



VMENTORZ – Data Protection Policy

Version: 1.0

Effective Date: January 29, 2026

1. Purpose

This Data Protection Policy ("Policy") establishes the internal governance framework adopted by VMENTORZ Private Limited ("VMENTORZ" or "Company") for the lawful collection, processing, storage, use, retention, protection, and deletion of personal data in accordance with the Digital Personal Data Protection Act, 2023 ("DPDP Act"), applicable rules, notifications, and other relevant laws.

This Policy applies to all individuals and entities processing personal data on behalf of VMENTORZ, including:

- Employees
- Directors
- Contractors
- Mentors / Practitioners
- Technology vendors
- Service providers
- Any other authorised person handling data under the Company's control

This Policy is an internal governance document and governs operational conduct, accountability, and compliance practices within VMENTORZ.

2. Definitions

For the purpose of this Policy:

Personal Data

Personal Data means any data about an individual who is identifiable directly or indirectly by or in relation to such data, including but not limited to name, contact information, account details, transaction records, digital identifiers, or any information linked to a specific individual.

Sensitive / Health Data

Sensitive / Health Data means Personal Data relating to an individual's mental health condition, assessment responses, therapy or counselling notes, psychological disclosures, session summaries, audio/video session content (where applicable), or any information revealing physical or mental health status.

For internal governance purposes, such data shall be classified as Highly Sensitive Data and subject to enhanced access, storage, and security safeguards.

Data Principal

Data Principal means the individual to whom the Personal Data relates, including users of the Platform, mentors, employees, contractors, or any identifiable individual whose Personal Data is processed by VMENTORZ.

Data Fiduciary

Data Fiduciary means VMENTORZ Private Limited, which alone or in conjunction with others determines the purpose and means of processing Personal Data under this Policy.

Data Processor

Data Processor means any individual or entity that processes Personal Data on behalf of VMENTORZ pursuant to documented contractual arrangements and defined instructions, including cloud service providers, payment processors, and technology vendors.



Processing

Processing means any operation or set of operations performed on Personal Data, whether automated or manual, including collection, recording, organisation, storage, structuring, use, transmission, sharing, retrieval, disclosure, anonymisation, or deletion.

Consent

Consent means a freely given, specific, informed, and unambiguous indication by the Data Principal, through a clear affirmative action, signifying agreement to the processing of Personal Data for a specified purpose.

Anonymised Data

Anonymised Data means data that has been irreversibly processed in such a manner that the individual cannot be identified, directly or indirectly, by any means reasonably likely to be used.

Aggregated Data

Aggregated Data means data that has been combined with other data in a manner that does not permit identification of any specific individual.

Data Breach

Data Breach means any unauthorised access, acquisition, disclosure, alteration, loss, destruction, or compromise of Personal Data that affects its confidentiality, integrity, or availability, whether accidental or unlawful.

3. Data Classification Framework

VMENTORZ classifies personal data into categories based on sensitivity, risk exposure, and potential impact in the event of unauthorised disclosure, misuse, or breach.

Data classification determines applicable access controls, retention standards, security safeguards, and breach response prioritisation.

3.1 General Personal Data

General Personal Data includes routine personal information required for platform operations, including but not limited to:

- Name
- Email address
- Phone number
- Account credentials
- Transaction records
- Appointment schedules
- Non-sensitive communications

Safeguards for General Personal Data include:

- Role-based access controls
- Secure cloud infrastructure
- Encryption in transit
- Standard authentication mechanisms

3.2 Sensitive / Health Data (Highly Sensitive Data)

Sensitive / Health Data includes:

- Mental health assessment responses
- Session notes
- Psychological disclosures
- Therapy or counselling summaries
- Audio or video session recordings (if implemented in future)



- Any information revealing physical or mental health status

Due to the nature of VMENTORZ's services, Sensitive / Health Data shall be internally classified as Highly Sensitive Data.

Enhanced safeguards shall apply, including:

- Restricted access strictly on a need-to-know basis
- Segregation from general operational datasets where feasible
- Strong encryption standards
- Access logging and monitoring where technically feasible
- Heightened breach response prioritisation

Practitioner-Generated Session Notes

Session notes created by Mentors are professional records generated in the course of independent service delivery. VMENTORZ does not control the professional judgment exercised by Mentors in determining the clinical or subjective content of such notes.

