

Hari and Company Investments Madras Private Limited

Data Protection and Privacy Policy

Version 1.0



Project/ Track Name	HCIMPL
Document Name	Data Protection and Privacy Policy
Document No	ISP-12
Revision no	1.0
Object Type	Policy Document

Revision History						
Version	Approval Date	Author	Affected Sections	Level 1 Reviewed By	Level 2 Reviewed By	Approved By
V1	April 01, 2026	InfoSec	All	Prasenjit Datta – CTO	Vineet Sukumar – CEO	Board

Table of Contents

- 1. Purpose 3
- 2. Scope..... 3
- 3. Data Protection Principles 3
 - 3.1. Lawfulness, Fairness, and Transparency 3
 - 3.2. Purpose Limitation 4
 - 3.3. Data Minimization 4
 - 3.4. Accuracy 4
 - 3.5. Storage Limitation 4
 - 3.6. Integrity and Confidentiality..... 4
 - 3.7. Accountability..... 4
- 4. Data Collection and Processing..... 5
- 5. Data Principal Rights 5
 - 5.1 Access to personal data..... 5
 - 5.2 Rectification of inaccurate data..... 5
 - 5.3 Erasure or the "right to be forgotten" 5
 - 5.4 Restricting data processing 5
 - 5.5 Data portability..... 5

5.6	Objection to processing.....	6
5.7	Not being subject to automated decision-making	6
5.8	Withdraw consent	6
5.9	Lodge a complaint	6
6.	Security	6
7.	Data Sharing and Transfer	6
8.	Third-Party Processors	7
9.	Data Privacy Impact Assessments (DPIA)	7
10.	Training and Awareness.....	7
11.	Compliance and Certification.....	7
12.	Review and Revision	7
13.	Contact Information.....	7
14.	Conclusion.....	7
15.	RACI	7

1. Purpose

Hari and Company Investments Madras Private Limited, being a responsible Non-Banking Financial Company (NBFC) registered in India, is committed to protecting and respecting the privacy and security of the personal data of our customers, employees, and stakeholders. This Data Protection Policy outlines our commitment to managing, protecting, and processing personal data in alignment with the ISO 27701:2019, ISO 27001:2022, the Digital Personal Data Protection (DPDP) Act 2023, and the Reserve Bank of India's guidelines on Digital Lending.

2. Scope

This policy applies to all personal data collected, processed, and stored by Hari and Company Investments Madras Private Limited and is applicable to all employees, contractors, and third parties who are entrusted with the processing of this data on our behalf.

3. Data Protection Principles

We strictly adhere to/ shall continue to adhere to the data protection principles below:

3.1. Lawfulness, Fairness, and Transparency

We are committed to processing all personal data in a lawful, fair, and transparent manner. We ensure/ shall ensure that every data processing activity is backed by a legal basis, such as consent or a contractual obligation. Transparency is maintained/ shall continue to be

maintained by providing clear, accessible, and understandable information to Data Principals about how their data is/ would be used, and ensuring their rights can be easily exercised.

Data Principals means and includes the individual to whom the personal data relates and where such individual is: (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes his/her lawful guardian, acting on his/her behalf.

3.2. Purpose Limitation

As part of our business, we act as a data fiduciary, the scope of this policy is to:-

- define and classify the data we need to collect in ordinary course of business,
- lay down process and guidance pertaining to storage of personal data.
- HCIMPL shall collect personal data strictly for identified, explicit, and legitimate purposes.
- Data shall not be further processed in any manner that is incompatible to the purpose for which the same is collected.
- We shall clearly inform the Data Principals of the underlying purpose/s /when the data is collected and to ensure to collect informed consent and understanding.

3.3. Data Minimization

We adhere/ shall continue adhere to the principle of data minimization, ensuring that only data that is necessary for the intended purposes is collected and processed. This minimizes privacy risks and ensures that no excessive data is retained. We shall continually review our processes to uphold this principle.

3.4. Accuracy

Accuracy of personal data is paramount. We have mechanisms in place to ensure that inaccurate or outdated data is amended or deleted promptly. Data Principals are encouraged and facilitated to update their data periodically to ensure it remains accurate and current.

3.5. Storage Limitation

We retain/ shall continue to hold personal data for a limited period, only as long as necessary to fulfill the purposes for which the data was collected or to comply with legal, regulatory or policy requirements. We hereby establish a clear data retention policies and procedures to ensure that data is securely deleted, anonymized, or archived after the retention period.

3.6. Integrity and Confidentiality

Personal data is/ shall be protected by suitable security measures designed to prevent unauthorized access, alteration, disclosure, or destruction. These include technological, organizational, and procedural measures such as encryption, access controls, and staff training to ensure the confidentiality and integrity of data.

