Savart Privacy Policy

Digital Personal Data Protection Act, 2023 (DPDP) Compliant

Last Updated: 18 March 2026

1. Scope and Applicability

This Privacy Policy explains how Savart ("we", "us", "our") collects, uses, stores, shares, and protects your personal data when you use our websites, mobile applications, products, and services (collectively, the "Services"). This policy is prepared in alignment with India's Digital Personal Data Protection Act, 2023 ("DPDP Act") and the Digital Personal Data Protection Rules, 2025 ("DPDP Rules"). It also reflects sectoral obligations applicable to our regulated activities, including obligations to securities market regulators, exchanges, depositories, and payment systems where relevant.

By accessing or using the Services, you acknowledge that you have read and understood this Privacy Policy. Where required, we will obtain your express consent prior to processing your personal data.

2. Key Definitions

For the purposes of this Privacy Policy:

- Personal Data means any data about an individual who is identifiable by or in relation to such data, processed in digital form (including data collected offline and subsequently digitized).
- 'Data Principal' means the individual to whom the personal data relates ("you").
- 'Data Fiduciary' means any person who determines the purpose and means of processing personal data (Savart).
- 'Data Processor' means any person who processes personal data on behalf of a Data Fiduciary (our vendors/service providers).
- 'Consent Manager' means a person registered with the Data Protection Board of India to act as a single point of contact to enable you to give, manage, review and withdraw consent.

3. Categories of Personal Data We Collect

Depending on how you interact with us, we may collect the following categories of personal data:

- Identity and KYC Data (e.g., name, date of birth, gender, PAN, proof of identity/address, KRA/CKYCR data).

- Contact Data (e.g., mailing address, email address, phone numbers).
- Financial and Transaction Data (e.g., bank account details, payment instrument details, transaction and portfolio information relevant to our advisory/execution services).
- Regulatory and Compliance Data (e.g., FATCA/CRS declarations, risk profiling responses, beneficiary and nominee details).
- Technical and Usage Data (e.g., IP address, device identifiers, app diagnostics, log data, cookies and similar technologies).
- Communications Data (e.g., service requests, call recordings where permitted, chat transcripts, feedback).
- Biometric Data (only if explicitly enabled for specific features, with separate notice and consent).

We collect personal data directly from you, from your authorised representatives, from publicly available sources or regulators where lawful, and automatically through your use of our Services.

- The methods by which we collect your Personal Information include but are not limited to the following:
- By filling a registration form,
- By providing details to our representatives,
- When you register on our website and/or Mobile Application (Mobile App),
- When you provide your Personal Information to us during course of receiving services,
- When you use the features on our website and/or Mobile Application (Mobile App),
- When you provide access to any other website and/or Mobile Application (Mobile App), or by the use of cookies.

4. Purposes of Processing and Legal Basis under DPDP

We process your personal data only for lawful purposes and in a manner that is fair and transparent. Under the DPDP framework, processing is primarily based on your consent or on legitimate uses provided under law. We use your data for:

- Service Delivery: creating and managing your account; risk profiling; providing investment advice/recommendations; executing instructions; customer support.
- Regulatory and Legal Obligations: know-your-customer (KYC), anti-money laundering (AML), tax and securities laws, responses to lawful requests from courts/regulators (including SEBI, stock exchanges, depositories).

- Security and Fraud Prevention: monitoring, detection, and investigation of suspicious activities; safeguarding systems and users.
- Communications: sending essential service messages, transaction alerts, and policy updates.
- Marketing (with your opt-in consent): sending newsletters, offers, insights; conducting surveys and analytics.
- Product Improvement and Research: analytics to improve features, performance, and user experience; anonymised or aggregated statistics that do not identify you individually.
- Mergers/Acquisitions/Restructuring: evaluating or completing corporate transactions as permitted by law.

Where we rely on consent, you may withdraw it at any time using the mechanisms described in Section 10. Certain processing may continue where required by law or for establishment, exercise, or defence of legal claims.

5. Children's Data and Persons with Disabilities

We do not knowingly provide Services directly to children. Where we process personal data of a child (as defined under the DPDP Act) or a person with disability who has a lawful guardian, we obtain verifiable consent from the parent or lawful guardian in the manner prescribed. If we learn that we have collected personal data from a child without such consent, we will promptly delete it.

6. Automated Decision-Making and Profiling

Certain features may use automated processing (including but not limited to algorithms) to generate risk profiles, recommendations, or alerts. We implement measures to safeguard your interests and provide meaningful information about the logic involved to the extent required by law. Where applicable, you may contact us to seek clarification.

7. Cookies and Similar Technologies

We use cookies, SDKs, and similar technologies to enable core functionality, remember preferences, analyse usage to personalise content and marketing. You can manage cookie preferences through in-product controls or your browser settings. Disabling certain cookies may impact site/app functionality.

During your interactions with us, it may happen that we provide/include references to third parties, and/or links and hyperlinks of third-party websites. It may also happen that you include links and hyperlinks of third-party websites. The reference of such third

parties or listing of such third-party external sites (by you or by us) does not imply endorsement of such party or site by us. Such third parties and third-party sites are governed by their own terms and conditions. We do not make any representations regarding the availability and performance of any of the third parties or third-party sites. We are not responsible for the content, terms of use, privacy policies and practices of such third-party websites.

