HIGHNESS FINANCE PRIVATE LIMITED

DIGITAL PERSONAL DATA PROTECTION POLICY

(DPDP POLICY)

Board Approved Policy

Applicable to Vehicle Finance, Personal Loans, Business Loans and the Company's Digital Platforms

Policy Number	DPDP/01/2026
Version	1.0
Effective Date	01/04/2026
Approved By	Board of Directors
Review Frequency	At least annually or upon material legal/regulatory change
Policy Owner	Compliance / Legal & Information Security Function
Classification	Internal Policy / Customer Privacy Framework

DOCUMENT CONTROL

Policy Name	Digital Personal Data Protection Policy
Policy Owner	Compliance / Legal Function
Approved Authority	Board of Directors
Applicability	All departments, branches, employees, agents, contractors and relevant service providers
Products Covered	Vehicle Finance, Personal Loans, Business Loans and other lending products
Systems Covered	Website, online loan application systems, LOS/LMS, CRM, accounting systems, e-mail, cloud and other digital systems
Review Cycle	Annual and whenever required by law, regulation, business or technology changes

VERSION HISTORY

Version	Date	Description	Approved By
1.0	01/04/2026	Initial Board-approved policy	Board of Directors

BOARD APPROVAL

This Policy was approved by the Board of Directors of HIGHNESS FINANCE PRIVATE LIMITED at its meeting held on 01/04/2026 and shall remain effective until amended or replaced.

Resolution No.1
Date: 01/04/2026

1. PURPOSE

This Policy est

ablishes the Company's framework for lawful, fair, transparent and secure processing of digital personal data. It is designed for a small NBFC operating its own website and offering vehicle finance, personal loans and business loans.

The Policy is intended to support compliance with the Digital Personal Data Protection Act, 2023 (DPDP Act), the Digital Personal Data Protection Rules, 2025 (DPDP Rules), applicable RBI directions and other applicable laws and regulatory requirements.

2. OBJECTIVES

• protect the privacy and security of individuals whose personal data is processed by the Company;

• ensure data is collected for lawful and specified purposes;

• collect only data reasonably required for the relevant purpose;

• maintain appropriate accuracy, security, access control and retention practices;

• provide mechanisms for applicable Data Principal rights and grievances;

• establish responsibilities for employees and Data Processors; and

• establish a documented response to personal data breaches.

3. SCOPE

This Policy applies to personal data processed digitally by or on behalf of the Company, whether collected through the website, online loan application, branch operations subsequently digitised, e-mail, customer service channels, loan-management systems or third-party service providers.

It covers borrowers, prospective borrowers, co-borrowers, guarantors, directors/partners/proprietors, nominees, website visitors, employees and other individuals whose personal data is lawfully processed in connection with the Company's activities.

4. REGULATORY FRAMEWORK

The Company shall have regard to the DPDP Act, the DPDP Rules, applicable RBI directions and circulars, KYC requirements, Prevention of Money Laundering requirements, credit-information laws, information-security requirements, contractual obligations and other applicable laws.

Where a sector-specific requirement provides a higher or more specific protection or retention requirement, the applicable legal/regulatory requirement shall prevail.

5. KEY DEFINITIONS

Personal Data: Data about an individual who is identifiable by or in relation to such data.

Data Principal: The individual to whom personal data relates.

Data Fiduciary: The person who determines the purpose and means of processing personal data. The Company will generally act as Data Fiduciary for its own processing.

Data Processor: A person who processes personal data on behalf of the Company.

Processing: An operation performed on digital personal data, including collection, storage, use, sharing, retrieval, disclosure or deletion.

6. DATA PROTECTION PRINCIPLES

The Company shall follow the principles of lawful processing, purpose limitation, data minimisation, reasonable accuracy, security safeguards, transparency, accountability and retention only for as long as required for lawful purposes.

Personal data shall not be collected merely because it may be useful in the future. Business functions shall identify the purpose and minimum information required before introducing new data fields or digital collection mechanisms.

7. PERSONAL DATA COLLECTED

The Company may process, as relevant to the product and lawful purpose: name, contact details, address, date of birth, PAN, KYC information, photographs/signatures, employment and income information, bank details, credit information, loan/account details, vehicle information, business information, collateral/security information, guarantor/co-borrower information, communication records, technical/device information and documents submitted for lending and regulatory purposes.

Sensitive or high-risk information shall be accessed only by authorised persons and processed only where necessary and legally permissible.

8. WEBSITE AND DIGITAL CHANNELS

The Company website shall provide an appropriate Privacy Notice at or before the point of collection, as applicable. The notice shall explain the personal data collected, purposes of processing, applicable rights, grievance mechanism and relevant contact details.

Online forms shall avoid collecting information that is not necessary for the stated purpose. Consent interfaces, where required, shall be clear and separate from unrelated terms and conditions. The Company shall maintain reasonable records of consent where consent is the basis for processing.

