PP Capital
Your Profit. Our Aim.

PAWAN PARMESHWAR CAPITAL PVT LTD

Regd. Office: 187, Dadiseth Agyari Lane, 4th Floor, Singhania Wadi, Mumbai – 400 002
Head Office: 136-138, ORM Wing B Co-Op Premises Soc. Ltd., Ground Floor, Royal Palm, Goregaon East, Mumbai – 400 065
Tel: 022-22014936 / 4961 3718

Member: NSE Code: 00188 | BSE Code: 0550

Information Technology and Data Privacy (DPDP) Policy

Version 1.0

Policy Title	Information Technology and Data Privacy (DPDP) Policy
Version	1.0
Date of Approval	16th October 2025
Effective Date	20th October 2025
Owner	Compliance Department with Information Technology Function
Approving Authority	Board of Directors of Pawan Parmeshwar Capital Pvt Ltd
Next Review Date	Annually, or earlier upon notification of further DPDP Rules or material regulatory change
Replaces	Not applicable — first formal version under the Digital Personal Data Protection Act, 2023

1. Introduction and Purpose

Pawan Parmeshwar Capital Pvt Ltd ("the Company") is a Stock Broker registered with the Securities and Exchange Board of India ("SEBI") and a Trading Member of the National Stock Exchange of India Ltd (NSE Code 00188) and BSE Limited (BSE Code 0550). In the conduct of its business the Company collects, holds and processes a significant volume of personal data of clients, employees, vendors and other persons.

This Information Technology and Data Privacy (DPDP) Policy ("Policy") sets out the framework within which the Company processes personal data and discharges its obligations as a Data Fiduciary, in compliance with:

- The Digital Personal Data Protection Act, 2023 ("DPDP Act") (whose substantive provisions are being progressively brought into force through notifications).

- The DPDP Rules notified or to be notified by the Central Government from time to time. The Company notes that as of the Effective Date, the Draft DPDP Rules issued for public consultation are pending finalisation, and this Policy shall be revised on notification of the final Rules.
- The Information Technology Act, 2000, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules").
- Section 43A of the IT Act, 2000 (compensation for failure to protect data) and Section 79 (intermediary obligations).
- The CERT-In Directions dated April 28, 2022.
- The SEBI Cybersecurity and Cyber Resilience Framework dated August 20, 2024 (as clarified April 30, 2025) ("CSCRF").
- The SEBI Master Circular for Stock Brokers SEBI/HO/MIRSD/MIRSD-PoD/P/CIR/2025/90 dated June 17, 2025.
- All other applicable Indian laws.

2. Scope and Applicability

This Policy applies to:

- All personal data processed by the Company in the course of its business, in whatever form (digital or non-digitised but subsequently digitised), whether collected directly from the Data Principal or obtained from a third party.
- All employees, directors, contractors, consultants and Service Providers of the Company involved in processing personal data.
- All information systems, applications, premises and Service Provider arrangements through which personal data flows.

Categories of Data Principals whose personal data the Company processes include:

- Clients (individuals; natural-person authorised signatories and beneficial owners of non-individual clients).
- Prospective clients (in the course of pre-onboarding interactions and document collection).
- Employees, ex-employees, candidates and their dependants (where covered by benefits).
- Vendors and contractor representatives.
- Visitors to the Company's premises.

- Recipients of the Company's communications (where relevant personal information is processed).

3. Definitions

4. Role of the Company

The Company acts as a Data Fiduciary in respect of personal data that it processes in connection with:

- Client onboarding and KYC, including OVD copies, photographs, signature samples, bank account proof, demat account details, FATCA / CRS information, beneficial-owner information, financial information.
- Operation of client accounts (trading, settlement, statements, communication, complaints).
- Employment of personnel, including identity, address, education, employment-history, payroll, banking, statutory contributions, performance-related and dependant information.
- Engagement of vendors and Service Providers, including their authorised representatives.