However:

- Mentors are contractually required to comply with applicable data protection laws;
- Mentors must apply data minimisation principles and record only information reasonably necessary for service delivery;
- Mentors must not store, download, copy, or retain session data outside authorised Platform systems unless legally required;
- Mentors must implement reasonable safeguards when accessing data.

VMENTORZ shall not be responsible for the professional opinions, clinical assessments, or narrative content recorded by Mentors, provided such records are created within the scope of lawful professional practice.

VMENTORZ reserves the right to review, restrict, suspend, or terminate Platform access where note-taking practices are found to violate applicable law, this Policy, platform standards, or user safety requirements.

3.3 Confidential Internal & Professional Data

Confidential Internal & Professional Data includes:

- Mentor credentials and verification documents
- Internal evaluation reports
- Performance metrics
- Internal investigation records
- Security configurations
- Access control logs
- System architecture details

Access to such data shall be restricted to authorised personnel only and protected against unauthorised internal disclosure.

3.4 Classification Review

Data classification categories and safeguards shall be reviewed periodically by the Data Protection Lead to ensure alignment with:

- Platform feature changes
- Introduction of proprietary recording infrastructure
- AI system expansion
- Regulatory developments
- Evolving security risks



4. Lawful Basis for Processing

VMENTORZ processes Personal Data strictly in accordance with applicable law and only on lawful grounds, including:

- Consent of the Data Principal, obtained through clear affirmative action for specified purposes;
- Performance of a Contract, where processing is necessary for providing services requested by the Data Principal;
- Compliance with Legal Obligations, where processing is required under applicable laws, regulations, or lawful governmental directives;
- Legitimate Uses as permitted under the DPDP Act, including purposes reasonably expected by the Data Principal in the context of service delivery, prevention of fraud, enforcement of legal rights, or internal operational security;
- Protection of Vital Interests, including emergency situations involving risk to life, health, or safety.

All processing activities shall be purpose-bound, proportionate, and limited to what is reasonably necessary to achieve the specified objective.

5. Data Minimisation & Purpose Limitation

VMENTORZ shall collect and process only such Personal Data as is reasonably necessary for specified, lawful, and clearly defined purposes related to platform operations, service delivery, legal compliance, security, and risk management.

Personal Data shall not be collected or retained where:

- It is unrelated to the defined service purpose;
- It is excessive in scope relative to the stated objective;
- The purpose can be reasonably achieved through anonymised or aggregated data.

All processing shall be:

- Purpose-bound;
- Proportionate to the intended objective;
- Limited in duration consistent with retention standards.

Internal teams shall ensure that:

- New platform features undergo data impact consideration prior to implementation;
- AI-enabled tools use anonymised or aggregated data where feasible;
- Additional data fields are not introduced without documented operational justification.

Any proposed expansion in categories of data collected shall be reviewed by the Data Protection Lead prior to deployment.

6. Roles & Responsibilities

Effective data protection governance requires clearly defined accountability structures within VMENTORZ.

6.1 Data Fiduciary

VMENTORZ acts as the Data Fiduciary under applicable law and is responsible for:

- Determining the purpose and means of processing Personal Data;
- Ensuring compliance with the DPDP Act and other applicable laws;
- Implementing reasonable technical and organisational safeguards;
- Enabling Data Principal rights;



- Maintaining internal records of data processing activities;
- Responding to data breaches in accordance with law.

Ultimate accountability for data protection rests with the Company.

6.2 Data Protection Lead / Compliance Officer

VMENTORZ shall designate a Data Protection Lead (or equivalent internal role) responsible for:

- Overseeing implementation of this Policy;
- Reviewing new data collection practices and feature deployments;
- Monitoring lawful basis for processing;
- Supervising breach response and documentation;
- Maintaining the Data Retention Matrix;
- Conducting periodic compliance reviews;
- Coordinating with legal advisors and regulators where required.

The Data Protection Lead shall have authority to recommend corrective actions where non-compliance is identified.