9. LAWFUL BASIS AND CONSENT

Personal data shall be processed on a lawful basis under the DPDP Act, including consent where required or a permitted legitimate use. Where consent is relied upon, the request shall be clear, specific, informed and capable of being withdrawn through an accessible mechanism.

Withdrawal of consent shall not affect processing lawfully carried out before withdrawal. Where processing is otherwise required or permitted by law, withdrawal shall not require the Company to stop such processing.

10. LENDING AND CREDIT ASSESSMENT

The Company may process personal data for KYC, identity verification, credit assessment, fraud prevention, income verification, credit-information checks, loan sanction, documentation, disbursement, account servicing, monitoring, collections, recovery, enforcement of security, legal proceedings, regulatory reporting and related lawful purposes.

Access to credit and financial information shall be limited to authorised employees and approved service providers on a need-to-know basis.

11. SHARING AND DISCLOSURE

Personal data may be shared where necessary and lawful with regulators and government authorities, credit information companies, KYC/verification agencies, technology and cloud providers, payment/service providers, auditors, legal advisers, collection agencies, dealers/business partners and other Data Processors.

Disclosure shall be limited to the minimum information reasonably required for the relevant purpose. Employees shall not disclose customer data to unauthorised persons.

12. DATA PROCESSORS AND OUTSOURCED SERVICES

Material Data Processors shall be subject to appropriate due diligence and contractual controls covering purpose limitation, confidentiality, security safeguards, access control, breach notification, retention/deletion, subcontracting and cooperation with the Company.

Where practical, contracts shall require processors to notify the Company promptly of suspected personal-data breaches and provide information necessary for regulatory or customer notifications.

13. INFORMATION SECURITY SAFEGUARDS

The Company shall maintain reasonable technical and organisational measures proportionate to its size, operations and risk. Controls may include role-based access, strong authentication, encryption where appropriate, secure transmission, firewalls, endpoint protection, backups, logging, vulnerability management, patching, secure software practices and periodic testing.

Access rights shall be reviewed periodically and removed promptly when an employee or service provider no longer requires access.

14. EMPLOYEE CONFIDENTIALITY

Employees, agents and contractors shall access personal data only for authorised business purposes. They shall not copy, download, forward, photograph or store customer information on personal devices or accounts except where specifically authorised.

Confidentiality obligations shall continue after termination of employment or engagement.

15. DATA PRINCIPAL RIGHTS

Subject to the DPDP Act and applicable Rules, the Company shall provide appropriate mechanisms for Data Principals to exercise applicable rights, including access to information, correction/completion/updating, erasure where applicable, withdrawal of consent where applicable, grievance redressal and nomination.

The Company may require reasonable information for identity verification and shall process requests within applicable legal timelines.

16. GRIEVANCE REDRESSAL

The Company shall designate a contact for privacy/data-protection grievances. Complaints shall be logged, acknowledged, investigated and resolved through an appropriate process. Material or systemic issues shall be escalated to senior management and, where appropriate, the Board.

Contact: Data Protection / Grievance Officer, Anilkumar .G, Head Credit, Highness finance Private limited, KMC14/1139, Ist Floor , Bathel commercial complex, Asramam, Kollam 691002 , E-mail: credit.hfpl@gmail.com, Telephone:+919495653606

17. PERSONAL DATA BREACH MANAGEMENT

Any suspected unauthorised access, disclosure, loss, destruction, alteration, ransomware incident, hacking or other compromise involving personal data shall be reported immediately to the designated internal contact.

The Company shall maintain a documented breach-response process covering identification, containment, assessment, remediation, evidence preservation, internal escalation, documentation and notifications to affected Data Principals and competent authorities where required by law.

18. DATA RETENTION AND DELETION

Personal data shall be retained only for the period necessary for the relevant purpose or as required by law, regulation, contractual rights, audit, accounting, fraud prevention, recovery, litigation or other lawful requirements.

The Company shall maintain a Data Retention Schedule. When retention is no longer required, data shall be securely deleted, destroyed or anonymised, subject to applicable legal holds and statutory requirements.

19. MARKETING AND CUSTOMER COMMUNICATION

Operational communications relating to loan servicing, transactions, repayment, security, collections, statutory requirements and customer support may be sent for lawful purposes.

Promotional communications shall comply with applicable consent, communication-preference and telecommunication requirements. Where consent is required, an appropriate opt-out/withdrawal mechanism shall be provided.

20. COOKIES AND WEBSITE ANALYTICS

The website may use cookies or similar technologies for security, functionality, analytics and service improvement. The Company shall provide appropriate information and, where required, obtain consent or provide user controls in accordance with applicable law.

21. CHILDREN'S DATA

The Company does not ordinarily provide lending products directly to children. Where personal data relating to a child is processed, the Company shall comply with applicable statutory requirements, including requirements concerning verifiable parental/guardian consent and restrictions applicable to children's data.

22. THIRD-PARTY DATA

Where applicants provide personal data relating to guarantors, co-borrowers, directors, partners, employees, nominees or other individuals, the Company may process such data where necessary for lending, verification, contractual, legal or regulatory purposes and in accordance with applicable law.

