AMBIT
Acumen at work
Global Private Client

Data Privacy Policy

Level 1

Ambit Wealth Private Limited

AMBIT
Acumen at work
Global Private Client

Document Information

Document Owner	IS Team
Document Approver	Board Of Directors
Version	1.0
Effective Date	January 08, 2026
Distribution	All employees, contractors as per information classification and access policy With customers after approval from authorized personnel

Revision History

Date	Version	Changes	Made By	Approved By	Approval Date
January 08, 2026	1.0	Initial Version	IS Team	Board of Directors	January 08, 2026

AMBIT
Acumen at work
Global Private Client

Contents

AMBIT
Acumen at work
Global Private Client

1. Introduction

Ambit Wealth Private Limited ("AWPL", "Company", "we", "our", "us") issues this Privacy Policy as a legally binding notice governing the collection, processing, use, storage, protection, and disclosure of Personal Data submitted through our official website and digital interfaces. This Privacy Policy is drafted in accordance with the Information Technology Act, 2000, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), and sector-specific expectations applicable to entities regulated under the Securities and Exchange Board of India (SEBI). This Policy is designed to provide a detailed, transparent, and comprehensive explanation of how your information is handled when you access, browse, submit information to, or otherwise interact with the Company's web-based properties.

We recognise that individuals accessing our digital platforms trust us to safeguard the confidentiality, integrity, and security of any information voluntarily submitted. AWPL is committed to maintaining a privacy posture aligned with the highest standards expected within the Indian financial ecosystem. This includes secure handling of information, adherence to legally mandated retention requirements, deployment of industry-standard cybersecurity controls, and transparent communication regarding data practices. This Privacy Policy outlines the legal and operational principles governing such data handling.

2. Interpretation and definitions

For the purpose of this Privacy Policy, the following terms shall carry the meanings ascribed below. These definitions are intentionally comprehensive to ensure clarity and consistency throughout this Policy and to fully align with the depth and structure of the template provided by the User.

- "Account" refers to any unique identifier, profile, or record created for a User for the purpose of communicating with the Company or accessing any online service modules.
- "Company" refers to Ambit Wealth Private Limited (AWPL), including employees, authorised personnel, and operational units responsible for processing Personal Data.
- "Cookies" refers to small data files placed on your device when you access the Company website, used to store session identifiers, user preferences, analytical information, security markers, or website functionality attributes.
- "Device" refers to any hardware unit capable of accessing the website, including but not limited to computers, laptops, mobile phones, tablets, and smart browsers.
- "Personal Data" refers to any data relating to an identified or identifiable individual, including but not limited to identity details, contact information, regulatory identifiers, technical diagnostics, and digital interaction logs.
- "Sensitive Personal Data or Information (SPDI)" includes, as defined under SPDI Rules, financial information (such as bank account or card details), passwords, biometric identifiers (if ever collected), and any information classified as sensitive under Indian law.
- "Usage Data" refers to automatically collected technical information, including IP addresses, browser metadata, interaction timestamps, device fingerprints, diagnostic logs, clickstream patterns, and system-level telemetry.
- "Service Provider" refers to any third-party vendor, technology partner, infrastructure provider, cybersecurity provider, or operational agency engaged by the Company for the purpose of service enablement, hosting, verification, security monitoring, or platform maintenance.

- "Website" refers to all domains, subdomains, microsites, and digital interfaces operated or controlled by AWPL.
- "User" or "You" refers to any natural person who visits, accesses, interacts with, or submits information through the Company's website.

