Vridhi FinServ Home Finance Limited (VFHFL)
(Also, Known as Vridhi Home Finance Limited)

Privacy Policy

Version 5.0

Approving Authority	Board of Directors / IT Strategy Committee
Reviewing Authority	Compliance Department
Original Issue Date	5th January 2023
Last Review Date	7th August 2025
Policy Making Body	IT Department
Effective Date	7th August 2025

1. Purpose

The privacy policy ensures that the personal information shared by customers, employees, and vendors with Vridhi Home Finance Limited (VHFL) is protected and not misused. This policy outlines the collection, use, storage, sharing, processing, and protection of such information in accordance with the data privacy regulation. The Board will review the Privacy Policy annually to ensure compliance with legal standards, reflect best practices, and address emerging privacy

2. Scope

This Privacy Policy applies to all personal and confidential information pertaining to employees, customers, and vendors. VHFL collects information during various processes such as loan applications, employment, and vendor engagements.

3. Objective

The objective of this privacy policy is to:

- The objective of the policy is to:
  - Protect data/information that is confidential or private.
  - Ensure effective procedures are in place to prevent the loss of confidential and confidential information.

- This policy applies to
  - All staff and employees of VHF
  - All contractors, suppliers, and other people working on behalf of VHF.
  - All the Customer who has taken a loan from Vridhi Home Finance

4. Definitions

- **Employee**: Individuals employed by VHFL.
- **Vendor:** Third-party service providers engaged by VHFL.
- **Customer:** Members who have taken a loan from Vridhi Home Finance, including those with current loans and those who have dropped out of the program.
- **Information/Data:** Financial and personal data collected from members at the time of loan application.

- **Financial Information:** Data regarding businesses, income, expenses, loans outstanding, repayment history, guarantors, or collateral.
- Sensitive Personal information: Financial information such as bank account details, credit card, debit card details or any payment mode details, Bank or account passwords, Sexual orientation, Biometric details.
- **Personal Information:** Data about family, health, consumption behavior, personal preferences, attitudes, beliefs, or living conditions.
- **Records:** Tangible objects or digital information.
- **Records Management:** Practice of maintaining records from data collection to disposal, including classification, storage, securing, and destruction or archival preservation.
- **Credit Bureau:** Independent organization compiling information from credit grantors and other sources regarding individuals' credit applications and payment behavior.
- **"Data Subject"** refers to the identified or identifiable individual whose Personal Data is processed by the Organisation.
- **"Privacy by Design"** refers to the approach to embedding data protection principles into the design of systems, processes, and technologies from the outset.
- **"Sensitive Personal Data"** refers to special categories of Personal Data which require higher levels of protection. This includes information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (when used for identification), health data, and data concerning a person's sex life or sexual orientation.

5. Principles of Policy Design

The privacy policy ensures that personal information shared by customers is protected and not misused. The following principles are adhered to:

Implementation Details

- **Information Collected at Origination:**
  - The data collection process must be transparent and fair in nature.
  - The data collection must be purpose driven, specified, explicit and lawful.
  - The data must be kept safe and secure. The confidentiality, integrity and availability of the data must be maintained.
  - Ensure the data must be kept accurate, relevant, and not excessive.
  - Only required documents as per KYC norms for identity and address proof will be collected.

- Photos collected for records and identification; written permission required for marketing use.
- Retain for no longer than necessary.

6. Processing of Sensitive/Personal Data

Personal data of customers/employees will be securely stored, in manual or electronic form, and in accordance with the IT Act. In addition, data collected for a specific purpose, product, or service may be stored at VFH with other information.

➢ Data transfer:

VFH shall not disclose an individual's personal/sensitive data outside the VFH office except:

- When VFH has express consent to do so, or in circumstances as explicit consent of the customer, or basis legitimate use between VFH and an individual. The consent obtained shall be free, specific, informed, and unambiguous.
- The Consent notice must be defined as per DPDPA, and DPDP Rules.
- When necessary, to our regulatory bodies and auditors.
- When VFH is required or permitted to do so by law
- Fraud prevention agencies were required.

In case the data is processed/shared with third parties, for any purpose, including cross-selling and cross-marketing, the specific purpose is required to be disclosed in the consent notice.

7. Procedures and Guidelines for Data Privacy

VHF MUST maintain physical, technological, and procedural safeguards and security that comply with the IT Act and privacy law. Below are some of the steps that VFH should take to ensure customer/ employee data privacy:

- Access to sensitive/personal data should be provided strictly based on the need to know, including the access to application, server files, database, Sharedrive etc.
- Backups should be kept in a safe and secure environment.
- Sensitive personal data should be shared with proper authorization as required.
- Logs of the systems should be taken periodically and reviewed to identify the user access to the applications and servers containing sensitive personal data.
- In addition, training procedures should be in place for all employees of VFH, to ensure ambitious standards of data protection.

Action	Principle
Internal	Collecting information: Discretion and adherence to RBI regulations.
	Using customer information: Protection of customer interest from misuse internally.
External	Sharing information with third parties: Any sharing will be with customer's explicit consent.
	In other circumstances, customer information will be shared only if directed by the customer or with written permission.

