Data Privacy policy

Document Number:	RAB-ISMS-D100
Document Version:	1.0
Last Revision Date:	01-Sep-2026
Issue Date:	01-09-2026
Next Review Date:	31-Aug-2027
Classification:	Public

COPYRIGHT © RABWIN ● ALL RIGHTS RESERVED

ATTENTION: This document is used exclusively within RABWIN. Part of the document or all of it can be photocopied or printed for internal use only. A written authorization by the Information Security Manager is required before this document or part of it can become available in any way or form outside RABWIN.

DOCUMENT CONTROL

Approvals

Version	Date	Name and Designation	Approval
1.0	01-09-2026	P BALAKRISHNAN	ISSC Chairman

Approver: refers to the individual(s) with the authority to approve the document such that it can be issued and implemented.

TABLE OF CONTENTS

This policy is drafted with reference to two Indian legal frameworks: the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules"), issued under Section 43A of the Information Technology Act, 2000; and the Digital Personal Data Protection Act, 2023 ("DPDPA"), read with the Digital Personal Data Protection Rules, 2025 ("DPDP Rules").

1. PURPOSE

This policy sets out how RABWIN INDUSTRIES PRIVATE LIMITED collects, uses, discloses, stores, secures, and disposes of personal information and sensitive personal data or information belonging to employees, customers, vendors, and other individuals ("Data Principals" / "Providers of Information"), in compliance with the SPDI Rules, 2011 and the DPDPA, 2023 (together with the DPDP Rules, 2025).

2. Scope

This policy applies to:

- All personal data and Sensitive Personal Data or Information (SPDI) collected, processed, stored, or transmitted by the Organization, in physical or digital form.
- All employees, contractors, third-party vendors, and data processors who handle such data on behalf of the Organization.
- All business units, systems, and locations of the Organization, including cross-border data transfers.

3. Key Definitions

Term	Meaning
Personal Information	Any information that relates to a natural person, which, either directly or indirectly, in combination with other information, is capable of identifying that person (SPDI Rules).
Sensitive Personal Data or Information (SPDI)	Passwords; financial information (bank account, card, or other payment instrument details); physical, physiological, and mental health condition; sexual orientation; medical records and history; biometric information; and any information received for processing under lawful contract (SPDI Rule 3).

Digital Personal Data	Personal data in digital form, or non-digital personal data digitized subsequently (DPDPA, Section 2).
Data Principal	The individual to whom the personal data relates (and, for children, the parent/lawful guardian; for persons with disability, the lawful guardian) (DPDPA, Section 2).
Data Fiduciary	Any person who, alone or with others, determines the purpose and means of processing personal data (DPDPA, Section 2).
Significant Data Fiduciary (SDF)	A Data Fiduciary notified as such by the Central Government based on volume/sensitivity of data, risk to Data Principals, and other factors (DPDPA, Section 10).
Data Processor	Any person who processes personal data on behalf of a Data Fiduciary (DPDPA, Section 2).
Consent Manager	A registered entity that enables a Data Principal to give, manage, review, and withdraw consent through an accessible, transparent platform (DPDPA, Section 2; DPDP Rule 4).
Body Corporate	Any company, firm, sole proprietorship, or other association of individuals engaged in commercial or professional activities (IT Act, Section 43A).

4. Regulatory Framework — What Each Law Covers

4.1 SPDI Rules, 2011 (Section 43A, IT Act, 2000)

- Applies to body corporates that collect, receive, possess, store, deal with, or handle SPDI in the course of business.
- Governs only Sensitive Personal Data or Information, not all personal information.
- Mandates reasonable security practices; failure resulting in wrongful loss/gain attracts civil liability for compensation under Section 43A.

4.2 DPDPA, 2023 and DPDP Rules, 2025

- Applies to processing of digital personal data within India, and processing outside India where goods/services are offered to Data Principals in India.
- Notified via Gazette Notification G.S.R. 846(E) dated 13 November 2025, with phased commencement (see table below).
- Covers all personal data, not just "sensitive" categories, and introduces enforceable rights for Data Principals along with a statutory Data Protection Board.