3. Categories of personal data collected

The Company collects Personal Data strictly in accordance with the principles of necessity, proportionality, and purpose limitation. The categories of Personal Data collected through the Website include but are not limited to the following:

- Identity Information: Name, email address, phone number, and any identity particulars voluntarily submitted.
- Regulatory Information: Information required or submitted in relation to SEBI-mandated suitability assessments or compliance interactions.
- Communication Records: Enquiry forms, contact messages, advisory requests, and communication logs exchanged with the Company.
- Technical & Diagnostic Data: IP addresses, session identifiers, browser metadata, device characteristics, timestamps, crash diagnostics, and security event telemetry.
- Voluntarily Submitted Documents: Any files uploaded for business-related communication (AWPL does not solicit SPDI such as financial details through the website unless explicitly required for a defined regulatory purpose).
- Financial Information (SPDI): Bank account details, account numbers, IFSC codes, and payment instructions collected from employees, interns, vendors, consultants, and service providers for payment processing purposes.

4. Consent for Collection and Processing

By accessing, browsing, or submitting information through AWPL's Website, Users provide their explicit and voluntary consent for the collection, processing, storage, and use of Personal Data in accordance with this Privacy Policy. Such consent constitutes lawful authorisation under the Information Technology Act, 2000 and the SPDI Rules for the Company to process Personal Data for the purposes outlined herein.

Where Personal Data is submitted through enquiry forms, contact submissions, uploads, or any interactive feature on the Website, the User expressly acknowledges and agrees that:

- the information has been provided voluntarily and with full understanding of the purposes of processing.
- AWPL may process the information for service response, communication, compliance, security, and operational requirements.
- AWPL may retain and process the information subject to applicable retention and archival obligations under the AWPL Data Retention and Disposal Policy.
- Personal Data may be shared with authorised service providers strictly for legitimate business or compliance purposes; and
- the User has the right to withdraw consent at any time, subject to legal, regulatory, and operational constraints.

5. Withdrawal of Consent

Users may withdraw consent to the processing of their voluntarily submitted Personal Data by submitting a written request to ***Investor.grievance@ambit.co*** Upon receipt of a valid withdrawal request:

- AWPL will assess the request in accordance with statutory, regulatory, audit, and business continuity requirements.
- Certain data may be retained despite withdrawal, where required under SEBI regulations, internal audit trails, security logs, legal obligations, or the AWPL Data Retention and Disposal Policy.
- Withdrawal of consent does not retroactively invalidate processing lawfully conducted prior to such withdrawal.

Where withdrawal is permitted, AWPL may limit or terminate its ability to respond to or continue usage of the services requested by the User, as certain processing activities may be operationally necessary.

6. Cookies and Tracking Technologies

The Website uses cookies and similar technologies to ensure proper functioning, security, and performance. These technologies help with session management, security monitoring, analytics, and improving user experience. You may disable cookies through your browser settings, but this may affect certain Website features.

7. Use of personal data and Purpose for collection

The Company shall process Personal Data strictly for legitimate, lawful, and operationally necessary purposes. Given the regulated nature of AWPL's business environment, the processing activities undertaken are aligned with obligations derived under the Information Technology Act, 2000, SPDI Rules, and sectoral expectations enforced by SEBI. The following paragraphs provide an exhaustive and explanatory description of the various purposes for which Personal Data may be collected and processed.

Service Delivery and Response Management: Personal Data is used to acknowledge, process, and respond to enquiries submitted through the Website, including advisory requests, general communication, and operational questions. User identity data is used to maintain a record of communication history and ensure accuracy and proper context in subsequent interactions.

Regulatory Compliance and Legal Mandates: As an entity indirectly governed through group-wide SEBI-regulated financial services, the Company processes Personal Data to comply with obligations related to record maintenance, verification, audit trail management, suspicious activity detection, and any lawful order issued by statutory authorities. This may include the verification of data authenticity submitted during communication.

Fraud Detection, Prevention, and Security Assurance: The Company processes technical and diagnostic data to investigate irregularities, detect unauthorized access attempts, mitigate cybersecurity risks, and enforce IP-based restrictions where applicable. Such processing is essential to maintain the confidentiality, integrity, and availability of the Website and its associated systems.

Internal Quality Monitoring and Operational Analytics: AWPL may process anonymised or aggregated technical interaction data for internal performance monitoring, diagnostic reviews, load assessment, and improvement of Website functionality.

