EVAM FINANCE PRIVATE LIMITED

India's Climate Finance Platform | RBI-Registered NBFC

COMPREHENSIVE PRIVACY POLICY

Framework for Processing of Personal Data — DPDP Act 2023 & DPDP Rules 2025

1. Purpose & Scope

Evam Finance Private Limited ("Evam" or the "Company") collects and processes personal data of its customers, employees, applicants, counterparties, vendors, and other stakeholders in the course of its regulated NBFC business. This Comprehensive Privacy Policy ("Policy") establishes the principles, obligations, and operational framework that govern how Evam processes such personal data — fully aligned with the Digital Personal Data Protection Act, 2023 ("DPDP Act") and the Digital Personal Data Protection Rules, 2025 ("DPDP Rules") notified on 13/14 November 2025.

This Policy applies to:

- All personal data processed by Evam, in any form (electronic or otherwise), as a Data Fiduciary, irrespective of where the data is stored or processed;
- All Evam employees, directors, officers, contractors, and third-party service providers processing personal data on Evam's behalf;
- All processing activities — collection, recording, storage, retrieval, use, alignment, disclosure, transfer, deletion, or destruction of personal data.

This is an internal governance Policy.

2. Applicable Legal Framework

Evam Finance Private Limited ("Evam" or the "Company") is a Non-Banking Financial Company (NBFC) registered with the Reserve Bank of India (RBI). This Policy is framed and maintained in accordance with applicable provisions of the Companies Act, 2013, the Reserve Bank of India Act, 1934, and the RBI Master Directions and Circulars applicable to NBFCs, including — without limitation — the RBI Master Direction on Scale-Based Regulation for NBFCs (as amended), applicable Fair Practices and Conduct guidelines, and the Company's Board-approved governance framework.

This Policy gives effect to and shall be read together with:

- Digital Personal Data Protection Act, 2023 (DPDP Act);
- Digital Personal Data Protection Rules, 2025 (DPDP Rules) — notified on 13/14 November 2025, with phased commencement: Phase 1 immediate (Data Protection Board); Phase 2 (Consent Manager framework) effective ~November 2026; Phase 3 (substantive obligations — notices, security, breach notification, erasure, rights, cross-border transfer, SDF obligations) effective ~May 2027;
- Information Technology Act, 2000 and the IT (Reasonable Security Practices) Rules, 2011 — to the extent operative;
- RBI Master Direction – Know Your Customer (KYC) Direction, 2016 (as amended);
- Prevention of Money Laundering Act, 2002 and PML Rules, 2005;
- RBI Fair Practices Code for NBFCs;
- RBI Master Direction on IT Governance, Risk, Controls and Assurance Practices, 2023 (voluntarily adopted as best practice — direct applicability commences upon transition to NBFC-Middle Layer);
- Credit Information Companies (Regulation) Act, 2005;
- Companies Act, 2013;

- Bharatiya Sakshya Adhiniyam, 2023.

Where the DPDP Act / Rules provide a higher standard of protection than other applicable laws, the DPDP Act / Rules shall prevail. Where another sector-specific law (e.g., RBI KYC retention) requires retention or processing that the DPDP Act / Rules might otherwise restrict, the sector-specific law shall apply to the extent of such requirement.

3. Key Definitions (DPDP Act)

Term	Meaning
Personal Data	Any data about an individual who is identifiable by or in relation to such data.
Data Principal	The individual to whom the personal data relates; for children, includes parents / lawful guardians; for persons with disabilities, includes lawful guardians.
Data Fiduciary	Any person who, alone or in conjunction with others, determines the purpose and means of processing personal data — Evam acts as a Data Fiduciary.
Data Processor	Any person who processes personal data on behalf of a Data Fiduciary.
Processing	Any operation or set of operations performed on personal data — including collection, recording, organisation, storage, alteration, retrieval, use, disclosure, sharing, transfer, restriction, erasure, or destruction.
Significant Data Fiduciary (SDF)	A Data Fiduciary or class of Data Fiduciaries notified by the Central Government, having regard to volume / sensitivity of data processed, risk to Data Principals, risk to electoral democracy / sovereignty, public order, etc.
Consent Manager	A person registered with the Data Protection Board, enabling Data Principals to give, manage, review, and withdraw consent through an accessible, transparent, interoperable platform.
Personal Data Breach	Any unauthorised processing, accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity, or availability of personal data.
Data Protection Board / DPBI	The Data Protection Board of India established under the DPDP Act, vested with powers of investigation, adjudication, and imposition of penalties.

