CUSTOMER DATA STORAGE POLICY

Finexo Solutions Private Limited

1. INTRODUCTION

The Reserve Bank of India ("**RBI**") *vide* its Master Direction – Reserve Bank of India (Non-Banking Financial Company – Credit Facilities) Directions, 2025 dated November 28, 2025, as updated from time to time, requires Lending Service Provider ("**LSP**") companies to disclose guidelines regarding the storage of customer data including the type of data that can be stored, the length of time for which data can be stored, restrictions on the use of data, data destruction protocol and standards for handling security breach. Finexo Solutions Private Limited ("**Company**", "**Finexo**"," **We**", "**Us**", "**Our**") is an LSP that offers unsecured loans to its customers/ borrowers.

The board of directors of the Company ("**Board**") have formulated and approved the present policy regarding the handling and storage of customer data.

2. OBJECTIVE

This Customer Data Storage Policy ("**Policy**") discloses the practices adopted by the Company for storing information it may receive from Customers using Company's mobile Application or Website (hereinafter, collectively referred to as ("**Digital Lending Platforms**") or from Non-Banking Financial Company ("**NBFC(s)**") for the purposes of providing loans/ credit facilities to the customers/ borrowers ("**Services**").

3. DATA/INFORMATION COLLECTED

Finexo collects and processes Personal Data in order to provide and improve its products and services, administer relationships and interactions with all types of Users, process applications and service requests, prevent and detect fraud and comply with legal and regulatory obligations. The categories below set out the types of information we may collect and the manner in which it is obtained.

A. Information you provide to us

When you interact with Finexo in any capacity, for example, when you visit or use our Website or digital platforms, register for an online account, contact customer support, participate in a survey, engage with us as a shareholder, vendor or in any other business relationship, or otherwise communicate with us, you may provide Personal Data including, but not limited to:

- Identifiers and contact information: name (first/middle/last), email address, telephone/mobile numbers, postal address (temporary/permanent), customer ID / loan account number / application reference number, date of birth, gender, nationality, marital status.

Добавлено примечание ([1]): Finexo is not LSP, it`s DLA

Добавлено примечание ([AKP1R2]): Finexo as a DLA (Digital Lending App) works under the umbrella of the Company Finexo Solutions Pvt ltd, which is an LSP (Lending Service Provider).
As per RBI (NBFC – Credit Facilities) Directions, 2025, an LSP means an agent of an NBFC (including another lender) who carries out one or more of NBFC's digital lending functions, or part thereof, in customer acquisition, services incidental to underwriting and pricing, servicing, monitoring, recovery of specific loan or loan portfolio on behalf of the NBFC in conformity with extant outsourcing guidelines issued by the Reserve Bank.

Добавлено примечание ([2]): This section is in conjunction with the Privacy Policy.

- Government and identity numbers: PAN, CKYC ID, TIN, Aadhaar, passport number, voter ID, driving license number, OCI/NRI details and other government-issued identifiers (to the extent permitted by law).
- Location Data: approximate/coarse device location for serviceability, fraud prevention and onboarding (where applicable).
- SMS Data (with permission): SMS sender/metadata signals may be processed solely for verifying financial position and assessing credit risk for loan eligibility; you may revoke this permission in device settings.
- Media & Documents: we may request specific images/documents for KYC, underwriting, or complaint resolution; we do not access your device storage/media without your action.
- Financial Data: past credit behaviour, income details, loan application/loan account details, repayment history, bank account details and bank statements (only where required for a loan/credit application or servicing).
- Employment and education: employer, designation, employment history, salary/benefits, educational qualifications, professional licences and affiliations.
- Other personal details: visa details, property/vehicle registration details, (only where voluntarily provided or necessary for the product or as permitted by law).
- Authentication and security data: passwords, security questions and answers, one-time passwords and other credentials you provide to access online services.
- Preferences and feedback: marketing preferences, survey responses, contest or promotion entries, complaints and other feedback and preferences you voluntarily provide.

B. Information collected automatically when you use our services

When you visit and use our website, mobile applications or other digital services, we and our service providers may automatically collect technical, usage and device information, including but not limited to:

- Device and connection information: IP address, device identifiers (including MAC address where available), operating system and version, browser type and version, screen resolution, device model and mobile network information.
- Usage and performance data: date and time of visit, pages viewed, links clicked, referrer URL (the site from which you arrived), session duration, number of visits, error logs and other diagnostic data and default language settings.

- Location and geolocation data: approximate or precise geolocation information, where you permit location access on a device.

- Cookies and similar technologies: cookies, pixel tags, local storage and other identifiers used to recognise your device, store preferences, enable functionality, measure usage and support advertising and analytics. Please refer to our Cookie Policy for details on the types of cookies we use and how to manage them.

C. Information from third parties and public sources

We may supplement the information we collect from you with information obtained from third parties and public or commercially available sources, including but not limited to:

- Affiliates and group companies.