This includes monitoring response times, failure points, and navigation patterns to refine platform stability and user experience.

Audit and Risk Governance: Personal Data may be processed to support statutory, regulatory, and internal audit exercises conducted to evaluate compliance posture, operational resilience, and risk controls. Processing may also be undertaken to support the Company's internal governance, reporting obligations, and supervisory requirements.

Customer Support and Feedback Management: Personal Data is processed to document and analyse feedback submitted via the Website, ensure appropriate responses, and track completion of support-related requests. The Company may also maintain internal logs for training and improving service quality.

Security Operations and Incident Management: Technical telemetry, diagnostic logs, and session identifiers may be processed as part of threat hunting, security incident investigations, vulnerability analysis, and breach containment efforts. This includes correlation of logs to detect anomalies.

Business Continuity and Contingency Planning: Personal Data may be processed for backup, recovery, and continuity arrangements designed to ensure uninterrupted functioning of the Website, especially during maintenance cycles, outages, or unforeseen disruptions.

Legal Defence and Dispute Resolution: In the event of any legal claim, dispute, regulatory proceeding, or audit verification, the Company may process Personal Data necessary for establishing, exercising, or defending its legal rights or responding to statutory inquiries.

Payments Processing: Processing payroll, salary disbursements, invoice payments, retainer fees, and vendor payments to employees, contractors, consultants, interns, vendors, and service providers.

8. Retention of personal data

AWPL shall retain Personal Data only for such duration as is necessary for the fulfillment of the purposes outlined in this Policy or as mandated by applicable Indian laws. Retention periods may vary depending on the nature of the interaction, regulatory requirements, and operational needs. The Company adheres to the principles of necessity and proportionality when determining retention timelines and ensures full compliance with the retention, archival, and destruction requirements prescribed under the AWPL Data Retention and Disposal Policy

Regulatory and Statutory Retention: Certain categories of records may be required to be retained for fixed durations under applicable SEBI obligations relevant to financial group entities, Indian tax laws, audit mandates, statutory inspection requirements, and other supervisory frameworks. As mandated under the Data Retention and Disposal Policy, such records shall not be deleted prior to the expiry of the legally prescribed retention period.

Technical and Security Logs: Diagnostic logs, security event telemetry, platform usage data, access logs, and other operational security datasets may be retained to support cybersecurity monitoring, forensic readiness, incident investigation, internal audit, and compliance with reasonable security practices. Their retention parameters follow the log retention and destruction timelines defined under the Data Retention and Disposal Policy.

Deletion Upon Purpose Fulfilment: Personal Data that is no longer required for any legal, regulatory, operational, business continuity, or forensic purpose shall be deleted, anonymised, or securely destroyed in accordance with the approved disposal methods outlined in the Data Retention and Disposal Policy. All destruction activities shall follow the authorised procedures, documentation requirements, and safe disposal standards prescribed in the policy.

9. Transfer of personal data

AWPL does not transfer Personal Data outside India unless explicitly required and lawfully permitted under applicable Indian laws. All Personal Data is processed and stored on secure infrastructure located within India. Any future cross-border transfers, if applicable, shall be carried out only in accordance with legally recognized mechanisms and subject to adequate contractual and organisational safeguards.

Domestic Transfers: Personal Data may be transferred to authorised service providers, infrastructure partners, cybersecurity vendors, or affiliates strictly for lawful business purposes and only under confidentiality obligations.

Security Controls During Transfer: All transfers adhere to encryption, secure transmission protocols, and contractual measures ensuring that receiving entities maintain adequate security practices.

10. Disclosure of personal data

The Company may disclose Personal Data strictly under the circumstances described below. No disclosure shall take place unless such action is legally justified, operationally necessary, or explicitly consented to by the User.

Disclosure to Service Providers: Authorised vendors engaged in hosting, maintenance, analytics, communication support, security monitoring, or operational enablement may receive limited Personal Data strictly required to perform their contractual obligations.

