Privacy Policy

Introduction

KLM Axiva Finvest Limited ("Company") is a Non-Banking Financial Company (NBFC) registered with the Reserve Bank of India (RBI) as a middle-layer, non-deposit-taking NBFC, under Section 45-IA of the RBI Act, 1934. The Company provides a range of financial services including gold loans, vehicle financing, loans to Micro, Small, and Medium Enterprises (MSMEs), and other related offerings.

The official website of the Company is www.klmaxiva.com, which is owned and operated by KLM Axiva Finvest Limited.

Registered Office: LB Nagar, Mansoorabad, Ranga Reddy, Hyderabad, Telangana – 500074
Corporate Office: KLM Grand Estate, Bypass Road, Edappally, Ernakulum, Kerala – 682024
Corporate Website: www.klmaxiva.com

We are committed to protecting the personal and financial information shared with us. Appropriate measures are in place to prevent unauthorized access, disclosure, or misuse.

By using this website, you agree to the terms of this Privacy Policy. If you do not agree, please refrain from using the website or providing personal information.

Types of Personal Information Collected

Information Provided by You

- Personal details: Name, gender, date of birth, marital status, contact details, and addresses
- KYC data: PAN, KYC status, signature, photograph
- Financial information: Bank account and payment instrument details
- Any other information required for service delivery

Information Collected During Usage

- Transaction data: financial SMS data (excluding unrelated messages)
- Storage and media: uploaded/downloaded documents, images used for transactions
- Device information: model, OS, device ID, mobile network, interaction data
- Aadhaar details: collected directly with consent for e-KYC and onboarding, as permitted by law

Key Data Privacy Principles

This policy aligns with Indian privacy regulations, including the Information Technology Act, IT Rules, and the Aadhaar Act.

Sensitive Personal Data Includes:

- Passwords
- Health or medical information
- Sexual orientation
- Biometric data
- Aadhaar number or Virtual ID
- Any personal data provided in connection with service delivery

Publicly available information or data disclosed under applicable laws (like the Right to Information Act) is not classified as sensitive personal data.

Our Commitment to Privacy

We follow fair, lawful, and transparent practices when handling personal data.

- Users are informed about the use, sharing, and storage of their data.
- Written consent is obtained before collecting sensitive personal data.
- Users have the right to refuse or withdraw consent at any time, except where data sharing is mandated by law.
- Personal data may be shared only with informed consent, or when legally required.
- Aadhaar and identity data are collected solely for authentication and onboarding.

Only the data necessary for legitimate purposes is collected. Access is restricted to authorized personnel only.

Data Security and Confidentiality

We implement robust security controls to protect data, including managerial, technical, operational, and physical safeguards.

- Aadhaar data is collected using secured applications.
- OTPs and biometric data are encrypted.
- Aadhaar numbers and Personal Identity Data (PID) are not retained.
- All Aadhaar-related applications are audited annually.
- Only certified devices and personnel are used for Aadhaar operations.

Access, Correction, and Retention of Data

Users can access and request correction of their data. KLM Axiva Finvest is not responsible for verifying data unless KYC/AML processes apply.

Personal data is retained only for the period required for legal, business, or regulatory purposes, as defined in the company's policies.

Aadhaar authentication logs are retained for two years, archived for five more years, and deleted thereafter unless legally required.

Data may be transferred within India or to countries with adequate data protection, with appropriate consent and contractual safeguards.

Data Sharing and Third-Party Access

Data is shared only under lawful contracts or with the user's explicit consent.
Due diligence is performed to ensure third-party vendors follow strict security and privacy practices.
Biometric and Aadhaar data are shared only with proper encryption, as per applicable laws.
Sharing of sensitive personal data with third parties (other than regulators or under law) requires approval from the Data Privacy Officer.

Marketing and Promotions

Promotional and marketing communications are sent only with prior consent from the customer.

Collecting and Disseminating Personal Information

Before Collecting Data a formal request must be submitted to the Data Privacy Officer outlining:

- Purpose
- Type of data
- Retention period
- Storage methods
- Risks and consequences of misuse or loss
- Aadhaar usage (if applicable)

Sharing of Data:

- Only authorized personnel may access and share PII/SPI.
- Strong controls and monitoring mechanisms are enforced.
- Social media sharing is prohibited.
- Legal approval is required for law enforcement disclosures.

Log Files and Automatically Collected Data

When users visit our website, certain data is automatically recorded, including:

- Browser type and version
- Operating system
- IP address
- Date/time of visit
- Pages visited

This information is anonymized and used to improve user experience and analyze site usage trends.

Purpose of Information Collection

Personal information is collected and used only for:

- Service delivery and transaction processing
- Regulatory and compliance obligations

- Identity verification
- Application processing
- Communication and notifications
- Customer support and grievance handling
- Analytics and service improvement
- Legal compliance

Disclosure of Information

Personal data may be shared with:

- Regulatory bodies (RBI, SEBI, UIDAI, etc.)
- Judicial or law enforcement authorities
- KRAs and banks
- Statutory auditors
- Third-party service providers under confidentiality agreements
- Other entities in case of company restructuring or business transfers

Sensitive personal data is not disclosed or published without consent unless required by law.

Third-Party Service Providers

We may engage vendors and contractors for service delivery, analytics, or operations support. These entities have limited access and must comply with strict confidentiality obligations.

User Consent and Withdrawal

By using our services, you consent to the collection and use of personal data. You may withdraw consent at any time by contacting customer care. However, withdrawal may affect your ability to access certain services.

Communication and Notifications

By using the website or contacting us electronically, you agree to receive communication via email, SMS, or other electronic means. You can opt out of marketing messages where applicable.

Updating Your Information

You may request updates or corrections to your personal data. Any verified inaccuracies will be rectified.

Security Practices

We apply appropriate physical, electronic, and administrative safeguards to protect your data. While we strive to ensure complete security, no system is entirely immune to threats. Users are responsible for safeguarding their login credentials.

Data Privacy Grievances

For any data protection-related queries or grievances, please contact:it@klmaxiva.com
All grievances will be addressed in a time-bound manner.

Third-Party Website Links

This Privacy Policy does not cover external websites linked from our platform. We advise users to review the privacy terms of such websites before sharing any information.

Changes to the Privacy Policy

This policy may be updated periodically. Any changes will be posted on our website. Continued use of our services indicates your acceptance of the revised policy.