3.7. Accountability

We are committed to being accountable for our data protection practices. We have internal policies, procedures, and controls in place to ensure and demonstrate compliance with data

protection principles. These include regular audits, training, and a dedicated data protection officer to oversee compliance.

4. Data Collection and Processing

We commit to:

- Informing individuals regarding their data's collection and processing.
- Only collecting data for specific and legitimate purposes.
- Ensuring data accuracy and updating it as necessary.
- Storing data securely to maintain its confidentiality and abiding by the data localization principles defined by the regulator.

5. Data Principal Rights

We respect Data Principal rights and shall provide adequate support. Both rights of Data Principal and HCIMPL's commitment to abide by the request are detailed herein below :

5.1 Access to personal data

Data Principals have the right to obtain confirmation on whether their personal data is being processed, accessed, or stored. They can request a copy of their data and inquire about the purposes of the processing, categories of personal data involved, and the recipients or categories of recipients to whom the personal data has been or will be disclosed.

5.2 Rectification of inaccurate data

If the personal data we hold is inaccurate or incomplete, Data Principals have the right to have it corrected. We take reasonable steps to ensure that inaccurate data, considering the purposes for which they are processed, are erased or rectified without delay.

5.3 Erasure or the "right to be forgotten"

Data Principals can request the deletion or removal of personal data where there is no compelling reason for its continued processing. This includes situations where the individual withdraws consent, or the data is processed unlawfully. Provided however, the same is not in non-compliance of other applicable regulations and laws.

5.4 Restricting data processing

Individuals have the right to 'block' or suppress the processing of their personal data under certain conditions. When processing is restricted, we are permitted to store personal data but not process it further. Provided however, the same is not in non-compliance of other applicable regulations and laws

5.5 Data portability

Data Principals have the right to obtain and reuse their personal data for their purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way.

5.6 Objection to processing

Data Principals have the right to object to the processing of their personal data based on legitimate interests or the performance of a task in the public interest/exercise of official authority, direct marketing, and processing for purposes of scientific/historical research and statistics.

5.7 Not being subject to automated decision-making

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

5.8 Withdraw consent

Where the processing activities are based on consent, Data Principals have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

5.9 Lodge a complaint

Data Principals have the right to lodge a complaint with a supervisory authority, particularly in the Member State of their habitual residence, place of work, or place of the alleged infringement if the Data Principal considers that the processing of personal data relating to him or her infringes regulations.

At Hari and Company Investments Madras Private Limited, we are committed to enabling these rights and have established internal processes to facilitate the exercise of these rights by Data Principals. For exercising these rights, Data Principals can contact our Data Protection Officer, who will guide through the process and ensure compliance with the legal timeframes.

6. Security

We have instituted security measures to protect personal data, including:

- Assigning the appropriate classification for Personal identification information ("PII" data (any data that is handled shall be classified as PII, sensitive, confidential etc).
- Implementing access controls.
- Encrypting data during transmission and at rest.
- Masking and redacting PII as per requirements to ensure enough access control and protection.
- Regularly monitoring and testing security protocols.
- Establishing incident response and breach notification procedures.

7. Data Sharing and Transfer

In cases of data transfers to our vendor/co-lending partners, we ensure that adequate safeguards, confidentiality, and security measures are in place, in alignment with ISO27701, Indian privacy law, and RBI guidelines, and necessary consent has been obtained from the Data Principal

8. Third-Party Processors

We take steps to ensure that third-party processors adhere to our data protection and privacy requisites.

9. Data Privacy Impact Assessments (DPIA)

DPIAs are conducted for processing operations that pose specific risks to Data Principals' rights and freedoms and to assess the overall privacy impact that HCIMPL may have.

10. Training and Awareness

Employees receive and shall continue to receive periodic training as per the information security and privacy awareness policy, and we foster awareness regarding data privacy and protection.

11. Compliance and Certification

To align with industry standard, we propose to assess and seek certifications, such as ISO 27001:2022 and ISO 27701:2019 and regulations like DPDPA, to ensure compliance.

12. Review and Revision

This policy is subject to annual review and/or updates upon significant changes in data processing activities. including the rules to be laid out under Digital Personal Data Protection Act, 2023.

13. Contact Information

For queries or concerns, you can write to infosec@vivriticapital.com and the team will respond to the same.

14. Conclusion

We are committed to upholding the highest standards of data privacy and security, with continuous improvements to align with legal and regulatory requirements and industry standards.

15. RACI

Policy name	Responsible	Accountable	Consulted	Informed
Data protection and privacy Policy	All PII handlers	Data	InfoSec, Legal, Compliance	MD/CEO

----- End of Document -----