8. Sharing and Disclosure of Personal Data

We share personal data only on a need-to-know basis, under confidentiality and data protection obligations, with:

- Service Providers and Data Processors: IT hosting, cloud infrastructure, analytics, customer support, communications, KYC/AML providers, payment processors.
- Affiliates and Group Entities: for support services and intra-group processing in accordance with this Policy.
- Regulators and Government Authorities: as required by law (e.g., SEBI, stock exchanges, depositories, FIU-IND, tax authorities, law enforcement).
- Professional Advisors: auditors, lawyers, consultants under duty of confidentiality.
- Corporate Transactions: third parties in connection with mergers, acquisitions, financing, or sale of assets, subject to appropriate safeguards.

9. International (Cross-Border) Data Transfers

Where we transfer personal data outside India (for example, to global cloud service providers or support centres), we do so in accordance with the DPDP Act and DPDP Rules, and any notifications of permitted or restricted jurisdictions issued by the Government of India. We ensure appropriate contractual and technical safeguards with our processors, and we will inform you through this Policy or in-product notice if material changes affect such transfers.

10. Your Rights as a Data Principal and How to Exercise Them

Subject to applicable law, you have the following rights over your personal data:

- Correction and Erasure: to request correction, completion, and updating of your personal data.
- Consent Management: to give, manage, or withdraw consent at any time via our in-product settings or through a registered consent manager (when available).
- Grievance Redressal: to lodge a complaint and receive a response within the prescribed timelines.

- Nomination: to nominate another individual to exercise your rights in case of death or incapacity, as provided under the DPDP framework.

To exercise these rights, please use the in-app/web self-service options where available or contact our Grievance Officer using the details in Section 15. We may request information to verify your identity and authority before acting on your request. Some requests may be restricted or denied where allowed by law (for example, to comply with legal obligations or to protect the rights of others).

11. Data Retention and Deletion

We retain personal data only for as long as necessary to fulfil the purposes described in this Policy, to comply with legal, regulatory, accounting, or reporting requirements, and to establish or defend legal claims. We maintain and periodically review retention schedules to ensure compliance.

12. Security Safeguards

We implement reasonable technical and organisational measures appropriate to the risk, including encryption in transit and at rest where feasible, access controls and authentication, role-based access, secure development practices, network security, vulnerability management, employee training, background checks where appropriate, vendor due diligence, periodic audits, and incident response procedures. While we strive to protect your data, no system is completely secure; we continuously improve our controls to address emerging risks. While we will endeavor to take all reasonable and appropriate steps to keep secure any information which we hold about you and prevent unauthorized access, you acknowledge that the internet is not 100% secure and that we cannot provide any absolute assurance regarding the security of your Personal Information. We will not be liable in any way in relation to any breach of security or unintended loss or disclosure of information caused by us in relation to your Personal Information.

13. Personal Data Breaches

In the event of a personal data breach that is likely to result in a significant harm to you, we will notify the Data Protection Board of India and affected data principals in the manner and within the timelines prescribed under the DPDP Rules. We will also take appropriate remedial actions and keep you informed as required.

14. Our Responsibilities When Using Data Processors

Where we engage third-party processors to process personal data on our behalf, we do so under written contracts that require them to implement appropriate security and privacy safeguards, process data only on our documented instructions, and assist us in meeting our obligations under applicable law, including breach notification and deletion upon contract end.

15. Grievance Redressal, Consent Manager, and DPO

If you have questions or concerns about this Policy or our data practices, or if you wish to exercise your rights, please contact:

Grievance Officer	Grievance Officer, Savart
Email	compliance@savart.com
Consent Manager	Mr. Prakash Raju
Data Protection Officer (if designated as Significant Data Fiduciary)	Contact details to be updated if/when designation applies.

16. Significant Data Fiduciary (SDF) Obligations

If Savart is notified/designated as a Significant Data Fiduciary by the Government of India, we will comply with additional obligations including appointment of a Data Protection Officer based in India, conducting periodic data protection impact assessments and audits, and enhanced transparency and accountability measures. We will update this Policy accordingly.

17. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in law, technology, or our operations. When we make material changes, we will notify you by posting the updated Policy on our website/app and, where appropriate, through in-product notifications or email. The "Last Updated" date at the top indicates when this Policy was last revised.

18. Governing Law and Contact

This Policy shall be governed by and construed in accordance with the laws of India. For any unresolved concerns, you may approach the Data Protection Board of India as per the DPDP framework after following our grievance process.

19. Jurisdiction

Any and all disputes arising out of this policy are subject to the jurisdiction of the courts of Hyderabad, Telangana, India.

Appendix: Regulatory Basis and References

• Digital Personal Data Protection Act, 2023 (as notified).

• Digital Personal Data Protection Rules, 2025 (as notified and phased into effect through 2026–2027).

• Sectoral obligations applicable to securities market participants, including circulars and directions issued by relevant regulators and market infrastructure institutions.