8. Data Subject Rights

Under the provisions of data privacy, Data Principal, also known as Data Subjects, are additionally entitled to:

- The right to erasure of Personal Data.
- The right to obtain information regarding all data fiduciaries with whom Personal Data has been shared, inclusive of the categories of Personal Data shared, consolidated in one location.
- The right to seek initial redressal of grievances from the data fiduciary, followed by recourse to the Board; if necessary.
- The right to designate an individual to exercise the Data Principal's rights in events of the Data Principal's death or incapacity.
- Review, update, modify, or withdraw consent for Personal Information, and to exercise the above stated rights, Data Subjects should contact the Data Protection Officer **("DPO")** at dpo@vriddhihome.com.

9. Data Classification

- Electronic Records: Data stored in digital formats such as databases, emails, and system-generated files.

- Physical Documents: Data stored in tangible formats such as paper files, printed records, and physical media.

10. Data Disposal Methods

- Electronic Records:
    - Overwriting: Replacing existing data with random characters multiple times to ensure recoverability
    - Degaussing: Using strong magnetic fields to erase data from magnetic media
    - Cryptographic Erasure: Encrypting data and then deleting the encryption key.
    - Physical Destruction: Shredding, crushing, or incinerating electronic media.
- Physical Documents:
    - Shredding: Cutting paper documents into small pieces to prevent reconstruction
    - Incineration: Burning documents to ensure complete destruction
    - Pulverization: Crushing documents into fine particles

11. Data Disposal Monitoring and Confidentiality

- Monitoring: Regular audits and monitoring of data disposal activities to ensure compliance with data privacy regulation.
- Confidentiality: Maintaining confidentiality during the disposal process to prevent unauthorized access
- Verification: Verifying that data has been destroyed completely and maintaining audit trails

12. Incident Response

- Initial Assessment: The IRT will conduct an initial assessment to determine the nature and severity of the incident.
- Containment: Immediate steps will be taken to contain the incident and prevent further damage.
- Investigation: A thorough investigation will be conducted to identify the root cause and impact of the incident.
- Notification: Relevant stakeholders, including affected individuals and regulatory authorities.

13. Data Breach Notification

- Timeliness: Notifications must be made promptly, within the period specified.

- Content: Notifications must include details of the breach, potential impact, and measures taken to mitigate the breach
- Communication Channels: Notifications will be communicated through appropriate channels, such as email, phone, or official website.

14. Roles and Responsibilities

Role	Responsibilities
Senior Management	Senior Management must hold the ultimate responsibility for ensuring adherence to legal requirements concerning data privacy.
Data Protection Officer (DPO)	- Ensure Data privacy compliance - Conduct privacy impact assessments - Handle data protection queries and complaints - Monitor data processing activities - Report data breaches
Incident Response Team	- Identify and assess data breaches - Implement containment and remediation - Document and report incidents - Conduct post-incident reviews
Data Disposal Officer	- Ensure compliance with disposal policies - Authorize and verify data disposal - Maintain disposal records - Monitor disposal activities
IT Security Team	- Implement security measures - Conduct security audits - Monitor data access - Provide technical support
Human Resources (HR)	- Manage employee data - Conduct privacy training - Handle data access requests - Ensure secure storage and disposal of records

Role	Responsibilities
Customer Service Team	- Manage customer data - Inform customers of privacy rights - Handle data access requests - Ensure secure storage and disposal of records
Vendor Management Team	- Ensure vendor compliance - Include data protection clauses in contracts - Monitor vendor activities - Conduct vendor audits
Internal Audit Team	- Conduct privacy audits - Identify non-compliance - Recommend improvements - Ensure corrective actions
All Staffs/ Employees	Employees must understand and adhere to the data privacy policy.

15. Remediation

- Corrective Actions: Steps will be taken to rectify the vulnerabilities that led to the incident.
- Recovery: Efforts will be made to restore affected systems and data to their normal state.
- Documentation: All actions taken during the incident response will be documented for future reference and compliance audits

16. Training Employees, Vendors and Customers in Privacy Policy

Customers are made aware of their privacy rights and responsibilities before receiving loans. Responsibilities include understanding the privacy clause, keeping information updated, informing Vridhi Home Finance of misuse, and keeping financial data confidential.

17. Channel for Complaints

Customers can contact the customer complaint number available on the website to record complaints. Staff who have proven to have breached the privacy policy will face penalties as stated in the HR policy.

- **Promoting Awareness Among Staff**

- Staff will be trained in the privacy policy during induction and refresher training. At the appointment, staff will sign a non-disclosure/confidentiality clause to protect Vridhi Home Finance's and clients' data.

➢ **Monitoring**

- Regular monitoring of policy adherence by employees is conducted by the Internal Audit team during branch audits, with reports for corrective measures.

18. Information Security Mechanisms and Records Management

➢ **Vridhi Home Finance maintains physical and electronic safeguards to protect customer information. Mechanisms include:**

➢ **Records Management and Physical Data Security:** Safe storage of physical files at branches, authorized access, and engagement of third-party service providers under SLAs.

➢ **Information/IT Security Mechanisms:** Controlled data access and modification, individual usernames and passwords, periodic backups on cloud servers, and authorization for database changes.

19.Change Control Record

Version No.	**Change Request by**	**Memorandum of Change**	Approval date
1.0	IT Department	-	5th January 2023
2.0	IT Department	-	21st October 2023
3.0	IT Department	-	29th March 2024
4.0	IT Department	-	5th February 2025
5.0	IT Department	-	7th August 2025