objectives

- Protect customer information against unauthorised access, disclosure, alteration, loss, or misuse.
- Define the categories of customer data that may be collected and stored.
- Establish retention periods for customer records based on regulatory, legal, and business requirements.
- Define secure storage, localisation, archival, and destruction requirements and evidence.
- Uphold data-principal rights under the DPDP Act, 2023, consistent with mandatory retention obligations.
- Establish clear accountability, audit trails, and oversight for customer-data governance.

2. Scope and Applicability

This Policy applies to all customer information collected, processed, stored, transmitted, archived, or destroyed by or on behalf of the Company, in any format (structured or unstructured; electronic or physical), regardless of the systems, environments, or service providers involved.

2.1 In Scope

- All customer information across all business applications, databases, infrastructure, storage repositories, and backups maintained by or for the Company.
- All customer data hosted on Company-owned infrastructure, approved data centres in India, and approved cloud (IaaS/PaaS/SaaS) environments.
- All employees, directors, officers, consultants, contractors, and outsourced/cloud service providers who handle customer information.

2.2 Out of Scope

- Non-customer corporate records, governed by the Company’s general Records Retention arrangements.
- Personal use of consumer applications by employees, governed by the Acceptable Use Policy.

Where a conflict arises between this Policy and another internal policy, the more stringent control shall prevail, subject to CISO review. Where a provision conflicts with a mandatory regulatory requirement, the regulatory requirement shall prevail.

3. Definitions and Abbreviations

Term	Definition
Customer Data / Information	Any information relating to a customer or prospective customer, including identity, KYC, contact, financial, transaction, and digital-lending information, in any format.
Personal Data	Any data about an individual who is identifiable by or in relation to such data, as defined under the DPDP Act, 2023.



Term	Definition
Sensitive Personal Data (SPDI)	Information as defined under the SPDI Rules, 2011 (e.g., financial information, passwords), where applicable.
Retention Period	The minimum period for which a category of customer records must be retained to meet regulatory, legal, or business requirements.
Archival	The controlled transfer of records no longer in active use to secure storage for the remainder of their retention period, in a retrievable and usable form.
Legal Hold	A directive to preserve records – overriding scheduled destruction – where they are relevant to an audit, investigation, litigation, or regulatory proceeding.
Secure Disposal / Destruction	Rendering records permanently irrecoverable using approved methods, on expiry of the retention period and absent any legal hold.
Data Localisation	The regulatory requirement that certain categories of data be stored (and in some cases processed) within India.
Data Principal	The individual to whom personal data relates, as defined under the DPDP Act, 2023.

4. Regulatory and Reference Framework

This Policy is designed to align with applicable regulatory directions and standards, and shall be kept current as regulations evolve. Key references (as applicable and amended from time to time) include:

- Reserve Bank of India (Non-Banking Financial Companies – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026.
- Reserve Bank of India (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025.
- RBI Master Direction on Know Your Customer (KYC)-2025, and the Prevention of Money-Laundering Act, 2002 and Rules-2005 thereunder (customer-record retention).
- RBI directions on Storage of Payment System Data (data localisation), where the Company operates or participates in payment systems.
- RBI Guidelines on Digital Lending under RBI Direction on Credit Facilities for NBFCs-2025, where customer data arises from digital-lending arrangements.
- Applicable Scale-Based Regulation (SBR) framework requirements for NBFCs (Middle Layer).
- The Digital Personal Data Protection (DPDP) Act, 2023 and rules made thereunder.
- Information Technology Act, 2000 and the SPDI Rules, 2011.
- Applicable industry standards adopted by the Company, including ISO/IEC 27001, ISO/IEC 27017/27018, and SOC 2.

Note: Legal and Compliance must validate the specific clauses, retention periods, and regulatory citations against the Company's licence category, activities, and the latest RBI instructions before adoption. Where any provision conflicts with a mandatory regulatory requirement, the regulatory requirement prevails.

5. Data Governance Principles

- **Data Minimisation:** only information necessary for legitimate business, regulatory, legal, and operational purposes shall be collected and retained.
- **Purpose Limitation:** customer information shall be collected and processed only for lawful, specified, and authorised purposes.
- **Storage Limitation:** customer data shall not be retained beyond the longest applicable retention period, after which it shall be securely disposed of unless under legal hold.
- **Security by Design:** appropriate technical and organisational controls shall be embedded throughout the data lifecycle.



- **Data Sovereignty:** customer and regulated data shall remain within Indian jurisdiction unless a documented, legally permissible exception is approved.
- **Accountability Retained:** use of vendors or CSPs does not transfer the Company's accountability to its customers or regulators.
- **Traceability and Auditability:** storage, access, retention, archival, and destruction actions shall be logged and auditable.