In limited situations the Company may act as a Data Processor, for example where it processes data on behalf of an Exchange or Clearing Corporation in respect of routed orders. In such situations the obligations of a Data Processor under the DPDP Act and the underlying contract shall apply.

5. Principles of Processing

Personal data processed by the Company shall be subject to the following principles:

- Lawful purpose: Personal data shall be processed only for a lawful purpose for which the Data Principal has given consent or for which processing is permitted under a Legitimate Use.
- Specified purpose: The purpose of processing shall be specified at the point of collection and shall not be expanded without further consent.
- Purpose limitation: Personal data shall be used only for the purpose for which it was collected, save where further use is permitted by law.
- Data minimisation: Only personal data necessary for the specified purpose shall be collected.
- Accuracy: Reasonable efforts shall be made to ensure that personal data processed is accurate and complete; corrections shall be effected on identification of inaccuracy.
- Storage limitation: Personal data shall be retained only for so long as necessary for the purpose, subject to legal retention obligations (Section 8 of the DPDP Act and the SEBI / PMLA retention obligations).
- Security safeguards: Reasonable security safeguards shall be implemented to protect personal data.
- Accountability: The Company shall be accountable for compliance with these principles.

6. Grounds for Processing

6.1 Consent

Where personal data is processed on the basis of consent (Section 6 of the DPDP Act), the Company shall:

- Provide a notice to the Data Principal before or at the time of collection, in clear and plain language, in English or such Indian language as the Data Principal may select from those offered by the Company.
- The notice shall describe: the personal data being collected; the purpose for which it is being processed; the manner in which the Data Principal may exercise rights under the DPDP Act; and the manner in which a complaint may be made to the Data Protection Board of India ("DPB").
- Obtain free, specific, informed, unconditional and unambiguous consent through a clear affirmative action.

- Maintain a record of the consent obtained, including the version of the notice and the date and means of obtaining consent.
- Provide a clear mechanism for the Data Principal to withdraw consent, as easily as the giving of consent.

6.2 Legitimate Uses (Section 7)

The Company may process personal data without consent only where the processing falls within a Legitimate Use as defined in Section 7 of the DPDP Act, including (without limitation):

- Voluntary provision by the Data Principal for the specified purpose.
- For the performance of any function under any law, including compliance with SEBI requirements, the SEBI (Stock Brokers) Regulations, 1992, PMLA and other applicable laws.
- For compliance with any judgement, decree or order of any court or tribunal.
- For purposes of employment, including prevention of conflicts and protection of the Company's interests.

The basis for processing each category of personal data (consent or Legitimate Use) shall be documented in the Company's Record of Processing (Section 12 below).

6.3 Children's Data

Where the Data Principal is a child (under 18 years of age), processing shall be effected only with verifiable consent of the parent or lawful guardian, and the processing shall not be such as is detrimental to the well-being of the child, in accordance with Section 9 of the DPDP Act. The Company shall not undertake any tracking or behavioural monitoring of children or any targeted advertising directed at children. In the broking context, the Company shall not onboard a minor as a client save through the lawful guardian and only where permitted by the regulatory framework.

6.4 Persons with Disabilities

Where the Data Principal is a person with disability who is unable to give consent themselves, processing shall be effected only with the consent of the lawful guardian, in accordance with Section 9 of the DPDP Act and the Rights of Persons with Disabilities Act, 2016.

7. Notice to Data Principals

The Company shall provide a notice to each Data Principal at the time of collection of personal data, in the format prescribed under the DPDP Rules (as and when notified). The notice shall be:

- Available in English and in such other Indian languages from those listed in the Eighth Schedule of the Constitution as the Company may make available, as selected by the Data Principal.
- In clear and plain language.
- Provided through an itemised format describing the personal data, the purpose and the rights of the Data Principal.

Where the Company has obtained personal data prior to the commencement of the relevant provisions of the DPDP Act, the Company shall issue a notice as soon as reasonably practicable after commencement, in accordance with Section 5(2) of the DPDP Act.

