DATA PROTECTION POLICY

Document Control:

Document Name	Data Protection Policy
Document ID	DPDP _20ML_01/2026
Security Classification	Internal

Authorization:

Document Owner	Reviewed by	Authorized by
Mr.Nitin Anerao	Board of Directors	Board of Directors

Table of Content

1. Introduction

20 Microns Limited ("20ML") recognises the fundamental importance of digital privacy and data protection. With the DPDP Act, 2023 now in force and its operational Rules notified on 13 November 2025, 20ML commits to full compliance with the statutory obligations imposed on Data Fiduciaries under the Act & Rules.

This Policy provides the framework for lawful, fair, transparent, and secure handling of digital personal data across all group entities and business operations.

2. Scope

This Policy applies to:

- 20 Microns Limited, all its subsidiaries, associate companies, JVs, and group entities
- All employees (permanent, contractual, consultants, interns), directors, officers
- All third-parties, vendors, service providers, cloud providers and business partners who process or have access to personal data on behalf of 20ML
- All processing of **digital personal data**, whether collected online or offline (and later digitalised), within India, or outside India if tied to providing goods/services to individuals in India — as applicable under DPDP Act.

3. Objective

- To ensure that all processing of personal data by 20ML is lawful, transparent, secure and in compliance with DPDP Act & Rules.
- To protect the rights of individuals (data principals) whose personal data is processed — including consent, access, correction, erasure, grievance redressal.
- To embed data protection by design and by default across business operations, systems and processes.
- To minimize risk of data breaches, regulatory non-compliance, reputational damage and ensure accountability.

4. Roles & Responsibilities

Data Fiduciary / Data Protection Officer (DPO)

- 20ML (and its subsidiaries/Wholly Owned Subsidiaries/JV/Associate) acts as Data Fiduciary — responsible for deciding purpose & means of processing.
- Designated DPO (or equivalent) shall oversee compliance — ensure consent management, notices, respond to data subject requests, maintain records, coordinate with any regulatory authorities or the Data Protection Board of India (DPBI), as required.

Data Processors

- All vendors / service providers / sub-contractors must comply with 20ML's Data Processing Agreement (DPA), ensure security safeguards, follow instruction of 20ML, and not process data beyond defined scope.

All Employees and Internal Stakeholders

- Must comply with policy, ensure data confidentiality, report breaches, maintain secure practices, and cooperate in audits / assessments and training.

5. Key Definitions (As per DPDP Act / Rues)

- **Data Principal**: The individual whose personal data is processed (in case of children or persons with disability, guardian or parent as applicable).
- **Data Fiduciary**: Entity deciding purpose and means of data processing (e.g., 20ML)
- **Data Processor**: Entity processing data on behalf of Data Fiduciary under contract.
- **Consent Manager**: If 20ML uses any third-party or internal mechanism to manage consents / withdrawals / subject requests — must comply with Rules.
- **Significant Data Fiduciary (SDF)**: If 20ML qualifies (by volume/sensitivity of data) — additional obligations apply: independent audits, DPIAs, algorithmic governance, stricter security, compliance reporting, etc.

6. Data Protection Principles & Policy Provisions

6.1 Lawful Processing & Consent Requirement

- Personal data shall be processed only after obtaining **clear, informed, explicit and unambiguous consent** from the Data Principal (or guardian in case of children / persons with disability), or on another lawful basis recognized under DPDP Act / Rules.
- Pre-ticked boxes, bundled consents or implied consent are prohibited.
- Consent shall include purpose of data collection/use, types of data, duration, rights to withdraw consent, grievance mechanism, contact of DPO / grievance officer, manner to raise complaints.

6.2 Notice & Transparency Obligations

- Before collecting any personal data, 20ML must issue a **clear, comprehensible notice** (in plain language; may be in English or a Schedule-VIII language, as applicable) explaining: nature of data collected, purpose, retention period, rights, how to withdraw consent or lodge grievance.
- 20ML must publicly display / provide contact details of DPO or grievance officer for data-related queries.

6.3 Data Minimisation, Purpose Limitation & Storage Limitation

- Only the minimal personal data strictly necessary for the stated purpose shall be collected.
- Data shall be processed only for specified, lawful purposes.
- Data shall not be retained longer than required; once the purpose is satisfied, data should be archived/deleted in compliance with retention schedule.