Phase	What Comes Into Force	Date
Phase I	Provisions establishing the Data Protection Board of India (DPBI)	13 Nov 2025
Phase II	Consent Manager registration and related obligations (Rule 4)	~Nov 2026
Phase III	Substantive compliance obligations — notice, consent, breach reporting, retention, cross-border transfer — become fully enforceable, with the Board's full adjudicatory and penalty powers	~May 2027

The Organization treats the DPDPA/DPDP Rules as the primary, overarching framework for digital personal data and continues to apply the SPDI Rules' security and consent baseline wherever it is stricter or still legally applicable (e.g., for non-digital/offline SPDI processing).

5. Core Privacy Principles

- Lawfulness and purpose limitation — data is collected and processed only for specified, lawful purposes clearly notified to the Data Principal (SPDI Rule 5(2); DPDPA Section 5).
- Notice — Providers/Data Principals are informed of the data collected, the purpose, intended recipients, and details of the collecting/retaining entity, in clear and plain language (SPDI Rule 4; DPDPA Section 5, DPDP Rule 3).
- Consent — data is collected only with free, specific, informed, unconditional, and unambiguous consent, evidenced by clear affirmative action (SPDI Rule 5(1); DPDPA Section 6).
- Data minimization — only data necessary for the identified purpose is collected.
- Retention limitation — data is retained only as long as necessary for the stated purpose or as required by law (SPDI Rule 5(4); DPDPA Section 8(7), DPDP Rule 8).
- Security safeguards — reasonable security practices and procedures protect data against unauthorized access, damage, use, modification, disclosure, or impairment (SPDI Rule 8; DPDPA Section 8(5), DPDP Rule 6).

- Accountability and transparency — the Organization demonstrates compliance and maintains an accessible privacy notice/policy.
- Rights of the individual — Providers of Information and Data Principals may access, review, correct, and withdraw consent for their data, and seek grievance redressal.

6. Collection of Personal Data and SPDI

- SPDI/personal data is collected only for a lawful purpose connected to a function or activity of the Organization, and only where collection is necessary for that purpose (SPDI Rule 5(2)).
- Before collection, a clear notice is given specifying: the fact of collection; the purpose; the intended recipients; and the name and address of the collecting/retaining agency (SPDI Rule 4; DPDP Rule 3 — notice in English or any of the 22 Eighth Schedule languages, on request).
- The Provider/Data Principal has the option to not provide the data sought, and the option to withdraw consent at any time, without affecting the lawfulness of processing carried out before withdrawal.
- Where consent is withdrawn, the Organization ceases processing within a reasonable time, unless retention/processing is required or authorized under law.

7. Consent and Consent Management

- Consent must be free, specific, informed, unconditional, and unambiguous, given through clear affirmative action, and limited to the personal data necessary for the specified purpose (DPDPA Section 6).
- A Data Principal may give, manage, review, or withdraw consent through a Consent Manager, registered with the Data Protection Board under DPDP Rule 4 (obligation phased in from ~November 2026).
- Under the SPDI Rules, consent for collection of SPDI must be obtained in writing, through letter, fax, or email, prior to collection.

- Deemed consent / legitimate uses apply in limited circumstances recognized under the DPDPA (e.g., voluntary disclosure, compliance with law, medical emergency, employment purposes, specified public-interest functions) — applied narrowly and documented.
- Consent requests for children and persons with disabilities require verifiable consent of a parent or lawful guardian; the Organization does not undertake tracking, behavioral monitoring, or targeted advertising directed at children.

8. Disclosure and Transfer of Data

- SPDI is disclosed to a third party only with prior permission of the Provider of Information, or where necessary for compliance with a legal obligation (SPDI Rule 6).
- Personal data may be transferred to another body corporate/data processor only if that entity maintains the same level of data protection required under the SPDI Rules, and the transfer is necessary for lawful performance of a contract, or the Provider has consented (SPDI Rule 7).
- Under the DPDPA, the Organization may transfer personal data outside India except to countries specifically restricted by the Central Government (a "blacklist" approach, in contrast to the SPDI Rules' contractual-equivalence approach).
- All data processors and vendors handling personal data on the Organization's behalf are bound by a written contract obligating them to process data only as instructed and to maintain equivalent security safeguards (DPDPA Section 8(2)).