8. Rights of Data Principals

Subject to the DPDP Act and the Rules thereunder, Data Principals have the following rights, which the Company shall give effect to:

8.1 Right to Access

The right to obtain a summary of personal data of the Data Principal that is being processed by the Company, the processing activities undertaken, and the identities of all Data Fiduciaries and Data Processors with whom the personal data has been shared, in respect of personal data processed on the basis of consent (Section 11).

8.2 Right to Correction, Completion, Updating and Erasure

The right to correct inaccurate or misleading personal data, complete incomplete personal data, update personal data, and erase personal data that is no longer necessary for the purpose for which it was processed, subject to legal retention obligations (Section 12).

8.3 Right of Grievance Redressal

The right to have grievances in respect of any act or omission of the Company regarding the discharge of its obligations under the DPDP Act addressed through the Company's grievance redressal mechanism (Section 13).

8.4 Right to Nominate

The right to nominate, in the manner that may be prescribed, another individual who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal (Section 14).

The Company shall publish a clear procedure for the Data Principal to exercise these rights. Requests shall be responded to within the timelines that may be prescribed under the DPDP Rules (as and when notified). Pending such prescription, the Company shall endeavour to

respond within 30 days of receipt of a valid request, subject to verification of the identity of the Data Principal.

9. Duties of Data Principals

Section 15 of the DPDP Act imposes duties on Data Principals, including:

- Compliance with applicable law.
- Not impersonating another person while providing personal data for a specified purpose.
- Not suppressing material information while providing personal data.
- Not registering a false or frivolous grievance or complaint.
- Furnishing only authentic, verifiable information.

Breach of these duties may attract penalty under the DPDP Act.

10. Security Safeguards

The Company shall implement reasonable security safeguards to prevent personal data breach. These safeguards shall be commensurate with the volume and sensitivity of data processed and aligned with the controls in the Cyber Security and Cyber Resilience Policy v1.0. They shall include:

- Access controls under the principle of least privilege and role-based access controls.
- Multi-factor authentication for systems containing personal data.
- Encryption of personal data in transit (TLS 1.2 or higher) and, for Restricted-category personal data, at rest.
- Segregation of personal data from environments that do not require access (e.g., development / test environments shall not use live personal data, except in pseudonymised / masked form).
- Logging of access to personal data and monitoring for anomalies.
- Secure disposal of personal data on retention expiry (secure wiping, physical destruction).
- Backup and recovery arrangements (cross-reference: Business Continuity Plan v1.0).
- Reasonable practices and procedures within the meaning of Section 43A of the IT Act, 2000.

11. Personal Data Breach

11.1 Detection

Personal Data Breach is identified through the mechanisms established under the Cyber Security and Cyber Resilience Policy v1.0 (including logging, monitoring, employee reporting, vendor reporting).

11.2 Response

On identification of a Personal Data Breach, the Company shall:

- Trigger the Incident Response Plan under the Cyber Security Policy v1.0.
- Contain the breach (e.g., isolate affected systems, revoke compromised credentials, block exfiltration).
- Investigate the cause, scope and effect, including the number of Data Principals affected and the categories of personal data involved.
- Take remedial action.

11.3 Notification

On identification of a Personal Data Breach, the Company shall notify:

- The Data Protection Board of India, in the form and within the timeline that may be prescribed under the DPDP Rules (Section 8(6) of the DPDP Act).
- The affected Data Principals, in the form and within the timeline that may be prescribed under the DPDP Rules.
- CERT-In within 6 hours of identification where the breach falls within the categories prescribed under the CERT-In Directions dated April 28, 2022.
- SEBI, NSE, BSE, the Clearing Corporations as required under the CSCRF and the bye-laws / circulars of the Exchanges.
- Other authorities as may be required (FIU-IND if AML-related; insurer / banker on a need-to-know basis to mitigate consequential risk).