4. Core Privacy Principles

1. Lawfulness — personal data shall be processed only for lawful purposes, on a legal basis recognised under the DPDP Act.
2. Notice & Transparency — Data Principals shall receive clear, plain-language notice about the personal data collected, purposes, exercise of rights, and grievance channels.
3. Consent (where applicable) — where consent is the legal basis, it shall be free, specific, informed, unambiguous, given by clear affirmative action, and limited to the purposes for which it is necessary.

4. Purpose Limitation — personal data shall be used only for the purpose(s) for which it was collected, or compatible / connected purposes.
5. Data Minimisation — only personal data necessary for the identified purpose shall be collected.
6. Accuracy — reasonable efforts shall be taken to ensure data is accurate, complete, and up to date.
7. Storage Limitation — data shall not be retained beyond the period necessary, subject to legal retention obligations.
8. Reasonable Security Safeguards — data shall be protected through reasonable technical and organisational measures.
9. Accountability — Evam is responsible for, and able to demonstrate, compliance with the DPDP Act and this Policy.
10. Rights of Data Principals — Evam shall facilitate exercise of the access, correction, erasure, grievance redressal, and nomination rights.

5. Categories of Personal Data Processed by Evam

Data Principal Category	Indicative Categories of Personal Data
Loan applicants & customers (including promoters / directors / authorised signatories / guarantors of corporate customers)	Name, address, contact details, date of birth; KYC data (PAN, Aadhaar, passport, voter ID, driving licence); photographs; bank account / financial information; income / financial statements; income-tax / GST records; credit bureau data; signature; references; transaction history; security / asset information; communication records (calls, emails); web / mobile-app usage data (where applicable)
Employees, applicants, contractors	Name, address, contact details, family / dependent information; KYC; bank / PF / ESI / tax data; salary and benefits; education and professional credentials; performance records; medical / disability information (where voluntarily provided); CCTV / access-card data at offices
Counterparties / vendors / partners (and their representatives)	Name, designation, contact details, business address; KYC of authorised representatives; bank account details; commercial terms; correspondence
Website / digital-channel visitors	IP address, device identifiers, browser / OS information, cookies, behavioural / usage data (where applicable)

6. Legal Basis for Processing

Evam processes personal data on one or more of the following legal bases recognised under the DPDP Act:

6.1 Consent (Section 6)

Free, specific, informed, unconditional, and unambiguous consent, given by a clear affirmative action. Consent shall:

- Be sought through a standalone, plain-language Notice explaining the personal data sought, the specific purposes, the manner of withdrawal, and how to lodge a complaint;
- Be granular — separate consent for distinct purposes;
- Be withdrawable at any time, with the consequences of withdrawal explained;
- Be capable of being given in English or any language listed in the Eighth Schedule to the Constitution of India, at the Data Principal's option;
- Be obtainable directly or through a Consent Manager (once the Consent Manager framework is operational per the DPDP Rules timeline).

6.2 Legitimate Uses (Section 7 — Specified Without Consent)

Personal data may be processed without consent for certain "Legitimate Uses" specified under Section 7 of the DPDP Act, including:

- Voluntary provision by the Data Principal for a specified purpose, where withdrawal of consent has not been signalled;
- Provision of any service / benefit by the State or its instrumentalities under law;
- Performance of any function under law;
- Compliance with a judgment or court order;
- Responding to a medical emergency;
- Disaster / breakdown of public order;
- Employment purposes (including verification, payroll, benefits, performance management, safeguarding the employer's interests, and prevention of corporate espionage / theft) — Evam relies on this basis for employee data processing.

6.3 RBI Compliance & Regulatory Obligation

Personal data may be processed where required to comply with RBI directions, PMLA, KYC norms, credit bureau reporting, or any other applicable law or judgment, even in the absence of independent consent for the specific processing.

7. Notice to Data Principals

Pursuant to Section 5 of the DPDP Act and Rule 3 of the DPDP Rules, every Data Principal whose personal data is processed by Evam shall be given a clear, standalone Notice that:

- Identifies Evam as the Data Fiduciary;
- Provides an itemised description of the personal data being collected;
- States the specific purpose(s) for which the personal data is to be processed;
- Describes the goods, services, or uses enabled by such processing;
- Explains the manner in which the Data Principal may exercise rights under Sections 11–14 of the DPDP Act (access, correction, erasure, grievance, nomination);
- Explains the manner of withdrawal of consent (where consent is the legal basis);
- Provides the contact information of the Data Protection Officer / Grievance Officer;

- Explains the manner of lodging a complaint with the Data Protection Board of India.

The Notice shall be available in English and may be requested in any of the 22 languages listed in the Eighth Schedule. Notices are independent of, and shall not be combined with, terms and conditions or unrelated content.

