Data Retention and Disposal Policy

CONFIDENTIAL

Document Control

Organisation	Ecofy
Title	Data Retention & Disposal Policy
Filename	Ecofy Data Retention and Disposal Policy
Owner	CISO, DPO
Classification	CONFIDENTIAL

Version History

Version	Issue Date	Prepared By	Approved By	Description of Revision
Draft	03-07-2026	CTO		First draft
1.0	15-07-2026	CTO	Board of Directors	Review comments incorporated from Internal Audit

Disclaimer:

This document is solely for the information of Ecofy and should not be used, circulated, quoted or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without our prior written consent.

CONFIDENTIAL

Contents

1. OBJECTIVES 4
2. SCOPE AND APPLICABILITY 4
3. DEFINITIONS 4
4. DATA RETENTION SCHEDULE 5
4.1. CUSTOMER IDENTIFICATION, KYC AND AML RECORDS 5
4.2. LENDING, CREDIT AND COLLECTIONS RECORDS 6
4.3. CYBER SECURITY RECORDS 6
5. DISPOSAL STANDARDS 6
6. LEGAL HOLD 7
7. ROLES AND RESPONSIBILITIES 7
8. GOVERNANCE AND REVIEW 8

CONFIDENTIAL

1. OBJECTIVES

Ecofy, being a Non-Banking Financial Company registered with the Reserve Bank of India ("RBI"), creates, collects, and processes a large volume of personal, financial, and operational data during its lending, payments, and customer-facing operations. This Policy establishes the principles, retention timelines, and disposal mechanisms governing all data created or held by the Company, whether in physical or electronic form.

This Policy is framed to give effect to two complementary, and at points overlapping, regulatory regimes:

- **RBI's record-keeping mandates** — which require Regulated Entities to preserve KYC, transaction, audit, IT governance, and outsourcing records for prescribed minimum periods to support supervision, anti-money laundering (AML) enforcement, and fraud investigation

- **The Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 ("DPDP Act")** — which require that personal data be retained no longer than is necessary for the purpose for which it was collected, and be erased once that purpose is served, subject to overriding legal retention obligations.

Where the two regimes appear to conflict — i.e., where the DPDP Act's storage-limitation principle would require earlier erasure than an RBI-mandated minimum period — **the longer, legally-mandated retention period prevails**.

2. SCOPE AND APPLICABILITY

- All employees, officers, directors, and contractual/temporary staff of the Company
- All data — physical and electronic — created, collected, processed, or stored by or on behalf of the Company, including data held by third-party service providers, cloud infrastructure providers, Business Correspondents, Digital Lending App (DLA) partners, Lending Service Providers (LSPs), and other outsourced vendors acting as Data Processors
- All systems and repositories: core Loan Management System (LMS), Loan Origination System (LOS), core accounting systems, CRM, collections platforms, email and collaboration tools, backups, and physical registries/archives

3. DEFINITIONS

Term	Definition
Personal Data	Data about an individual who is identifiable by or in relation to such data, as defined under Section 2(t) of the DPDP Act, 2023.
Data Fiduciary	The Company, which determines the purpose and means of processing personal data (Section 2(i), DPDP Act).
Data Principal	The individual to whom the personal data relates, including a customer, borrower, guarantor, employee, or vendor contact (Section 2(j), DPDP Act).

CONFIDENTIAL

Term	Definition
Data Processor	Any person who processes personal data on behalf of the Company, including cloud hosting providers, DLA partners, and BPO/collections vendors (Section 2(k), DPDP Act).
Record Owner	The functional head (e.g., Head-Credit, Head-Operations, CFO, CISO) accountable for a defined category of records under this Policy.
Retention Period	The minimum period for which a record/data category must be preserved, as set out in the Retention Schedule (Section 6).
Legal Hold	A suspension of routine disposal applicable to specific records subject to litigation, regulatory inquiry, or law-enforcement request.
Secure Disposal	Irreversible destruction or anonymisation of data such that it cannot be reconstructed, in line with Section 8 (Disposal and Erasure Standards).

4. DATA RETENTION SCHEDULE

The table below sets out the minimum retention period for each category of data/record held by the Company. Retention periods are computed from the trigger event stated (e.g., transaction date, relationship closure, financial year-end). No record listed below shall be erased before the stated minimum period unless an explicit, documented exception applies (Section 9).

