

Private & Confidential

## Privacy Policy

Version	Approval Date	Approved By	Review Frequency	Next Review Date
V1	30 <sup>th</sup> May 2024	Board of Directors	Annually	29 <sup>th</sup> May 2025
V2	14 <sup>th</sup> Feb 2026	Board of Directors	Annually	13 <sup>th</sup> Feb 2027

## 1. Introduction

Goyal Associates Limited (“the Company”, “we”, “us”, or “our”) is a Non-Banking Financial Company registered with the Reserve Bank of India and incorporated under the Companies Act, 2013. The Company is engaged in providing financial products and services, including business and personal loans, in accordance with applicable regulatory guidelines.

The Company recognizes that the protection of personal data is essential to maintaining customer trust and fulfilling its legal and regulatory obligations. As a regulated financial institution, we are committed to safeguarding the privacy, confidentiality, and security of personal information entrusted to us by customers, applicants, website users, guarantors, co-applicants, and other stakeholders.

This Privacy Policy explains how the Company collects, uses, processes, stores, discloses, and protects personal information in connection with its lending operations and related services. The Policy applies to information collected through:

- Physical interactions at our offices or through authorized representatives;
- Telephonic or electronic communication;
- Use of our website or digital platforms;
- Digital onboarding processes, including KYC verification;
- Services facilitated through authorized Lending Service Providers (“LSPs”).

Where loans are sourced or facilitated through digital platforms or third-party service providers, Goyal Associates Limited remains the lender of record and retains ultimate responsibility for ensuring that personal data is handled in compliance with applicable laws and regulatory standards.

This Policy has been formulated in alignment with applicable legal and regulatory requirements, including the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, RBI Digital Lending Guidelines, and other directions applicable to Non-Banking Financial Companies. Personal data shall be processed only for lawful purposes, in a fair and transparent manner, and strictly to the extent necessary for providing financial services and complying with regulatory obligations.

By accessing our website, submitting a loan application, or availing our services, you acknowledge that you have read and understood this Privacy Policy and consent to the collection and processing of your personal information in accordance with its terms.

## 2. Legal and Regulatory Framework

This Privacy Policy has been formulated in accordance with the legal and regulatory framework governing data protection and digital lending activities in India. The Company is committed to complying with applicable laws, regulatory directions, and supervisory expectations, including but not limited to:

- The Digital Personal Data Protection Act, 2023;
- The Information Technology Act, 2000 and rules framed thereunder, including provisions relating to sensitive personal data and reasonable security practices;
- The Reserve Bank of India's Digital Lending Guidelines, as amended from time to time;
- The Master Directions and circulars issued by the Reserve Bank of India applicable to Non-Banking Financial Companies;
- RBI guidelines governing outsourcing of financial services and engagement of Lending Service Providers;
- Applicable cybersecurity, information security, and data protection standards.

The Company shall process personal data in a manner consistent with these legal and regulatory requirements. This Privacy Policy shall be reviewed and updated periodically to reflect changes in law, regulatory guidance, technological developments, or operational practices.

## 3. Lender of Record

Goyal Associates Limited shall remain the lender of record for all loans originated in its name, including loans sourced, facilitated, or serviced through authorized Lending Service Providers ("LSPs") or other outsourced partners.

Engagement of an LSP shall not dilute or transfer the Company's regulatory responsibilities. The Company retains full accountability for compliance with applicable laws and regulatory guidelines, including obligations relating to data

protection, information security, fair practices, grievance redressal, and customer protection.

All personal data collected in connection with such loans shall be processed under the authority and supervision of the Company, and in accordance with this Privacy Policy and applicable regulatory requirements.

#### **4. Information We Collect**

The Company collects personal information only to the extent necessary for providing lending services, complying with regulatory obligations, preventing fraud, and fulfilling contractual commitments. Information collected is proportionate to the nature of the product or service applied for.

Certain information may be mandatory for loan processing and regulatory compliance, while other information may be voluntary. Failure to provide mandatory information may affect the Company's ability to process an application.

