



Avanti Finance Private Limited

Client Privacy Policy

This document was:

Version	Drafted by	Reviewed by	Committee approval date	Board approval and adoption date
Version 1	-	-	NA	June 04, 2021
Version 2	Mr. Nagaraj Subramanya, CISO/ CRO	Mr. Manish Thakkar, COO	NA	March 13, 2023
Version 3	Mr. Manish Thakkar, COO	Mr. Nagaraj Subramanya, CISO/ CRO	NA	August 10, 2023
Version 4	Mr. Manish Thakkar, COO	Mr. Nagaraj Subramanya, CISO/ CRO	October 27, 2023	October 31, 2023
Version 5	Mr. Manish Thakkar, COO	Mr. Nagaraj Subramanya, CISO/ CRO	December 19, 2024	December 19, 2024
Version 6	Ms Sonali Yadav	Mr. Manish Thakkar, COO	June 29, 2026	July 06, 2026

Document Classification: Public

Table of Contents

1. SCOPE AND PURPOSE OF THIS POLICY	3
2. TYPES OF CLIENT INFORMATION COLLECTED	3
3. PURPOSE OF COLLECTION	5
4. DISCLOSURE OF CLIENT INFORMATION	6
5. RETENTION OF CLIENT INFORMATION	6
6. SECURITY PRACTICES AND CONTROL MECHANISM	7
7. Data Principal Rights and Grievance Redressal Mechanism	8
8. POLICY REVIEW UPDATED	9

1. SCOPE AND PURPOSE OF THIS POLICY

- 1.1 In this Client Privacy Policy ("**Policy**"), "**we**" or "**us**" or "**our**" means Avanti Finance Private Limited ("**Company**"), and includes its executive directors, officers, employees, as the context may require.
- 1.2 The scope of this Policy is to ensure the protection of interests of Clients (as defined below) of Company in respect of personal information shared by Clients with Company and provide a broad-level mechanism to regulate the use of such information by the Company.
- 1.3 This Policy has been framed in accordance with the Digital Personal Data Protection Act, 2023 ("DPDP Act"), applicable rules issued thereunder, the Information Technology Act, 2000, RBI directions applicable to Non-Banking Financial Companies (NBFCs), Digital Lending Guidelines, and other applicable laws of India.
- 1.4 Avanti Finance Private Limited acts as a Data Fiduciary under the DPDP Act in relation to personal data processed for the provision of financial products and services. The Company is committed to processing personal data in a lawful, fair, transparent, secure, and accountable manner.
- 1.5 This Policy applies to all persons (natural or juristic) who seek to or have availed loan from Company or from any other financial institution wherein Company acts in the capacity of Data Fiduciary or any other similar capacity ("**Clients**"), and have, in the process, shared their personal information with Company ("**Client Information**").
- 1.6 This Policy delineates various measures that we shall endeavor to take in operationalising our commitment.
- 1.7 The Company processes personal data on the basis of consent provided by the Client and/or other lawful uses permitted under the DPDP Act and applicable regulations. Where consent is relied upon, such consent shall be free, specific, informed, unconditional, unambiguous, and provided through a clear affirmative action.
- 1.8 Clients may withdraw consent at any time, subject to applicable legal and regulatory retention requirements and the consequences of such withdrawal as communicated at the time of obtaining consent.

2. TYPES OF CLIENT INFORMATION COLLECTED

- 2.1 Company may, for the purpose of providing services to Clients, collect the following types of Client Information:

2.1.1 Personal Information: Includes any information collected from the Client that is about his/her family, health, consumption behaviour, personal preferences, attitudes, beliefs or living conditions. It may include the following:

- (i) Name, gender, residential / correspondence address, telephone number, date of birth, marital status, size of family, details of family members, email address or other contact information; and/or
- (ii) PAN, KYC Status, signature and/or photograph.

No biometric data is stored/ collected in the systems, unless allowed under extant statutory guidelines

2.1.2 Financial Information: Includes any information collected from the Client regarding his/her businesses, income, expenses, immoveable assets, moveable assets, loans outstanding, repayment history, guarantors, or collateral Bank account or other payment instrument details; or any other detail which may be required by us for providing services.

2.1.3 Digital Lending & Credit Assessment: The Company may collect and process information necessary for credit assessment, underwriting, fraud prevention, repayment monitoring, collections management, regulatory reporting and servicing of loans, including:

- (a) credit bureau information and credit scores;
- (b) loan application and repayment history;
- (c) bank account information;
- (d) Account Aggregator data obtained with explicit consent;
- (e) mandate registration information including NACH and e-mandates;
- (f) customer due diligence and KYC records;
- (g) device, application and transaction metadata where permitted by law and necessary for fraud prevention or security purposes.

2.2 Client Information is collected only for specified, lawful and legitimate purposes communicated to the Client through privacy notices, consent forms, loan application forms, digital interfaces or other approved communication channels. The Company shall collect only such personal data as is reasonably necessary for the identified purpose and shall not collect excessive or irrelevant information.