The notifications shall include: a description of the breach; the nature and approximate volume of personal data and Data Principals affected; the potential consequences; the measures taken or proposed to mitigate the consequences; and the contact details of the person from whom further information may be obtained. Records of all breach notifications shall be retained.

12. Records of Processing

The Company shall maintain a Record of Processing covering:

- Categories of personal data processed (e.g., identification documents, contact, financial, biometric).
- Categories of Data Principals (clients, employees, vendors).

- Purposes of processing and basis (consent / Legitimate Use under Section 7).
- Recipients of personal data (KRAs, CKYCR, Exchanges, Clearing Corporations, tax authorities, vendors, Service Providers).
- Retention periods.
- Security safeguards applicable.
- Cross-border transfer arrangements, where applicable.

The Record shall be maintained by the Compliance Officer in coordination with the IT function and reviewed at least annually.

13. Cross-Border Transfer of Personal Data

Personal data shall ordinarily be stored within India, in line with the data-localisation principle in the Cyber Security and Cyber Resilience Policy v1.0 and the CSCRF. Where the Company transfers personal data outside India (e.g., to a Service Provider whose processing infrastructure is partly outside India, or for cross-border reporting), such transfer shall be permitted only:

- To countries / territories not restricted by the Central Government under Section 16 of the DPDP Act.
- Subject to contractual safeguards equivalent to the protection afforded under Indian law.
- With the knowledge of the Compliance Officer and (for material transfers) with documented Board approval.

Cross-border transfer arrangements shall be reviewed annually. Where a Service Provider's hosting location is changed during the engagement, the change shall be referred to the Compliance Officer for prior assessment.

14. Data Processor Arrangements

Where the Company engages a Data Processor (e.g., back-office service provider, KYC verification agency, telephony recording vendor, payroll vendor), the engagement shall be governed by the Outsourcing Policy v2.0 and a written contract that includes:

- The categories of personal data and the purposes of processing.
- Restrictions on processing for any other purpose, and restrictions on onward transfer.
- Obligations of confidentiality.
- Security safeguards required (aligned with this Policy and the Cyber Security Policy v1.0).

- Personal Data Breach notification obligations on the Data Processor (within timelines no longer than those binding on the Company under Section 11 above).
- Sub-processor authorisation and notification.
- Cooperation in responding to Data Principal rights requests, audits and regulatory enquiries.
- Return or destruction of personal data on termination.

15. Significant Data Fiduciary Provisions

If the Company is notified by the Central Government as a Significant Data Fiduciary under Section 10 of the DPDP Act, the following additional obligations shall apply (Section 10(2)):

- Appointment of a Data Protection Officer (DPO) based in India.
- Appointment of an independent data auditor to evaluate compliance.
- Undertaking periodic Data Protection Impact Assessment.
- Undertaking periodic audit.
- Such other measures, including those relating to processing of personal data, as may be prescribed.

The Compliance Officer shall monitor any notification by the Central Government that would cause the Company to become a Significant Data Fiduciary, and shall present an implementation plan to the Board within 30 days of such notification.

16. Grievance Redressal

Data Principals may raise grievances regarding the Company's processing of their personal data through the following mechanism:

16.1 Level 1 — Compliance Officer of the Company

Grievances in the first instance shall be addressed to the Compliance Officer of the Company:

- Name: Mr. Rajkumar Pandey
- Designation: Compliance Officer
- Telephone: 022-22014936 / 4961 3718
- Address: Pawan Parmeshwar Capital Pvt Ltd, 136-138, ORM Wing B, Royal Palm, Goregaon East, Mumbai – 400 065.

The Compliance Officer shall acknowledge receipt of the grievance and shall respond within the timeline prescribed under the DPDP Rules (as and when notified); pending such prescription, within 30 days of receipt.

16.2 Level 2 — Data Protection Board of India (DPB)

Where the grievance is not satisfactorily resolved, the Data Principal may approach the Data Protection Board of India in accordance with the procedure prescribed under the DPDP Act and the Rules.