##### **4.1. Personal Information**

We may collect basic personal details such as:

- Full name
- Date of birth and gender
- Mobile number, email address, and residential address
- Employment details and occupation
- Income information
- Marital status (where relevant for credit assessment)
- Purpose of the loan

##### **4.2. KYC Information**

To comply with regulatory requirements, including RBI KYC Directions, we may collect:

- Permanent Account Number (PAN)
- Aadhaar number, where permitted by law and based on consent
- Passport, Driving License, Voter ID, or other officially valid documents

- Address proof documents
- Photograph and live image or video for identity verification, where applicable

KYC information is collected strictly in accordance with applicable legal and regulatory standards.

#### **4.3. Financial Information**

For credit appraisal and underwriting purposes, we may collect:

- Bank account details
- Income proof documents
- Credit bureau reports and credit scores
- Existing loan and repayment history

#### **4.4. Technical and Device Information**

When customers access our website or digital platforms, we may collect limited technical information necessary for system security, fraud prevention, and operational integrity, including:

- IP address
- Device type and operating system
- Browser type
- Application usage logs
- Session and transactional metadata

The Company does **not** access personal contacts, SMS messages, call logs, photo galleries, or unrelated personal files for lending purposes. Device permissions, where required for KYC verification or fraud prevention, shall be sought transparently and only to the extent necessary.

### **5. Information from Third Parties**

In the course of processing loan applications and servicing credit facilities, the Company may obtain personal or financial information from authorized third parties, where legally permissible and necessary for legitimate business purposes.

Such sources may include:

- Credit Information Companies (credit bureaus) for credit history and score verification;
- Account Aggregators, where consent-based financial data access is utilized;
- KYC verification agencies and authentication service providers;
- Payment service providers and banking partners for transaction verification;
- Government or statutory databases, where access is permitted under applicable law;
- Authorized Lending Service Providers acting on behalf of the Company.

Information obtained from third parties shall be processed strictly in accordance with applicable legal and regulatory requirements. Where required, explicit customer consent shall be obtained prior to accessing such information, particularly in cases involving financial data, Aadhaar authentication, or account aggregation services.

The Company shall ensure that third-party service providers engaged for data processing are bound by appropriate confidentiality, security, and data protection obligations.

## 6. Purpose of Processing

The Company processes personal information only for lawful, specific, and clearly defined purposes that are directly connected with the provision of its financial products and services, compliance with regulatory obligations, and protection of legitimate business interests. Personal data shall be collected and processed in a manner that is fair, transparent, and proportionate to the purpose for which it is obtained.

Personal information may be processed for the following purposes:

- **Identity verification and regulatory compliance:** To conduct Know Your Customer (KYC), Anti-Money Laundering (AML), and related due diligence procedures as required under RBI regulations and applicable law.

- **Credit appraisal and underwriting:** To assess eligibility, determine creditworthiness, evaluate repayment capacity, and make informed lending decisions.
- **Verification and validation:** To verify information provided by applicants through credit bureaus, financial institutions, account aggregators, or other lawful sources.
- **Fraud detection and risk management:** To detect, prevent, and investigate fraudulent activities, identity theft, misrepresentation, or other unlawful conduct, and to safeguard the Company's systems and customers.
- **Loan disbursement and servicing:** To facilitate loan disbursement, manage repayment schedules, generate statements, send transactional alerts, and provide customer support.
- **Regulatory and statutory reporting:** To report information to credit information companies, regulatory authorities, financial intelligence units, or other statutory bodies as mandated under applicable law.
- **Collection and recovery activities:** To manage overdue accounts and undertake lawful recovery measures in accordance with RBI guidelines and contractual terms.
- **Operational improvement and analytics:** To analyze trends, improve service delivery, enhance customer experience, strengthen internal controls, and develop new products or services.
- **Legal enforcement and dispute resolution:** To enforce contractual rights, defend legal claims, comply with court orders, and respond to lawful requests from regulatory or law enforcement authorities.

The Company shall not process personal data for purposes that are incompatible with the purposes stated above without obtaining fresh consent where required under applicable law.

Under no circumstances does the Company sell, lease, or trade personal information to third parties for commercial marketing or unrelated commercial gain.

Processing may also be undertaken where necessary for legitimate business interests of the Company, provided such processing does not override the rights of individuals.

## 7. Consent and Withdrawal

The Company processes personal data on lawful grounds, including consent where required under applicable law. Consent shall be obtained in a free, informed, specific, and unambiguous manner through clear affirmative action.

Where digital onboarding or electronic processes are used, consent shall be captured through explicit mechanisms such as checkboxes, digital acceptance, or electronic signatures. Pre-ticked boxes or implied consent mechanisms shall not be used where express consent is required.