2.3 To ensure the accuracy and adequacy of the Client Information, Client shall at all times have the option of reviewing the same by requesting Us in the manner as provided under paragraph 7.2 of this Policy.

2.4 Rights of Data Principals

Subject to applicable law, Clients may exercise the following rights:

2.4.1 the right to obtain information regarding personal data being processed by the Company;

2.4.2 the right to request correction, completion or updating of inaccurate personal data;

2.4.3 the right to request erasure of personal data where retention is no longer required for the purpose for which it was collected, subject to legal and regulatory retention requirements;

2.4.4 the right to withdraw consent where consent is the basis of processing;

2.4.5 the right to nominate another individual to exercise rights in the event of death or incapacity of the Client;

2.4.6 the right to seek grievance redressal in accordance with this Policy and the DPDP Act.

3. PURPOSE OF COLLECTION

3.1 Company collects, retains, and uses Client Information in order to provide financial and other services to Clients. Accordingly, such information is collected for specified business purposes, such as:

3.1.1 to process financial and non-financial transaction request;

3.1.2 to undertake research and analytics for offering or improving Company services;

3.1.3 to check and process Client's applications which may be submitted for availing any financial services;

3.1.4 to share any updates/changes to the services and their terms and conditions with Client;

3.1.5 to take up and investigate any complaints/claims/disputes;

3.1.6 to respond to Client's queries and feedback submitted by Client;

3.1.7 for verification of Client's identity and other parameters; and

3.1.8 to fulfil the requirements of applicable laws / regulations and / or court orders /regulatory directives.

3.1.9 to comply with RBI directions, KYC requirements, anti-money laundering obligations, fraud prevention obligations and regulatory reporting requirements;

- 3.1.10 to perform credit assessment, underwriting, risk management and loan servicing activities;
- 3.1.11 to prevent, detect and investigate fraud, cyber incidents, security breaches and unauthorized activities
- 3.1.12 to comply with contractual obligations with lending partners, co-lenders, service providers and regulators.

4. DISCLOSURE OF CLIENT INFORMATION

- 4.1 Company may disclose Client Information only under the following circumstances
 (List available at <https://www.avantifinance.in/policies#digital-lending-compliance>)
 - 4.1.1 RBI/SEBI/ NSE/ BSE/ MCX /Asset Management Companies of Mutual Funds /Registrar and transfer Agents / Collecting Banks / KYC Registration Agencies and other such agencies, solely for the purpose of processing your transaction requests for serving you better;
 - 4.1.2 To process loans with any other bank/non-banking financial company/other financial institution where Company is acting as agent/banking correspondent or in any similar capacity under a valid contract;
 - 4.1.3 As part of valid contracts with service providers such as Credit bureaus, NSDL etc; as required for the purpose of loan processing and any research agencies/ external consultants, etc.;
 - 4.1.4 Where Client has permitted Company to disclose Client Information to a third party located in India or outside India, Company shall ensure that there is written permission from the Client authorising the disclosure, except where the disclosure is required under law.
 - 4.1.5 The Company may share personal data with Data Processors, service providers, technology partners, collection agencies, credit bureaus, Account Aggregator ecosystem participants, payment service providers, KYC agencies, cloud service providers, auditors, legal advisors and other entities engaged for legitimate business purposes, subject to contractual obligations requiring appropriate confidentiality, security and data protection controls.
 - 4.1.6 Where personal data is shared with third parties acting on behalf of the Company, such parties shall process personal data only in accordance with documented instructions of the Company and shall implement appropriate technical and organisational security safeguards.
 - 4.1.7 The Company shall not sell personal data of Clients. Personal data shall not be disclosed for unrelated marketing purposes without obtaining appropriate consent where required by applicable law.

5. RETENTION OF CLIENT INFORMATION

- 5.1 Company shall not retain or store Client Information for periods longer than is required except when such information may lawfully be used or is otherwise required under any other law for the time being in force or for the purpose of fraud prevention or regulatory compliance. The Company shall retain personal data only for as long as necessary to fulfil the purpose for which it was collected, or as required under applicable laws, regulatory requirements, litigation hold requirements, fraud prevention obligations, audit requirements or contractual commitments.
Typically, Company may retain Client Information for 8 (eight) years. For the first 5 (five) years, such Client Information shall be deemed (for internal purposes) as 'Active Data' and which may be accessed by Company's personnel (on a need-to-know basis) for the purpose of delivery of Company's services, internal records management, permitted disclosure to third parties and/or compliance under law. Thereafter, provided there is no interaction of Company with the relevant Client, it shall be treated (for internal purposes) as 'Passive Data'. Company's personnel may be provided access to Passive Data only upon express written permission of Chief Risk Officer (CRO).
- 5.2 By agreeing to avail the services offered by Company, Client has agreed to the collection and use of Client Information by Company. Client has the right to refuse or withdraw his/her consent to share/disseminate Client Information by contacting the Chief Operating Officer of the Company. However, in the event of your refusal or withdrawal of consent, Client shall not be able to avail any services of Company to the fullest extent.
- 5.3 **Data Destruction Practices:** Subject to law, Company's data destruction practice is set out herein. All computer desktops, laptops, hard drives, and portable media are processed for proper disposal. Paper and hard copy records shall be disposed of in a secure manner. The destruction of data shall address the following:
 - 5.3.1 evaluation and final disposition of sensitive information, hardware, or electronic media regardless of media format or type.
 - 5.3.2 procedures may include shredding, incinerating, or pulp of hard copy materials so that sensitive information cannot be reconstructed.
 - 5.3.3 Electronic Media (physical disks, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard-drives, etc.) shall be disposed of by one of the methods:
 - (i) Overwriting Magnetic Media - Overwriting uses a program to write binary data sector by sector onto the media that requires sanitization;
 - (ii) Degaussing - Degaussing consists of using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state.