- Public databases, credit bureaus, background check providers, government registries, regulators (RBI / relevant financial sector regulators; credit information companies; CKYC/CERSAI (as applicable) and other publicly available sources.

- Social media platforms and any other third-party services you connect to or permit to share data with us.

- Data aggregators and marketing/data enrichment providers.

D. Information created or derived in the course of providing services

We may create or derive additional information about you in the course of providing services, such as:

- Risk assessments and underwriting outcomes.

- Loan/credit product application, account, servicing and transaction records.

- Aggregated or anonymised analytics prepared for statistical, reporting or product development purposes.

- Records of your interactions with us, including video and/or telephone recordings of calls with customer service (where permitted by law and notified to you), emails, messages and other correspondence.

E. Consequences of non-provision or withdrawal of information

The information described above is important for assessing applications, facilitating disbursement/repayment, servicing accounts (where applicable), and compliance, managing risks and complying with legal and regulatory requirements. Where information is necessary, or where consent is the lawful basis, not providing information or withdrawing consent may affect our ability

to provide certain services (including processing a credit/loan application, where applicable) or may require us to suspend/discontinue the relevant service to the extent permitted by law.

4. DATA RETENTION

Retention of information is done as per this policy and in compliance with applicable law/regulatory requirements in India and as mandated in our arrangements with our business partners to provide services to you, unless such consent is withdrawn by you. We take reasonable steps to ensure that User information is available only for so long as is necessary for the purpose for which it is processed, or longer if required under any applicable law, subject to appropriate safeguards. Please note that we ensure that all information collected and stored is secured with adequate technical safeguards. Furthermore, you explicitly consent and agree that we will be entitled to use such data or information freely, without any restrictions other than those set out under applicable law. Once any portion of the User information collected by us is no longer necessary for the purpose for which it is processed, or is no longer required under any applicable law, whichever is later, such User information shall be forthwith deleted, without retention of any copies, save as required by law.

5. RESTRICTION ON USE OF DATA

The Company will not use Customer Data for any purpose other than as set out in this Policy and/or the Company's Privacy Policy available at [kviku.in].

6. DATA DESTRUCTION PROTOCOL

All physical data will be disposed-off by shredding or otherwise making unreadable confidential record. All electronic data will be disposed-off in a responsible manner and in compliance with applicable laws.

We may also retain and use your basic personal information inter alia name, contact number, transactional details, and address details as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements which shall always be in accordance with applicable laws. Subject to this section, we may delete your data upon reasonable written request for the same at any stage. However, you may not be able to use the services after deletion.

7. STANDARDS FOR HANDLING SECURITY BREACH

A. Incident Logging and Tracking

- All suspected or reported security breaches or violations shall be logged and tracked from initiation of the preliminary analysis to determine whether there was a security breach or violation till completion of actions taken.
- Tracking shall begin immediately upon detection and continue until the final Post-Incident Review (PIR) is completed.
- System Logs shall be maintained securely for a rolling period of 180 days within Indian jurisdiction.

B. Reporting to Authorities

- We shall report all cyber data breach incidents (e.g., ransomware, data breaches, unauthorized access) to CERT-In within 6 hours of noticing or being informed of the incident.
- If the breach involves personal data, we shall notify the Data Protection Board of India (DPBI) and all affected individuals without delay as mandated by the DPDP Act, 2023.
- Appropriate contacts with local cyber cells and relevant law enforcement authorities shall be maintained to escalate criminal activities as required.

C. Operational Response Steps

- Move quickly to secure systems, isolate affected segments, and fix vulnerabilities to prevent further spread.
- Rotate all administrative access codes and revoke any compromised credentials immediately.
- Before cleaning or deleting data, preserve system images, memory dumps, and logs for forensic analysis and audit.

8. REVOCATION OF CONSENT TO STORE DATA

You may reach out to us on [support@kviku.in] if you wish to revoke the consent provided here including deletion of your Personal Information and we shall ensure the same. However, once you are onboarded, Information which needs to be stored and/or shared with the Partners and service partners as per regulatory and statutory requirements will be retained by Finexo and the Partners and service partners. Any other data which is not mandatory to be stored and / or transferred will be deleted on your request.

List of Third Parties with whom personal information may be shared is available in Annex – I of Finexo's Privacy Policy, available at [kviku.in].

9. FURTHER INFORMATION

For any further concerns or queries about or related to this Policy, feel free to write to us at [kviku.in].

Добавлено примечание ([3]): Shall we indicate here names of the partners and purpose for transfer/storage and processing of data?

Добавлено примечание ([AKP3R2]): Third parties allowed to collect data are sufficiently disclosed in the Privacy Policy. A reference to the Third Party List in Privacy Policy has been inserted. There is no legal requirement to have a separate list here.

Добавлено примечание ([AKP4]): Inserted reference to third party list in Privacy Policy.