Consent may be obtained for purposes including, but not limited to:

- KYC verification and identity authentication;
- Access to financial information through Account Aggregators;
- Credit bureau checks;
- Electronic communication and documentation;
- Processing of sensitive personal data, where applicable.

The Company shall maintain appropriate records of consent obtained for regulatory and audit purposes.

Customers may withdraw consent for the processing of their personal data at any time, subject to applicable legal, regulatory, and contractual obligations. Withdrawal of consent shall not affect the lawfulness of processing carried out prior to such withdrawal.

Where consent is withdrawn, the Company may be unable to continue providing certain services, including loan processing, servicing, or digital access. In such cases, the Company shall inform the customer of the potential consequences.

Withdrawal requests may be submitted through the contact details provided in this Policy.

## 8. Data Sharing and Disclosure

The Company may share personal information with third parties only to the extent necessary for legitimate business purposes, regulatory compliance, or performance of contractual obligations. Such sharing shall be proportionate, purpose-specific, and subject to appropriate safeguards.

Personal information may be shared with:

- **Authorized Lending Service Providers (LSPs):** for sourcing, onboarding, servicing, or collection activities carried out on behalf of the Company;
- **Credit Information Companies:** for obtaining credit reports and reporting repayment performance in accordance with regulatory requirements;
- **Payment gateways, banking partners, and settlement service providers:** for loan disbursement, repayment processing, and transaction verification;
- **KYC verification agencies and authentication service providers:** for identity verification and regulatory compliance;
- **Collection agencies and recovery partners:** for lawful recovery of dues in accordance with RBI guidelines;
- **Auditors, legal advisors, and compliance professionals:** for internal governance, statutory audit, and regulatory review;
- **Regulatory authorities, law enforcement agencies, courts, or statutory bodies:** where disclosure is required under applicable law or pursuant to lawful orders.

All third parties engaged by the Company are required to adhere to strict confidentiality, data protection, and information security obligations. Where personal data is processed by service providers, such processing shall be governed by written agreements incorporating appropriate safeguards.

The Company shall not share personal information with unrelated third parties for commercial exploitation, unsolicited marketing, or purposes inconsistent with this Privacy Policy.

Personal data shall not be transferred outside India except in accordance with applicable legal and regulatory requirements.

## 9. Data Storage and Retention

All customer data is stored on secure servers located within India. The Company implements appropriate technical and organizational safeguards to ensure that personal information is protected against unauthorized access, alteration, disclosure, or destruction.

Personal data shall be retained only for as long as necessary to:

- Fulfill the purposes for which it was collected;
- Comply with applicable regulatory, statutory, or contractual obligations;
- Meet record-keeping requirements under RBI regulations and other applicable laws;
- Resolve disputes or enforce contractual rights.

Retention periods shall be governed by the Company's Board-approved Record Retention Policy and applicable legal requirements. Upon expiry of the applicable retention period, personal data shall be securely deleted, anonymized, or archived in accordance with internal data management procedures.

The Company does not store biometric data. Where biometric authentication is used through authorized service providers for verification purposes, such data is handled in accordance with applicable legal and regulatory standards.

## 10. Security Safeguards

The Company maintains appropriate technical, administrative, and organizational safeguards to protect personal information against unauthorized access, disclosure, alteration, misuse, or destruction. Security measures are implemented in accordance with applicable regulatory expectations and reasonable security practices.

Such safeguards include, but are not limited to:

- Encryption of sensitive personal and financial information during transmission and storage;
- Role-based access controls to restrict data access on a need-to-know basis;
- Secure authentication mechanisms and password management protocols;
- Network security controls, firewalls, and intrusion detection systems;
- Periodic vulnerability assessments and security audits;
- Logging, monitoring, and incident response mechanisms to detect and address security events;
- Secure data handling practices for employees and authorized service providers.

Access to personal information is strictly limited to authorized personnel who require such access for legitimate business or regulatory purposes. All employees and service providers are required to adhere to confidentiality and data protection obligations.

The Company periodically reviews and updates its security framework to address emerging risks and technological developments.