23. CROSS-BORDER PROCESSING

Where personal data is transferred or processed outside India, the Company shall comply with applicable restrictions, directions or requirements prescribed under the DPDP Act, DPDP Rules or other applicable law.

24. GOVERNANCE AND RESPONSIBILITIES

Board of Directors: overall oversight and approval of this Policy and material changes.

Senior Management: implementation, resources and risk oversight.

Compliance/Legal: regulatory monitoring, policy ownership, grievances and compliance coordination.

IT/Information Security: technical safeguards, access management, logging, security monitoring and incident response.

Credit/Operations: lawful collection and handling of applicant/borrower information.

Collections: lawful and confidential use of customer data for recovery activities.

HR: employee confidentiality and awareness.

Business/Procurement: due diligence and contractual controls for Data Processors.

25. TRAINING AND AWARENESS

Employees handling personal data shall receive periodic awareness/training covering privacy, confidentiality, phishing, secure handling of KYC documents, password security, e-mail/messaging controls and breach reporting.

26. AUDIT AND MONITORING

The Company shall periodically review privacy controls, including website notices, consent mechanisms, access rights, vendor arrangements, retention, deletion, grievances and breach incidents. Material deficiencies shall be assigned corrective actions and tracked to closure.

27. RECORD KEEPING

The Company shall maintain appropriate records relating to notices, consent where applicable, Data Principal requests, grievances, breaches, processor arrangements, training, retention schedules, access reviews and other compliance activities.

28. POLICY REVIEW AND EXCEPTIONS

This Policy shall be reviewed at least annually and whenever there is a material change in law, RBI requirements, technology, products, digital platforms or the Company's risk profile.

Any exception shall be documented, justified, approved by the appropriate authority and reviewed periodically. No exception shall override a mandatory legal or regulatory requirement.

29. BOARD APPROVAL AND EFFECTIVE DATE

This Policy is effective from Ist April 2026 and shall remain in force until amended or replaced by the Board of Directors or an authority duly authorised by the Board, subject to the Company's governance framework.

ANNEXURE I – WEBSITE PRIVACY NOTICE

HIGHNESS FINANCE PRIVATE LIMITED ("Company", "we", "us") respects your privacy. This Privacy Notice explains how we collect and use personal data when you visit our website, submit an enquiry, apply for a loan or use our digital services.

Information we may collect includes name, mobile number, e-mail, address, KYC information, PAN, employment/business information, income and financial information, bank details, credit information, loan information, vehicle/business details, documents and technical information necessary for website security and operation.

We may use information for KYC, identity verification, loan processing, credit assessment, fraud prevention, sanction and disbursement, account servicing, collections, customer support, regulatory compliance, audit, security and other lawful purposes.

We may share information where necessary and lawful with regulators, government authorities, credit information companies, KYC/verification agencies, technology and cloud providers, payment/service providers, auditors, legal advisers, collection agencies, dealers/business partners and other authorised Data Processors.

We maintain reasonable safeguards to protect personal data. You may contact our Data Protection/Grievance Officer for applicable rights and privacy complaints.

Data Protection / Grievance Officer: Name : Anilkumar .G Address: Highness Finance Private Limited, KMC 14/1139, Ist Floor , Bathel Commercial Complex, Asramam, Kollam 691002 E-mail:credit.hfpl@gmail.com , Telephone: +919495653606

ANNEXURE II – DATA RETENTION SCHEDULE (BASE FRAMEWORK)

Data Category	Business Purpose	Indicative Retention	Owner
Loan/KYC records	Customer identification, lending, regulatory/audit	As required by applicable law/RBI/KYC record retention; thereafter subject to legal hold	Compliance/Operations
Loan transaction/account records	Servicing, accounting, audit, recovery	As required by applicable law and Company record-retention schedule	Operations/Finance
Credit assessment records	Underwriting and risk management	As per legal/regulatory and internal retention requirements	Credit
Website enquiries	Customer service/business enquiries	Only as long as required for purpose or lawful business need	Marketing/Operations
Consent records	Demonstrating consent where relied upon	For period necessary to demonstrate compliance and as required by law	Compliance/IT
Breach/incident records	Security and regulatory compliance	As required by law and internal incident-retention requirements	IT/Compliance

ANNEXURE III – DATA BREACH RESPONSE SOP

1. Report: Any employee/vendor detecting a suspected breach shall immediately notify [Incident Contact].

2. Contain: IT shall take reasonable steps to isolate affected systems/accounts and prevent further unauthorised access.

3. Assess: IT and Compliance shall identify the nature of data, affected individuals, likely impact and whether notification is required.

4. Escalate: Material incidents shall be escalated to senior management and other designated governance forums.

5. Notify: Where required, the Company shall make notifications to affected Data Principals and the competent authority within applicable statutory timelines.

6. Remediate: Correct vulnerabilities, reset credentials, recover systems and implement preventive measures.

7. Record: Maintain an incident record, evidence, actions, notifications and closure assessment.