6. SECURITY PRACTICES AND CONTROL MECHANISM

- 6.1 Company uses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of Client Information. These include internal reviews of our data collection, storage and processing practices and security measures, such as appropriate encryption and physical security measures to guard against unauthorized access to systems where we store personal data.
- 6.2 Company maintains physical and electronic safeguards to protect Clients' personal and financial information. Company has placed the mechanisms outlined below to ensure information – both physical and electronic data storage, access, retrieval, sharing of data.
- 6.3 The Company implements a risk-based information security program that includes access controls, encryption, authentication controls, vulnerability management, logging and monitoring, incident response procedures, vendor risk management and periodic security reviews in accordance with applicable RBI requirements and industry standards.
- 6.4 The Company may process or permit processing of personal data through service providers located outside India only where such processing is permitted

under applicable law and subject to implementation of appropriate contractual, technical and organisational safeguards. The Company shall comply with any restrictions notified by the Government of India regarding transfer of personal data to specified countries or territories.

Information Management and Data Security

- 6.5 Records may be transferred from and between offices of Company/ third party service providers for record keeping purposes. We ensure that such third-party service providers maintain strict confidentiality (ensuring the same level of confidentiality as maintained by Us) in respect of Client Information.
- 6.6 The database of current Clients and those Clients who do not have any current loan outstanding with Company are properly archived and kept and stored in the same manner as we store data/ documents of our Clients.
- 6.7 All Client data/ records/ documents/ information shall be maintained by Company for such time period as may be required as per applicable laws.

Specific Authorization

- 6.8 Authorized personnel may see data from all the branches, but rights to edit or modify the data are given to select personnel with specific login access.
- 6.9 Client database changes require the Chief Risk Officer, Chief Operating Officer and Chief of Partnerships to authorise / approve the changes.

- 6.10 Each personnel who accesses the database uses an individual username and password.
- 6.11 Whenever an employee logs into the database, their name, the information they query.
- 6.12 Company has a strong back-up system in which it uses a combination of hardcopy and digital backups of Client information. Company's system backs- up all information on our cloud servers located in India periodically.
- 6.13 The Company maintains procedures for identification, assessment, containment, investigation and remediation of personal data breaches. Where required under applicable law, the Company shall notify affected Data Principals and the appropriate regulatory authorities of personal data breaches in accordance with statutory requirements.

7. Data Principal Rights and Grievance Redressal Mechanism

- 7.1 It is the Company's constant endeavour to put the interests of its Clients first and to provide them with financial solutions that are right for them. In keeping with its promise, the Company looks forward to receiving both positive and negative feedback from the Clients on its products and services.

- 7.2 Any discrepancies and grievances related to the processing and use of Client information can be raised to the grievance officer appointed by Company as below:

Nodal Officer

Name: Saurabh Kumar
Designation: Nodal Officer
Email: saurabh.kumar@avantifinance.in

Grievance Officer
Name: Edwin Samuel
Designation: Grievance Officer
Email: edwin.samuel@avantifinance.in

- 7.3 Clients may submit requests relating to access, correction, updating, erasure, withdrawal of consent, nomination, or any privacy-related grievance through the channels specified in this Policy. The Company shall acknowledge and address such requests within timelines prescribed under applicable laws and internal procedures.
- 7.4 Where a Client is dissatisfied with the Company's response to a privacy-related grievance, the Client may seek remedies available under applicable law, including the Digital Personal Data Protection Act, 2023.

The grievances of the Clients will be redressed in the manner provided below:

- (i) Clients can register grievances through email id and toll-free number provided at the Company's branches / Head Office / website and at any other place where the

business of the Company is transacted.

- (ii) After examining the matter, the Company will endeavour to send the Client its response expeditiously and intimate the stakeholder how to escalate the complaint to higher level, if they are not satisfied with the response.
- (iii) Clients have to confirm whether the grievance has been resolved to their satisfaction or not. The grievance will be deemed to be closed, if Client does not respond via toll free number or email.
- (iv) The Company shall also request the Client to provide feedback on the services rendered. This can be done through direct contact by staff or through specific stakeholder satisfaction surveys that may be conducted from time to time.
- (v) A periodical review of the above mechanism at various levels of management would be undertaken by the Company.

8. POLICY REVIEW UPDATED

This document shall be reviewed by the CRO and shall be reviewed at least once a year. Reviews shall also account for any significant business changes and/or any regulatory requirements.