Disclosure to Regulatory Authorities: AWPL may disclose Personal Data upon receipt of lawful requests, notices, directions, or orders from government authorities, enforcement agencies, or regulatory bodies. Such disclosures may be required for inspections, audits, supervisory reviews, or legal proceedings.

Disclosure to Affiliates: Personal Data may be shared with Ambit Group affiliates solely for operational enablement, continuity planning, or legally mandated coordination. All such transfers shall comply with confidentiality obligations.

Legal Requirements: Personal Data may be disclosed for the protection of legal rights, compliance with court orders, enforcement of Company policies, or prevention of unlawful activities.

11. Security of personal data

AWPL implements a multi-layered cybersecurity framework to ensure the confidentiality, integrity, and availability of Personal Data processed through its Website. These measures are aligned with recognised security standards and expectations applicable to entities operating within the Indian financial services ecosystem.

Technical Safeguards: The Company employs encryption (AES-256 for data at rest, TLS 1.2+ for data in transit), network firewalls, Web Application Firewalls (WAF), Intrusion Detection Systems (IDS), endpoint protection mechanisms, and secure hosting infrastructure.

Operational Safeguards: AWPL maintains access control through Role-Based Access Control (RBAC), conducts periodic Vulnerability Assessment and Penetration Testing (VAPT), monitors system events, and operates structured incident response procedures.

Organisational Safeguards: Employees and authorised personnel are subject to confidentiality obligations, role-based permissions, and periodic security awareness initiatives.

Continuous Monitoring: Logs, events, and telemetry are continuously analysed to detect anomalies, mitigate security threats, and ensure prompt containment of potential incidents.

12. Children's privacy

AWPL may onboard minor clients or collect minor nominee information where permitted by applicable regulations, subject to explicit consent and authorized representation by the parent/legal guardian. AWPL does not knowingly collect data directly submitted by minors without parental/guardian authorization.

13. Access and correction of personal data

Users are entitled to request access to the Personal Data that AWPL holds about them and may also seek correction of any information that is inaccurate, incomplete, or outdated. Such rights arise under the Information Technology Act, 2000 and the SPDI Rules, which permit individuals to review the information they have voluntarily provided and request rectification where necessary.

Users may exercise these rights by submitting a written request to AWPL's Grievance Redressal Officer. For verification and security purposes, the request must include the User's full name, registered email address or mobile number, and a clear description of the specific information for which access or correction is sought.

All requests should be directed to:

Email: ***Investor.grievance@ambit.co***

Upon receipt of a valid request, AWPL shall review the submission, initiate identity verification, and provide the User with access to their Personal Data or carry out the requested corrections, unless restricted by legal, regulatory, or operational constraints. Certain records may not be modifiable where retention in original form is mandated under SEBI regulations, statutory audit requirements, or applicable Indian laws.

AWPL endeavours to respond to all access and correction requests within a reasonable timeframe and in accordance with applicable legal timelines.

14. Data deletion procedure

Users may request deletion of their Personal Data submitted through AWPL's Website, subject always to AWPL's statutory, regulatory, contractual, audit, archival, litigation-hold, and information-governance obligations. The deletion workflow implemented by AWPL is aligned with the AWPL Data Retention and Disposal Policy and follows the principles of mandatory retention, secure archiving, periodic review, and controlled destruction required under the policy.

14.1. Submission of Request

Users must submit a written deletion request to AWPL's Grievance Redressal Officer at ***Investor.grievance@ambit.co***. The request must include the User's full name, registered mobile number or email ID, and a clear description of the Personal Data for which deletion is sought. Proof of identity may be requested.

14.2. Identity Verification

AWPL will validate the identity of the requestor using the contact information on record to prevent unauthorized deletion attempts.