17. Training and Awareness

The Compliance Officer shall ensure that:

- All employees receive annual training on the DPDP Act, the SPDI Rules, this Policy and the related Cyber Security Policy v1.0.
- New joiners receive induction training on data privacy as part of the induction programme.
- Employees in roles handling significant volumes of personal data (KYC, Operations, IT, HR) receive focused training appropriate to their role.
- Updates in the regulatory framework (notification of further DPDP Rules; SEBI / CSCRF advisories on personal data) are communicated to relevant personnel.

18. Records and Retention

Records relating to personal data processing shall be retained as follows:

- KYC and client account records: as required under the PMLA, PML Rules and SEBI Master Circular for Stock Brokers — typically 5 years from cessation of the business relationship or 8 years from the transaction, whichever is longer (cross-reference: KYC Policy v2.0).
- Trading and transaction records: as required under SEBI / Exchange framework — typically 8 years.
- Records of consent and notices: as long as the underlying personal data is retained, plus an additional 3 years.
- Records of grievance and breach notifications: 8 years from the date of resolution / notification.
- Personnel records: as required under labour law and the Companies Act.

On expiry of the retention period, personal data shall be erased or anonymised, save where law requires longer retention or proceedings remain pending.

19. Roles and Responsibilities

- Board of Directors: Approves this Policy; reviews periodic reporting; takes ultimate responsibility for the Company's data privacy compliance; monitors and approves transition to SDF obligations if and when notified.
- Compliance Officer (Mr. Rajkumar Pandey): Owns this Policy; oversees Record of Processing; manages Data Principal rights requests and grievances; coordinates breach notifications; integrates with Cyber Security Policy v1.0 and Outsourcing Policy v2.0; reports to the Board.
- Designated Officer for Cyber Security (DO-CS): Implements security safeguards under Section 10 above; coordinates incident response with the Compliance Officer; supervises cross-border transfer arrangements (technical safeguards).
- Information Technology Function: Implements technical controls, manages access controls, encryption, logging and monitoring; supports breach investigation; manages secure disposal.
- Human Resources Function: Ensures employee-related personal data is handled in accordance with this Policy; manages employee notices and consents; coordinates training.
- All employees: Comply with this Policy; handle personal data only in accordance with assigned responsibilities; recognise and report suspected breaches; cooperate with audit and rights-request handling.

20. Reporting and Review

The Compliance Officer shall present to the Board:

- A quarterly summary of Data Principal rights requests, grievances received, breach incidents (if any), and material changes in Service Provider data-handling arrangements.
- Material developments in the DPDP Act / Rules and the Company's implementation roadmap.
- Material communications from the DPB or other authorities and the response.
- An annual review of the Policy and recommendations for revision.

This Policy shall be reviewed annually and updated on:

- Notification of the DPDP Rules in their final form.
- Any further amendment to the DPDP Act.
- Notification of the Company as a Significant Data Fiduciary.
- Amendments to the CSCRF, the SEBI Master Circular for Stock Brokers, the SPDI Rules, the IT Act or the CERT-In Directions.

- Material change in the Company's processing operations.

21. Monitoring Items — DPDP Rules

The Company notes that, as of the Effective Date, the Draft DPDP Rules issued for public consultation are pending finalisation by the Central Government. The Company shall:

- Monitor the issuance of the final DPDP Rules through the Ministry of Electronics and Information Technology (MeitY) website and the Gazette.
- Within 30 days of notification of the final Rules, conduct a gap-analysis between this Policy and the final Rules and refer required amendments to the Board.
- Update the consent notice, the rights-request procedure, the breach-notification process and the retention schedule in line with the final Rules.
- Re-issue notices to existing Data Principals where required.

Annexure A — Record of Processing (Summary Template)

This is a high-level template. Detailed records are maintained by the Compliance Officer in coordination with the IT and HR functions.