6. Customer Data Categories

The Company may collect and maintain the following categories of customer information, subject to data minimisation:

Category	Examples
Identity Information	Name, photograph, date of birth, gender, signature, customer identification number.
KYC Information	PAN, Aadhaar (as permitted by law), passport, driving licence, voter ID, CKYC identifier.
Contact Information	Address, mobile number, email address.
Financial Information	Bank-account details, income documents, credit-bureau information, repayment information.
Transaction Information	Loan applications, sanction details, repayment history, collection records.
Digital-Lending Information	Consent records, Key Fact Statements, digital acceptance records, audit logs.

7. Data Storage, Security and Localisation

7.1 Storage Standards

- Customer information shall be stored only on Company-owned infrastructure, RBI-compliant cloud environments approved by the Company, or authorised data centres located within India.
- Customer information shall not be stored on unauthorised devices, removable media, personal systems, or unapproved cloud platforms.

7.2 Security Controls

The following minimum controls shall apply: encryption of sensitive information at rest and in transit; role-based access control; multi-factor authentication for privileged users; database activity monitoring; security logging and audit trails; tested backup and recovery; and periodic Vulnerability Assessment and Penetration Testing (VAPT). Encryption keys shall remain under the Company's control where technically feasible.

7.3 Data Localisation and Residency

- Customer data and other regulated data shall be stored within India in accordance with applicable RBI directions and data-protection law, throughout storage, archival, and back-up.
- Any storage, processing, or cross-border transfer outside India shall be undertaken only where permitted by the DPDP Act, 2023 and applicable RBI requirements, subject to prior Legal/Compliance review, and shall not derogate from localisation obligations.
- Approved CSPs shall provide documented evidence of the physical location(s) where customer data is stored and processed.

7.4 Data Masking

Sensitive identifiers such as PAN, Aadhaar number, and bank-account number shall be masked in user interfaces, reports, and non-production environments wherever operationally feasible.



8. Access Control

Access to customer information shall be governed by the need-to-know and least-privilege principles and enforced through Role-Based Access Control (RBAC). User access shall be formally approved, periodically reviewed, and revoked immediately upon employee separation or role change. Privileged access shall be logged and time-bound where technically feasible.

9. Customer Data Retention

Customer information shall be retained only for as long as necessary to fulfil business, legal, audit, and regulatory requirements, and shall then be disposed of in accordance with Section 12. Where multiple periods apply to the same record, the longest applicable period governs. The minimum retention periods below are indicative and shall be validated by Legal/Compliance against the current statutory and RBI text before adoption.

Record Category	Minimum Retention	Legal / Regulatory Basis
KYC & Customer Identification Records	5 years after end of business relationship	PMLA / RBI KYC MD
Transaction Records	5 years from date of transaction	PMLA
Loan Application Files	10 years	Business / legal
Loan Agreements	10 years after closure of account	Limitation Act / recovery
Repayment & Collection Records	10 years	Business / audit
Credit-Information (CIC) Records	As per CICRA / RBI	CIC (Regulation) Act
CKYC Records	10 years	RBI KYC MD / CERSAI
Digital-Lending Records (KFS, consent)	10 years	RBI Digital Lending
Customer Communications	8 years	Business
Audit Logs	Minimum 2 years	RBI IT MD on Cybersecurity, Technology: Risk, Resilience and Assurance Framework
Security Logs	Minimum 180 days online; archived for applicable period	RBI cyber-security

Where any investigation, litigation, audit, inspection, or regulatory proceeding is pending or reasonably anticipated, relevant records shall be preserved under legal hold (Section 11) until its closure, notwithstanding the periods above.

10. Data Archival

Data no longer required for active operations but still within its retention period shall be archived in secure repositories. Archived records shall remain encrypted, be protected against unauthorised modification, retain their audit trails, and be recoverable in a usable format when required. Archival location shall satisfy the localisation requirements in Section 7.3.



11. Legal Hold and Preservation

Scheduled destruction shall be suspended for records required for RBI inspections, internal or external audits, litigation, law-enforcement investigations, or regulatory proceedings. A legal hold shall be issued in writing, identify the records and custodians affected, be logged, and remain in force until formally released by the authorising function. Records under hold shall not be altered, moved, or destroyed.

12. Data Sharing, Third-Party and Outsourcing

Customer information may be shared only with customer consent where required, to comply with a legal or regulatory obligation, or with authorised service providers under valid contractual arrangements. Where storage, archival, or destruction is performed by a third party or CSP, the Company's Cloud Adoption Policy and outsourcing controls apply in addition to this Policy.