4.1. Customer Identification, KYC and AML Records

Data / Record Category	Examples	Minimum Retention Period
Customer KYC records	Identity & address proof, photographs, PAN/Aadhaar references, CKYC data, customer risk profile	8 years after end of customer relationship / account closure
Transaction records	Loan disbursement, repayment, NACH/UPI mandates, ledger entries	8 years from the date of transaction
Video-KYC (V-CIP) recordings and digital KYC artefacts	V-CIP video, liveness check data, geo-tagging metadata	8 years after end of relationship, subject to RBI V-CIP storage norms

CONFIDENTIAL

4.2. Lending, Credit and Collections Records

Data / Record Category	Examples	Minimum Retention Period
Loan application & origination data	Application forms, income proof, bureau pulls, sanction letters, loan agreements	8 years from loan closure / settlement / write-off
Credit appraisal & underwriting records	Credit memos, BRE/scorecard outputs, approval notes	8 years from loan closure
Digital Lending App (DLA) data and consents	App permissions log, data collected via DLA, borrower consent artefacts	8 years from loan closure; consent withdrawal honoured promptly
Collections & recovery records	Call logs, field visit notes, legal notices, recovery proceedings	8 years from recovery action closure, or until conclusion of litigation plus limitation period

4.3. Cyber Security Records

Data / Record Category	Examples	Minimum Retention Period
System access & authentication logs	Privileged access logs, login/logout events, VPN logs	Minimum 1 year (aligned to log retention norm); longer if linked to an open incident
Cybersecurity incident & SOC logs	SIEM alerts, forensic images, incident response reports	Minimum 3 years from closure of the incident, or until conclusion of any regulatory proceeding

5. DISPOSAL STANDARDS

On expiry of the applicable retention period, records shall be disposed of as follows:

- **Electronic data:** secure overwrite or cryptographic erasure (destruction of the encryption key) for encrypted cloud storage where overwriting is not feasible.
- **Backups:** expired data is excluded from live access and purged on the next backup-rotation cycle. Immediate deletion from immutable backups is not required where technically not feasible, provided the backup is encrypted and inaccessible through normal channels.
- **Physical media:** degaussing, shredding, or incineration by a certified vendor. A Certificate of Destruction is obtained and logged.
- **Vendor / cloud environments:** written deletion instructions are issued to the relevant Data Processor or vendor. Written certification of deletion must be obtained and filed.

CONFIDENTIAL

Every disposal event must be logged, capturing the record category, disposal method, date, and authorising Record Owner. Disposal logs are retained for 5 years as audit evidence.

6. LEGAL HOLD

Routine disposal is suspended for any record subject to a Legal Hold. A Legal Hold is activated when:

- Litigation, arbitration, or regulatory/enforcement proceedings are pending and the records are potentially relevant.
- RBI, CERT-In, the Data Protection Board, or law enforcement has requested specific records.
- A cybersecurity or breach investigation is in progress and the records form part of the forensic evidence.

The Legal and Compliance function issues a written Legal Hold Notice identifying the records covered, the reason, and the responsible Record Owner. No record under an active Hold may be disposed of until the Hold is formally lifted in writing. The CISO is notified simultaneously.

7. ROLES AND RESPONSIBILITIES

Role	Responsibility
Board of Directors	Approves this Policy
IT Strategy Committee (Board-level)	Provides ongoing oversight of technology data risks; reviews material control failures.
CISO / DPO	Policy owner. Maintains the Data Inventory and Retention Register, oversees disposal events, coordinates Legal Holds, and serves as regulatory contact with RBI and the Data Protection Board.
Legal and Compliance	Issues and lifts Legal Holds; advises on conflicts between RBI retention minimums and DPDP erasure obligations.
IT / Infrastructure / Security Teams	Implement retention controls, automated erasure jobs, log-integrity configurations, and backup-purge cycles. Execute and document disposal of expired records. Ensures outsourcing and cloud contracts include retention and disposal clauses; obtains data-deletion certificates on vendor exit.
IS Audit / Internal Audit	Independently verifies adherence to this Policy as part of the annual IS Audit; reports exceptions to the Audit Committee.
Technology Vendors and Data Processors	Comply with the retention and disposal requirements in their contracts; certify deletion in writing on contract exit or request.

CONFIDENTIAL

8. GOVERNANCE AND REVIEW

- This Policy is approved by the Board of Directors and comes into effect from the date of such approval.
- The CISO / DPO is the Policy Owner and is responsible for maintaining the Technology Data Inventory and Retention Register.
- The Policy is reviewed annually, or earlier on a material change in RBI / DPDP Rules or the Company's technology architecture.
- A half-yearly compliance dashboard (active Legal Holds, disposal events, outstanding erasure requests) is presented to the IT Steering Committee. An annual summary is presented to the IT Strategy Committee.
- Any reduction in a minimum retention period below the regulatory floor requires prior approval of the CTO, CISO and DPO.
- This Policy supersedes all prior informal or departmental practices on technology data retention and disposal.

CONFIDENTIAL