9. Security Safeguards

- The Organization implements reasonable security practices and procedures, including managerial, technical, operational, and physical controls, commensurate with the information assets being protected (SPDI Rule 8).
- Under the SPDI Rules, compliance with IS/ISO/IEC 27001 or an equivalent, industry-recognized, audited security standard is treated as satisfying the "reasonable security practices" requirement.

- Under DPDP Rule 6, reasonable security safeguards independently prescribed include: encryption, obfuscation, tokenization, or equivalent measures; access controls; continuous monitoring and logging for detection of unauthorized access; retention of logs for at least one year (unless a longer period is required by law); and data backup arrangements to ensure continued processing in the event of compromise.
- Security controls are documented, audited annually (by an independent auditor where required), and updated in response to identified risks.

10. Data Retention and Deletion

- Personal data/SPDI is not retained for longer than required for the purpose for which it was collected, or as otherwise required under applicable law (SPDI Rule 5(4)).
- Under DPDP Rule 8, specified classes of Data Fiduciaries (e.g., e-commerce entities, social media intermediaries, and online gaming platforms meeting notified user thresholds) must erase personal data upon expiry of three years from the date of the Data Principal's last interaction, unless retention is necessary for a specified purpose or legal compliance.
- Data Principals are notified at least 48 hours before scheduled erasure, to allow them to log in or otherwise retain the relationship if they choose.
- Upon fulfilment of the purpose, withdrawal of consent, or expiry of the retention period (whichever is earliest), data is securely erased or anonymized, including copies held by data processors.

11. Rights of Data Principals / Providers of Information

- Individuals have the right to:
- Obtain confirmation of whether their personal data is being processed, and access a summary of the data and processing activities.
- Seek correction, completion, updating, and erasure of their personal data (DPDPA Section 12).
- Withdraw consent at any time, as easily as it was given.

- Nominate another individual to exercise their rights in the event of death or incapacity (DPDPA Section 14).
- Lodge a grievance with the Organization and, if unresolved, escalate to the Data Protection Board of India.
- Under the SPDI Rules, review the information provided and ensure inaccurate or deficient data is corrected.
- The Organization will respond to such requests within the timelines prescribed under applicable law and its internal grievance redressal procedure (Section 13).

12. Personal Data Breach Notification

- Any suspected or confirmed breach of personal data/SPDI is reported immediately to the Organization's designated incident response team/Data Protection Officer.
- The Organization notifies the Data Protection Board of India, with detailed particulars and mitigation measures, generally within 72 hours of becoming aware of the breach (or such period as the Board may allow).
- Affected Data Principals are notified without delay, in clear and plain language describing the nature, extent, and likely consequences of the breach, and the measures taken to mitigate it.
- Breach records, root-cause analysis, and remedial actions are documented and retained as part of the Organization's compliance records.

13. Grievance Redressal

- The Organization designates a Grievance Officer (SPDI Rules) and, as applicable, a Data Protection Officer (DPO) (mandatory for Significant Data Fiduciaries under the DPDPA), whose name and contact details are published on the Organization's website/privacy notice.
- Grievances relating to processing of personal data or SPDI are acknowledged and redressed within the timeline prescribed by applicable law.

- If a Data Principal is not satisfied with the resolution, they may escalate the grievance to the Data Protection Board of India.

Grievance Officer contact details:

Field	Details
Name	Purusothaman.S
Designation	Senior Manager-Information Security
Email	is@rabwin.in
Mobile Number	9952744933
Postal address	SF NO 155, SNMV College Rd, Malumichampatti, Tamil Nadu 641050
Collecting and retaining entity address	SF NO 155, SNMV College Rd, Malumichampatti, Tamil Nadu 641050

14. Additional Obligations for Significant Data Fiduciaries (if applicable)

Where the Organization is notified as a Significant Data Fiduciary, it additionally:

- Appoints a Data Protection Officer based in India, reporting to the Board of Directors/equivalent governing body, who serves as the point of contact for grievance redressal.
- Appoints an independent data auditor to periodically evaluate compliance.
- Conducts a Data Protection Impact Assessment (DPIA) and periodic compliance audits.
- Undertakes such other measures as may be prescribed with respect to algorithmic accountability and cross-border data flow restrictions.