6.4 Data Security & Safeguards

- 20ML must implement “reasonable security safeguards” (encryption, access controls, secure storage, logging, regular audits, firewalls, secure backups, etc.).

- For SDF (if applicable), enhanced security, periodic independent audits, impact assessments are required.
- Data stored on paper must be in locked cabinets; electronic data should not be downloaded on personal devices; access on need-to-know basis only; backups stored securely.

6.5 Data Subject Rights

20ML recognises and will respect the following rights of Data Principals (as per DPDP Act & Rules):

- Right to access personal data held by 20ML;
- Right to correction / rectification of inaccurate or incomplete data;
- Right to erasure / deletion when lawful;
- Right to withdraw consent at any time;
- Right to data portability (i.e. receive data in structured format, if requested);
- Right to nominate another person to exercise rights (in case of death, incapacity etc.);
- Right to grievance redressal (complaint mechanism, right to approach DPBI, appeal to Tribunal).

Procedures for requests (access / rectification / erasure / withdrawal) will be defined in separate SOPs/forms (Consent Form, Data-Erasure Request Form, etc.).

6.6 Data Breach & Incident Management

In case of any personal data breach or security incident, 20ML must:

1.Immediately notify the designated DPO / grievance officer.

2. Undertake containment, damage assessment, remediation.

3. Notify the affected Data Principals in plain language (explain nature of breach, possible impact, remedial steps taken), via available contact channel.

Also ensure reporting to regulatory authority (DPBI) if required under the Rules.

6.7 Data Retention, Classification & Disposal

- Data shall be classified (e.g. Public / Internal / Confidential / Highly Confidential) as per sensitivity and business/ regulatory requirements.
- Retention schedule will be defined — data not needed beyond purpose or statutory retention period must be securely deleted or archived.
- Secure disposal methods to be used (shredding for physical records; secure wipe for electronic records).

6.8 Cross-border Data Transfers

- Any transfer of personal data outside India must comply with conditions specified under DPDP Rules. 20ML must assess the destination country's adequacy or provide adequate safeguards (as may be notified).
- Ensure Data Principals are informed in the consent notice about possible cross-border transfer and obtain explicit consent where required.

6.9 Third-Party / Vendor Compliance & Data Processing Agreements (DPA)

- All third-parties or processors engaged by 20ML must sign a Data Processing Agreement (DPA) mandating compliance with DPDP Act / Rules, confidentiality, security safeguards, limitation to instructions, and prohibition on onward transfers except as permitted.
- For any vendor handling significant personal data, 20ML will conduct due diligence including security assessment and periodic audits.

6.10 Privacy by Design & DPIA

- At design or procurement stage of any new system, product, process or service — 20ML must incorporate privacy and data protection controls (minimisation, encryption, access control, consent management, ability for subject requests, logging, audit trails).
- Where processing involves large volumes, sensitive data or high risk (e.g. children's data, financial data, health data) — conduct a formal Data Protection Impact Assessment (DPIA) before launch. For SDF, DPIA may be mandatory.

7. Compliance, Governance & Audit

- 20ML will maintain records of processing activities, consents, breach incidents, audits, DPIAs, vendor assessments, subject requests etc. — to demonstrate compliance.
- For SDF (if 20ML qualifies), periodic independent data protection audits must be carried out.
- Non-compliance with this Policy will attract disciplinary action. Violations may also expose 20ML to penalties under DPDP Act (up to ₹250 crore for serious violations, breach of security safeguards, or failure to notify breach / comply with obligations).

8. Staff Guidelines & Awareness

- All employees will undergo mandatory data protection training (at induction and regular intervals).
- Access to personal data shall be strictly on "need-to-know" basis.
- Strong passwords, multi-factor authentication (MFA), secure log-offs / screen-locks, no storing of data on personal devices.
- Report any suspected data breach / misuse immediately to DPO / Grievance Officer.
- Respect data subject rights — facilitate access / correction / erasure / withdrawal requests as per SOPs.

9. Review and Revision

- This Policy shall be reviewed at least annually, or earlier if there is change in law (amendment to DPDP Act/Rules), business model, technology environment, or a data incident.
- Any revision must be authorised by the Board and communicated to all relevant stakeholders.