## 11. Data Breach Response

The Company maintains an internal incident response framework to address data security incidents in a structured and timely manner. In the event of a suspected or confirmed data breach, unauthorized access, or cybersecurity incident affecting personal information, the Company shall promptly take appropriate measures to contain, assess, and mitigate the impact of such incident.

The Company shall:

- Initiate an internal investigation to determine the nature and scope of the incident;
- Take immediate steps to secure affected systems and prevent further unauthorized access;
- Assess the potential impact on customers and stakeholders;
- Implement corrective and preventive measures to reduce recurrence risk.

Where required under applicable law or regulatory directions, the Company shall notify the appropriate authorities, including the Indian Computer Emergency Response Team (CERT-In) and the Reserve Bank of India, within the prescribed timelines.

Where the incident is likely to materially affect customers, the Company shall take appropriate steps to inform affected individuals, in accordance with applicable legal and regulatory requirements.

All incidents shall be documented and reviewed internally to strengthen security controls and compliance oversight.

## 12. Rights of Individuals

Subject to applicable laws and regulatory requirements, individuals whose personal data is processed by the Company (“data principals”) are entitled to exercise certain rights in relation to their personal information.

An individual may request access to the personal data held by the Company and seek confirmation regarding the manner in which such data is being processed. Where personal information is found to be inaccurate, incomplete, or outdated, the individual may request correction or updating of such information.

Individuals may also request erasure of personal data where it is no longer necessary for the purpose for which it was collected, subject to applicable regulatory, contractual, or statutory retention requirements. In cases where data retention is mandated by law or regulatory direction, the Company may retain such information for the prescribed period.

Where processing is based on consent, individuals may withdraw such consent at any time. Withdrawal of consent shall not affect the lawfulness of processing carried out prior to such withdrawal and may impact the Company’s ability to continue providing certain services.

In accordance with applicable data protection laws, an individual may nominate another person to exercise rights under this Policy in the event of death or incapacity.

Requests for exercising any of the above rights may be submitted using the contact details provided in this Privacy Policy. The Company shall respond to such requests within a reasonable period and in accordance with applicable legal requirements.

## 13. Cookies and Website Usage

**13.1. Use of Cookies:** The Company’s website may use cookies and similar tracking technologies to enhance user experience, improve website functionality, and analyze usage patterns. Cookies are small text files stored on a user’s device that help recognize repeat visits and facilitate navigation.

Cookies used by the Company do not collect sensitive financial information such as bank account details, passwords, or loan credentials.

**13.2. Purpose of Cookies:** Cookies may be used for purposes such as:

- Enabling essential website functions;
- Remembering user preferences;
- Improving website performance and user experience;
- Conducting aggregated analytics to understand website usage trends.

Any analytics data collected shall be processed in an anonymized or aggregated manner.

**13.3. Managing Cookies:** Users may control or disable cookies through their browser settings. However, disabling certain cookies may affect the functionality or availability of specific features on the website.

**14. Third-Party Links**

The Company's website may contain links to third-party websites, applications, or services that are not owned or controlled by the Company. Such links are provided for informational or convenience purposes only.

The Company does not endorse, control, or assume responsibility for the privacy practices, content, security, or policies of any external websites. Users are advised to review the privacy policies and terms of use of such third-party websites before providing any personal information.

Accessing third-party websites through links provided on the Company's website is done at the user's own discretion and risk.

**15. Updates to This Policy**

The Company may revise this Privacy Policy from time to time to reflect changes in applicable laws, regulatory guidelines, technological developments, or operational practices.

The updated version of this Policy shall be published on the Company's website and shall become effective from the date specified therein. Where required under applicable law or where material changes are made affecting the manner in which personal data is processed, the Company may provide appropriate notice through its website or other communication channels.

Users are encouraged to periodically review this Privacy Policy to remain informed about how personal information is protected.

## **16. Contact Details**

For any queries, requests, or concerns relating to this Privacy Policy or the processing of personal data, individuals may contact the designated Grievance Redressal & Nodal Officer at the details provided below:

### **Grievance Redressal & Nodal Officer**

Mr. Vuppala Naga Malleswara Rao

Director

401, Phoenix Complex, Waghodia Road, Vadodara – 390019, Gujarat, India

Phone: 8309995691

Email: [grievance@goyalnbfc.in](mailto:grievance@goyalnbfc.in)

The Company shall examine and respond to privacy-related requests or complaints in accordance with applicable legal and regulatory requirements.