- Vendors shall execute confidentiality and data-protection agreements and maintain security controls at least equivalent to the Company's standards.
- Contracts shall preserve the right of the Company, its auditors, and the RBI to audit and inspect, extending to sub-contractors.
- Contracts shall require secure deletion or return of customer data on termination, evidenced by a certificate of destruction and, for material data, independently assured.
- Data-localisation and breach-notification obligations shall flow down to the provider and its sub-processors.

13. Data Destruction and Secure Disposal

On expiry of the applicable retention period and absent any legal hold, customer information shall be securely destroyed using approved methods:

- **Electronic records:** secure deletion, cryptographic erasure, database purging, or media sanitisation.
- **Physical records:** cross-cut shredding, pulverisation, or secure destruction through authorised agencies.

Destruction shall be authorised by the designated approver and evidenced. The Company shall maintain a Data Destruction Register (Annexure A) recording the records destroyed, retention period completed, date and method of destruction, approving authority, and evidence of destruction.

14. Data-Principal Rights and Privacy

Consistent with the DPDP Act, 2023, the Company shall provide data principals with the ability to access, correct, and seek erasure of their personal data, and to raise grievances through the designated channel. Requests for erasure shall be honoured except where retention is required by law or regulation, in which case the data shall be retained only for the mandated period and purpose. Personal-data breaches shall be handled under the Incident Management process, including notification to affected data principals and the Data Protection Board of India and, where the breach also constitutes a cyber incident, reported to the RBI within six hours of detection on the RBI DAKSH platform (<https://daksh.rbi.org.in>) with notification to CERT-In, in accordance with the RBI (NBFCs – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026.

15. Roles and Responsibilities

Role	Key Responsibilities
Board of Directors	Approves the Policy; provides oversight of data governance; reviews the Policy at least annually.
IT Strategy Committee	Monitors implementation and recommends the Policy and material changes to the Board.



Role	Key Responsibilities
CIO / CTO	Owens the Policy; ensures methodology, resourcing, and implementation.
CISO	Ensures implementation of technical controls, monitoring, and security exceptions; oversees evidence.
Chief Compliance Officer	Confirms regulatory, localisation, and retention compliance; oversees any RBI reporting.
Chief Risk Officer	Oversees data and concentration risk; reviews KRIs and material adverse events.
Data Protection / Grievance Officer	Handles data-principal rights, consent, and privacy grievances under the DPDP Act, 2023.
Business Functions / Data Owners	Ensure proper handling, classification, retention, and disposal of customer information.
Internal Audit	Independently assesses the effectiveness of controls and compliance with this Policy.
All Employees & Contractors	Comply with this Policy and report suspected breaches or data-quality issues.

16. Audit, Monitoring and Metrics

Compliance with this Policy shall be monitored through a retention and disposal register, periodic access reviews, and internal audit. The Company shall track indicative metrics including records due for disposal versus disposed, overdue-for-destruction records, legal holds in force, access-review completion, and data-principal requests closed within timelines. Records shall be made available to internal audit and the RBI on request.

17. Policy Exceptions and Enforcement

Any exception to this Policy must be formally documented, justified on a risk basis, time-bound, and approved by the CISO and the relevant governance authority; exceptions involving regulatory requirements shall additionally be reviewed by Compliance and Legal. Exceptions shall be recorded in exceptions register and reviewed at expiry. Compliance with this Policy is mandatory; non-compliance may result in disciplinary or contractual action up to termination, regulatory reporting, and legal proceedings, as applicable.

18. Regulatory Compliance and Precedence

In the event of any conflict or inconsistency between the provisions of this Policy and the applicable laws, rules, regulations, notifications, circulars or directions issued by the Reserve Bank of India (RBI) or any other competent authority, the provisions of the applicable law or regulatory requirements shall prevail.

19. Review, Maintenance and Board Approval

This Policy shall be reviewed by the Board (or its delegated Committee) at least annually, or earlier upon any significant change in regulation, technology, the threat landscape, a security incident, or the Company's risk appetite. The Document Owner is responsible for initiating the review, and material changes require re-approval. This Policy has been reviewed and approved by the Board of Directors of Mufin Green Finance Ltd. and shall remain effective until amended or replaced.



Annexure A – Data Destruction Register (Template)

This register shall be maintained as evidence of secure disposal and made available to internal audit and the RBI on request.

#	Records Destroyed	Retention Completed	Date & Method	Approved By	Evidence Ref.
1					
2					
3					