7.1 Channels for Delivery of Notice

- Loan application forms / Sanction Letters — embedded or attached Notice;
- Evam website — published Privacy Notice and cookie notice;
- Customer-onboarding journeys (digital or physical);
- Employee onboarding — Notice provided at offer / joining;
- Vendor / counterparty engagement — Notice in master service / vendor agreements.

8. Consent Management

8.1 Obtaining Consent

- Consent shall be recorded in a verifiable form (digital tick-box with timestamp / IP; physical signature on Notice; recorded affirmation in V-CIP);
- Pre-ticked / inferred consent shall NOT be relied upon for personal data processing;
- Consent records shall be retained for the duration of the processing relationship and for evidentiary purposes thereafter (per Section 8 of the Storage of Data Policy).

8.2 Withdrawal of Consent

- Withdrawal of consent shall be as easy as giving consent;
- Evam shall provide a clear withdrawal channel — including an email / dedicated link to the Data Protection Officer;
- Upon withdrawal, Evam shall cease processing the personal data for the relevant purpose within a reasonable time, unless retention / processing is required under a separate legal basis (e.g., KYC / PMLA retention obligations, ongoing litigation hold);
- Consequences of withdrawal — including impact on continuation of any service / facility — shall be clearly communicated to the Data Principal.

8.3 Consent Manager Framework (effective ~November 2026)

When the Consent Manager framework comes into force under DPDP Rule 4, Evam shall enable Data Principals to give, manage, review, and withdraw consent through registered Consent Managers as well. Evam shall:

- Integrate with Consent Managers through interoperable interfaces;
- Honour consent decisions transmitted through Consent Managers as if directly received from the Data Principal;
- Track and act on consent-modification / withdrawal events received through Consent Managers in near-real-time.

9. Rights of Data Principals

9.1 Right to Access (Section 11)

Data Principals may request:

- Confirmation of whether Evam is processing their personal data;
- A summary of the personal data being processed and the processing activities undertaken;
- The identities of all Data Fiduciaries and Data Processors with whom the personal data has been shared, along with a description of such data.

9.2 Right to Correction & Erasure (Section 12)

Data Principals may request:

- Correction of inaccurate / misleading personal data;
- Completion of incomplete personal data;
- Updating of personal data;
- Erasure of personal data that is no longer necessary for the purpose, subject to legal retention obligations.

9.3 Right of Grievance Redressal (Section 13)

Data Principals shall first approach Evam's grievance channel before approaching the Data Protection Board. Evam's Grievance Officer / DPO shall respond within the timeframes prescribed under the DPDP Rules (currently a maximum of 90 days for grievance resolution under the Rules, with effort to resolve substantially earlier).

9.4 Right to Nominate (Section 14)

Data Principals may nominate another individual to exercise the above rights in the event of death or incapacity. Evam shall facilitate registration of such nominations.

9.5 Process for Exercising Rights

- Channel — email to dpo@evamfinance.com, or postal request to the registered office, or web form on the Evam website;
- Verification of identity of the Data Principal before processing requests;
- Acknowledgement within 3 business days of receipt;
- Substantive response within 30 days (or sooner) — with reasons if the request cannot be fulfilled in full (e.g., due to legal retention obligations);
- Records of all rights-requests and responses maintained per the Storage of Data Policy;
- Where Evam is unable to fulfil the request fully, the Data Principal shall be informed of the reasons and of the right to approach the Data Protection Board.

9.6 Duties of Data Principals (Section 15)

The DPDP Act prescribes certain duties on Data Principals — including not impersonating another person, not suppressing material information, not registering false / frivolous complaints, and providing only authentic information when exercising the right to correction / erasure. Evam may rely on these statutory duties.

10. Children's Data & Data of Persons with Disabilities

- Personal data of children (individuals below 18 years) shall be processed only with verifiable consent of the parent / lawful guardian.
- Tracking, behavioural monitoring, and targeted advertising directed at children shall not be undertaken.
- Personal data of persons with disabilities (where the disability necessitates lawful guardianship) shall be processed with verifiable consent of the lawful guardian.
- Evam shall implement reasonable measures to verify the age of Data Principals and the identity of the consenting parent / guardian, consistent with DPDP Rule 10.

Evam's primary business is wholesale lending to MSMEs / SMEs and corporate borrowers — direct interaction with children as Data Principals is not anticipated in the ordinary course. Nevertheless, the Company shall maintain readiness should any such situation arise (e.g., website visitor, employee dependant).