14.3. Mandatory Retention Assessment

Before any deletion action is initiated, AWPL will assess the data against the retention, archival, and preservation requirements defined in the AWPL Data Retention and Disposal Policy. Deletion may not be permitted where:

- The data is within an active retention period defined in the Retention Schedule.
- The data is required for SEBI regulatory record-keeping.
- The data is part of mandatory audit trails, security logs, or forensic readiness datasets.
- The data falls under an ongoing Litigation Hold.
- The disposal period has not yet matured as per the applicable data category.
- The data is required for fraud prevention, investigations, compliance, or operational business continuity.

14.4. Regulatory and Business Exemptions

AWPL may partially fulfil or fully decline a deletion request where retention is mandated under Indian law, SEBI guidelines, audit requirements, contractual obligations, or internal governance controls. Users shall receive a written explanation whenever a deletion request cannot be fulfilled fully.

14.5. Deletion of Eligible Data

Where deletion is permissible, AWPL shall securely execute one or more of the approved disposal methods defined in the Data Retention and Disposal Policy:

- Secure digital erasure
- Cryptographic erasure
- Anonymisation
- Logical deletion with access revocation pending systematic destruction
- Destruction of physical media using approved techniques such as shredding or secure disposal bins

All destruction activities shall be logged and carried out only by authorised personnel as mandated by policy.

14.6. Timeframe for Completion

AWPL will typically process deletion requests within 15–30 working days unless delays occur due to investigation requirements, litigation holds, regulatory constraints, or dependencies involving third-party processors.

14.7. Confirmation to the User

Upon completion, AWPL will notify the User in writing specifying whether the request was completed fully or partially, the categories of data deleted, and the lawful basis for retaining any non-deletable data.

15. User rights under Indian law

Users interacting with the Website are entitled to exercise the following rights in accordance with the IT Act, 2000 and SPDI Rules. These rights apply solely to information collected through AWPL's Website and do not extend to records governed under separate regulatory frameworks:

Right to Access: Users may request confirmation on whether their Personal Data is being processed and may seek a summary of such data, subject to verification requirements.

Right to Correction: Users may request rectification of inaccurate, incomplete, or outdated Personal Data.

Right to Withdraw Consent: Users may withdraw consent for processing of Personal Data that was voluntarily submitted. However, withdrawal shall not impact processing conducted under legal obligations.

Right to Restrict Processing: Users may request temporary restriction of processing where accuracy is contested or processing is believed to be unauthorized—pending internal review.

Right to Know Purpose of Processing: Users may request detailed explanation of how and why their data is being processed by AWPL.

Right to Know Categories of Disclosure: Users may request a list of categories of third parties to whom data has been disclosed, if applicable.

Right to File a Complaint: Users may escalate unresolved grievances to the Grievance Redressal Officer for independent review.

Regulatory Exceptions: These rights are subject to limitations where retention or disclosure is mandated under Indian law, SEBI guidelines, tax, audit, or enforcement requirements.

16. Grievance Redressal Officer

In accordance with the Information Technology Act, 2000 and SPDI Rules, AWPL appoints a Grievance Redressal Officer ("GRO") to address concerns relating to the processing of Personal Data. Users may direct complaints, requests, or inquiries to:

Grievance Redressal Officer

Ambit Wealth Private Limited (AWPL)

Email: ***Investor.grievance@ambit.co***

The GRO shall acknowledge complaints within a reasonable timeframe and endeavor to resolve them in accordance with statutory timelines and internal escalation procedures.

17. Policy and Procedure Reference

This Privacy Policy shall be read in conjunction with the following AWPL policies and procedures:

- Information Security Policy and Cybersecurity Policy
- Data Retention and Disposal Policy

These documents collectively define AWPL's governance, security, data-handling, and compliance expectations.

18. Review and Maintenance

This Privacy Policy shall be reviewed annually, or earlier if there are:

- Significant regulatory changes,
- Material updates to AWPL's technology stack or security practices,
- Changes to data-processing activities, or
- New internal governance requirements.

All revisions must be reviewed and approved by the Chief Information Security Officer (CISO) or an authorised designate prior to publication.