Processing Activity	Categories of Data Principal	Categories of Personal Data	Basis (Consent / Legitimate Use)	Retention
Client onboarding / KYC	Clients; natural-person signatories and beneficial owners of non-individual clients	Identification, address, contact, financial, FATCA/CRS	Consent + Legitimate Use (legal compliance — SEBI / PMLA / KRA / CKYCR)	5/8 years per KYC Policy v2.0
Order receipt and execution	Clients	Trading instructions; voice recordings; electronic messages	Legitimate Use (performance of contract; legal compliance)	Per Order Acceptance Policy v2.0 and Master Circular SB
Settlement and accounts	Clients	Bank account, demat, financial transactions	Legitimate Use (performance of contract; legal compliance)	Per Settlement Running Account Policy v1.0 and Master Circular SB
Communication and complaint handling	Clients; prospects	Contact, communication records	Consent + Legitimate Use	Per Complaint Redressal Policy v2.0
Employment lifecycle	Employees, candidates, dependants	Identification, contact, payroll, performance, statutory, benefits	Legitimate Use (employment under Section 7) + Consent for additional purposes	Per labour law / Companies Act
Vendor engagement	Authorised representatives of vendors	Identification, contact, professional	Legitimate Use (contract performance)	Per vendor contract + statute

Annexure B — Personal Data Breach Notification Register Template

Field	Particulars
Breach Reference Number	
Date and Time of Detection	
Description of Breach	
Categories of Personal Data Affected	
Approximate Number of Data Principals Affected	
Potential Consequences	
Containment / Remediation Measures	
CERT-In Notification (Date / Time)	
DPB Notification (Date / Time)	
Data Principal Notification (Date / Method)	
SEBI / Exchange / Clearing Corp Notification (where applicable)	
Board Notification (Date)	
Root Cause Analysis	
Lessons Learnt / Process Changes	
Closure Date and Sign-off by Compliance Officer	

Board Approval

This Information Technology and Data Privacy (DPDP) Policy (1.0) has been reviewed and approved by the Board of Directors of Pawan Parmeshwar Capital Pvt Ltd at its meeting held on 16th October 2025.

The Board has also recorded, on the same date, the following:

- The Board approves this IT and Data Privacy (DPDP) Policy as the framework for the Company's compliance with the Digital Personal Data Protection Act, 2023, the SPDI Rules under the IT Act, 2000, the CERT-In Directions dated April 28, 2022, the SEBI CSCRF dated August 20, 2024 (as clarified April 30, 2025), the SEBI Master Circular for Stock Brokers dated June 17, 2025, and other applicable Indian law.
- The Board notes that the Draft DPDP Rules issued for public consultation are pending finalisation as of the Effective Date and directs the Compliance Officer to update this Policy within 30 days of notification of the final Rules, as set out in Section 21.
- The Board confirms Mr. Rajkumar Pandey as the Compliance Officer responsible for the privacy framework, in coordination with the Designated Officer for Cyber Security (DO-CS) for technical safeguards.
- The Board directs the Compliance Officer to monitor any notification by the Central Government that would cause the Company to be designated a Significant Data Fiduciary under Section 10 of the DPDP Act, and to bring an implementation plan to the Board within 30 days of any such notification.
- The Board ratifies the data-localisation principle: personal data shall ordinarily be stored within India in accordance with the Cyber Security Policy v1.0 and the Outsourcing Policy v2.0.
- Cross-references to related policies (KYC Policy v2.0, AML/PMLA Policy v2.0, Cyber Security and Cyber Resilience Policy v1.0, Outsourcing Policy v2.0, Business Continuity Plan v1.0, Complaint Redressal Policy v2.0, Investor Charter v1.0, Mobile Phone Usage Policy v1.0, Registers and Records Manual v1.0) are noted.

For PAWAN PARMESHWAR CAPITAL PVT. LTD.

Director / Authorised Signatory

Director / Authorised Signatory

Name: Pawankumar Choudhary

Designation: Designated Director

Date: 16th October 2025

Place: Mumbai

PAWAN PARMESHWAR CAPITAL PVT. LTD. MUMBAI