11. Reasonable Security Safeguards

Evam shall implement reasonable security safeguards proportionate to the risk associated with the personal data processed, including:

- Role-based access control with least-privilege principle, multi-factor authentication on systems holding personal data;
- Periodic access reviews;
- Audit logging of access to personal data and privileged actions;
- Vulnerability assessment and periodic penetration testing (frequency proportionate to risk and Evam's regulatory layer);
- Patch / configuration management;
- Endpoint protection (anti-malware, disk encryption, mobile device management);
- Secure development practices for any in-house applications;
- Vendor security due diligence and contractual obligations on processors;
- Awareness training for employees;
- Physical security of premises and storage areas;
- Incident response plans and periodic drills.

12. Personal Data Breach Notification

Per Rule 7 of the DPDP Rules, 2025, in the event of a personal data breach, Evam shall undertake a two-stage notification:

12.1 Stage 1 — Initial Notification to the Data Protection Board

Without delay upon becoming aware of a breach, the Data Protection Officer shall notify the Data Protection Board of India with:

- A description of the breach (nature, extent, time of occurrence, location);
- Categories and approximate number of Data Principals affected;
- Likely consequences of the breach;
- Measures taken or proposed to address the breach and mitigate harm.

12.2 Stage 2 — Notification to Affected Data Principals

Within 72 hours of the Stage 1 notification, the DPO shall notify each affected Data Principal in plain language with:

- A description of what happened and what personal data was exposed;
- Likely consequences for the Data Principal;
- Protective measures the Data Principal can take;
- Steps Evam has taken to address the breach;
- Contact details of the DPO / Grievance Officer for queries.

12.3 Final Report

Within the timeline prescribed by the DPDP Rules, the DPO shall submit a final report to the Data Protection Board detailing findings, root cause analysis, remediation, and prevention measures.

12.4 Other Reporting Obligations

- Material cyber incidents shall additionally be reported to CERT-In within timelines under the CERT-In Directions of 28 April 2022 (currently 6 hours of noticing);
- Material incidents affecting financial soundness or customer interests shall be reported to RBI under applicable supervisory norms;
- The Audit Committee shall be informed of all material breaches without delay.

13. Data Processor / Vendor Management

- Personal data may be entrusted to a Data Processor only under a written contract.
- The contract shall require the processor to: (a) process personal data only on Evam's documented instructions; (b) implement reasonable security safeguards; (c) maintain confidentiality; (d) assist Evam in responding to Data Principal rights requests; (e) notify Evam of any personal data breach

without undue delay; (f) on termination, return or securely delete personal data; (g) submit to audit by Evam (and RBI, where applicable).

- Processors shall not engage sub-processors without Evam's prior written authorisation.
- Periodic review of processor compliance — minimum annually, with deeper reviews for processors handling Restricted data or large volumes.

14. Cross-Border Transfer of Personal Data

- Evam's default position is to store and process all personal data within India.
- Cross-border transfer / storage of personal data shall be undertaken only in accordance with Section 16 of the DPDP Act, any Government notifications restricting transfers to specified countries / territories, and any sector-specific RBI directions.
- Any proposed cross-border arrangement (e.g., a global cloud / SaaS provider, a foreign Group company performing back-office services) shall require prior CCO / CIO review, with documented assessment of (i) data category, (ii) destination jurisdiction, (iii) safeguards (contractual / technical / legal), and (iv) Evam's residual liability.
- Sector-specific localisation requirements (e.g., RBI Storage of Payment System Data Directions for any payment data) shall be observed.

15. Data Protection Officer / Grievance Officer

The Board shall designate a Data Protection Officer (DPO) — combined for the present with the role of Grievance Officer under the DPDP Act — to:

- Be the single point of contact for Data Principals, the Data Protection Board, and other regulators on personal-data matters;
- Oversee implementation of this Policy and ongoing compliance with the DPDP Act / Rules;
- Handle Data Principal rights-requests and grievances within prescribed timelines;
- Lead breach response, coordinate notifications, and submit reports to the Data Protection Board;
- Maintain the record of processing activities and consent records;
- Conduct periodic training and awareness;
- Liaise with the CCO, CIO, Legal, and business functions.

The DPO shall have appropriate seniority, access to the Board / Audit Committee, and resources to discharge these responsibilities.

15.1 If Designated a Significant Data Fiduciary (Future)

Should Evam be designated a Significant Data Fiduciary (SDF) by the Central Government under Section 10 of the DPDP Act, additional obligations shall apply, including:

- Appointment of a Data Protection Officer based in India who shall report to the Board;
- Appointment of an independent data auditor to conduct periodic audits;
- Annual Data Protection Impact Assessment (DPIA) and independent data protection audit;

- Reporting findings to the Data Protection Board;
- Heightened standards for algorithmic fairness and use of new / sensitive technologies.