15. Children's Data and Persons with Disabilities

- Processing of personal data of a child (below 18 years) or a person with disability who has a lawful guardian requires verifiable consent of the parent or lawful guardian before processing.
- The Organization does not process children's data in a manner likely to cause detrimental effect on their well-being, and does not undertake tracking, behavioural monitoring, or targeted advertising directed at children, except where exempted under law (e.g., certain healthcare, educational, or child-safety purposes as may be notified).

16. Roles and Responsibilities

Role	Responsibility
Data Protection Officer / Grievance Officer	Overall accountability for privacy compliance, grievance handling, and liaison with the Data Protection Board/regulators.
IT / Information Security Team	Implementation of technical and security safeguards, breach detection, and incident response.
HR / Business Units	Ensuring notice and consent are obtained at the point of collection within their function.
Legal & Compliance	Contractual obligations with processors/vendors, regulatory filings, and monitoring changes in law.
All Employees	Handling personal data only for authorized purposes and reporting suspected incidents immediately.

17. Training and Awareness

All employees and relevant contractors undergo periodic training on data privacy obligations under the SPDI Rules and DPDPA, including data handling, consent requirements, and breach reporting procedures.

18. Policy Review

This policy is reviewed at least annually, and on any material change in applicable law (including further notifications under the DPDP Rules, 2025, as additional Rules come into force through 2026 and May 2027), or following any significant security incident.

19. Non-Compliance and Penalties

- Non-compliance under the SPDI Rules may result in civil liability for compensation under Section 43A of the IT Act for wrongful loss or gain arising from failure to implement reasonable security practices.
- Non-compliance under the DPDPA may attract financial penalties imposed by the Data Protection Board of India, which can extend up to ₹250 crore per instance, depending on the nature and gravity of the breach.
- Internal non-compliance by employees or contractors may additionally result in disciplinary action under the Organization's internal conduct policies.

20. Integration into Rabwin Policies

Internal implementation section. Maintain this section in the controlled ISMS copy; publish the approved privacy text and verified contact details in an accessible public version.

Read this policy together with Rabwin's Digital Personal Data Protection Policy (RAB-ISMS-D096), Document Control Procedure (D041), Data Protection Procedure (D046), Access Control Procedure (D057), Incident Management Procedure (D047), Backup Procedure (D038), Media Handling Procedure (D043), Cloud Security Procedure (D044), Third Party Risk Management Procedure (D055), and approved DLP and retention policies. Confirm current titles, identifiers, and revisions against the Master Document Register.

- Management shall approve the policy and appoint the Grievance Officer.
- ISMS Head shall coordinate implementation and review.

- HR and department owners shall maintain data inventories, collection notices, consent evidence, retention decisions, and request responses.
- IT shall implement security and disposal controls.
- Procurement shall obtain appropriate provider commitments.
- Legal or the designated compliance reviewer shall verify applicability, disclosures, transfers, and statutory deadlines.

Annexure A — Categories of Sensitive Personal Data or Information (SPDI Rules, Rule 3)

Passwords; financial information (bank account/card/payment instrument details); physical, physiological, and mental health condition; sexual orientation; medical records and history; biometric information; and information received by a body corporate for processing, stored, or processed under a lawful contract.

Annexure B — Key DPDP Rules, 2025 Reference Points

Rule	Subject / Commencement
Rules 1, 2, 17–21	Short title, definitions, constitution of the Data Protection Board — 13 Nov 2025
Rule 4	Consent Manager registration and obligations — ~14 Nov 2026
Rule 3	Consent notice content and language requirements — ~14 May 2027
Rule 6	Reasonable security safeguards — phased per notification
Rule 8	Data retention and erasure timelines — phased per notification

Note: Confirm current commencement dates against the latest MeitY notification before finalizing/publishing this policy, as remaining DPDP Rules are being phased in through May 2027.

21. REVIEW AND APPROVAL

This Policy shall be reviewed at least annually and earlier upon a material legal or regulatory change, significant breach, major processing change, new technology, audit finding, SDF notification, change in business scope or change to related Rabwin ISMS documents. This policy shall be reviewed and approved once a year as per the document control procedures

(Doc. No : RAB-ISMS-D041) or whenever there is a major change in the operating environment.

22. EXCEPTIONS

Any exceptions to this policy need to be reviewed and approved by the ISSC.