Evam shall monitor for SDF designation and adopt voluntary best-practice elements (e.g., periodic DPIA for high-risk processing) in advance.

16. Records of Processing & Documentation

The DPO shall maintain (with input from Data Owners) a Record of Processing Activities (RoPA) covering:

- Categories of personal data processed and Data Principal categories;
- Purposes of processing and legal bases;
- Categories of recipients with whom data is shared (including processors and other Data Fiduciaries);
- Cross-border transfers (if any) and safeguards;
- Retention periods;
- Security measures (high-level description).

The RoPA shall be updated periodically and made available to the Data Protection Board on request.

17. Data Protection Impact Assessment (DPIA)

For new processing activities likely to entail higher risk to Data Principals — including new digital products, AI / ML-driven underwriting, large-scale profiling, automated decision-making, or significant changes in data sharing — Evam shall conduct a DPIA before launch. The DPIA shall:

- Describe the processing and its purposes;
- Assess necessity and proportionality;
- Identify risks to Data Principals (likelihood and severity);
- Specify mitigation measures;
- Be reviewed by the DPO and signed off by the relevant business / IT owner.

18. Website, Cookies & Digital Interactions

- Evam's website (www.evamfinance.com) shall display a Privacy Notice (consumer-facing) and a Cookie Notice, with appropriate consent mechanisms for non-essential cookies / trackers;
- Analytics shall be configured to minimise personal data collected from visitors;
- Marketing communications (where any) shall be sent only with appropriate consent and shall include an unsubscribe option.

19. Retention & Erasure

Personal data retention is governed by the Policy on Storage of Data. Key principles applied in conjunction with the DPDP Act:

- Personal data shall be retained only for as long as needed for the purpose for which it was collected;
- Statutory retention obligations (KYC — 5 years post relationship; books of account — 8 years; specific RBI / PMLA / Companies Act / Income-tax retention) override the right to erasure;
- Pre-erasure notice of at least 48 hours shall be provided to the Data Principal, per DPDP Rule 8;
- Erasure shall be effected across primary, backup, and processor copies;
- Erasure events shall be logged with audit trail.

20. Governance & Responsibilities

Role	Privacy Responsibility
Board of Directors	Approves this Policy; oversees privacy compliance outcomes; reviews material breaches
Audit Committee / Risk Management Committee	Periodic review of privacy risk, breach reports, audit findings
Chief Compliance Officer (CCO)	Owns this Policy; tracks DPDP / RBI developments; coordinates DPO function
Data Protection Officer (DPO) / Grievance Officer	Day-to-day operational ownership; rights-requests; breach response; RoPA; training
Chief Information Officer (CIO)	Technical security safeguards; vendor / cloud arrangements; incident response
Functional Heads (Credit, Operations, HR, Marketing)	Data owners for personal data in their function; ensure local processes comply with this Policy
Legal	Contracts with processors; DPIAs and legal hold; breach legal implications
Internal Audit	Independent assurance — annual audit of privacy compliance
All Employees	Adherence to Policy; report incidents promptly

21. Training & Awareness

- All employees shall complete annual DPDP / privacy training; new joiners shall complete the module before access provisioning;
- Role-specific training for customer-facing teams, IT, HR, Marketing, and Legal;
- Refresher training on material regulatory developments — particularly each DPDP Rules phase commencement (Consent Manager — Nov 2026; substantive obligations — May 2027);
- Awareness communications, posters, and quick-reference guides at offices.

22. Audit & Assurance

- Internal Audit shall conduct an independent privacy audit at least annually;

- Spot reviews by Compliance / DPO across functions;
- If designated SDF, annual independent data protection audit by an external auditor;
- Audit findings reported to the Audit Committee and remediated through documented action plans.

23. Consequences of Non-Compliance

The DPDP Act prescribes monetary penalties up to ₹250 crore per violation, with the actual penalty determined by the Data Protection Board considering the nature of the breach, number of Data Principals affected, Data Fiduciary's history of compliance, and remediation efforts. Indicative penalty heads include:

- Failure to implement reasonable security safeguards — up to ₹250 crore;
- Failure to notify the Board or Data Principals of a breach — up to ₹200 crore;
- Non-compliance with special provisions for children — up to ₹200 crore;
- Failure of additional SDF obligations — up to ₹150 crore.

Employees who breach this Policy may face disciplinary action up to and including termination, in addition to any personal liability under law. Service providers who breach contractual privacy obligations may face penalty, contract termination, and indemnity claims.