6.3 Operational Teams

All employees and contractors handling Personal Data shall:

- Access data strictly on a need-to-know basis;
- Comply with access control policies;
- Immediately report suspected breaches or misuse;
- Participate in mandatory data protection training.

Managers are responsible for ensuring team-level compliance with this Policy.

6.4 Mentors / Practitioners

Mentors operating on the Platform:

- Are independent professionals responsible for lawful handling of Personal Data accessed through the Platform;
- Must comply with applicable data protection laws and contractual obligations;
- Must not export, copy, or retain Personal Data outside authorised systems unless legally required;
- Must implement reasonable safeguards when accessing user information.

Failure to comply may result in suspension or termination of Platform access.

6.5 Data Processors & Vendors

Third-party service providers processing Personal Data on behalf of VMENTORZ:

- Must operate under written contractual arrangements;
- Must process data only in accordance with documented instructions;
- Must implement reasonable security safeguards;
- Must notify VMENTORZ of any suspected data breach without undue delay.

Vendor performance and security posture may be periodically reviewed.

7. Access Control & Role-Based Permissions

VMENTORZ implements role-based access controls (RBAC) to ensure that access to Personal Data is restricted strictly to authorised individuals based on functional necessity and operational responsibility.

Access shall be granted in accordance with the principle of least privilege, meaning individuals shall only have access to the minimum Personal Data required to perform their assigned duties.

7.1 Role-Based Access Structure

Access permissions shall be structured based on defined role categories, including but not limited to:



- Platform administrators
- Customer experience personnel
- Technical personnel
- Compliance personnel
- Mentors / Practitioners

Sensitive / Health Data shall be accessible only to those roles directly involved in service delivery, compliance oversight, or authorised operational support.

7.2 Authentication & Credential Controls

Access to systems containing Personal Data shall be protected through reasonable authentication controls, including:

- Secure password policies;
- Multi-factor authentication where technically and commercially feasible;
- Periodic credential review;
- Immediate revocation of access upon termination, contract expiry, or role change.

Shared credentials are prohibited.

Individuals are responsible for maintaining confidentiality of their access credentials.

7.3 Access Logging & Monitoring

Where technically feasible, VMENTORZ shall maintain system logs reflecting access to Sensitive / Health Data.

Access logs may be periodically reviewed to identify:

- Unauthorised access attempts;
- Excessive data queries;
- Suspicious or anomalous access patterns.

Where high-risk anomalies are identified, appropriate internal review and corrective action may be undertaken.

7.4 Access Review & Revocation

Access permissions shall be:

- Reviewed periodically by authorised personnel;
- Adjusted in accordance with changes in role or responsibility;
- Revoked immediately upon termination of employment, contract, or engagement.

Temporary access permissions, where granted, should be time-bound where feasible.

7.5 Mentor Access Restrictions

Mentors shall have access only to Personal Data relating to users assigned to them for the purpose of service delivery.

Mentors shall not access, attempt to access, or retrieve data relating to users not assigned to them, except where expressly authorised for legitimate operational purposes.

Unauthorised access, attempted access, or misuse of Personal Data may result in suspension or termination of Platform access and other corrective measures.

7.6 Progressive Security Enhancement

Security controls and access management practices shall evolve in proportion to platform growth, infrastructure capability, user volume, and regulatory expectations.

VMENTORZ shall periodically assess the need for enhanced safeguards, including but not limited to:

- Encryption of data at rest;
- Segregation of production and non-production environments;
- Segmented storage for Sensitive / Health Data;
- Infrastructure hardening measures.



Implementation of such measures shall be aligned with operational scale, risk profile, and resource availability, while maintaining reasonable security safeguards as required under applicable law.

8. Data Retention & Deletion Framework

VMENTORZ shall retain Personal Data only for as long as necessary to fulfil the specific purpose for which it was collected, or as required under applicable law, regulatory obligations, dispute resolution requirements, or legitimate operational needs.

Retention shall be proportionate to:

- The sensitivity of the data;
- The nature of the services provided;
- Applicable statutory or regulatory requirements;
- Risk management considerations;
- Contractual or audit requirements.

Personal Data shall not be retained indefinitely without defined operational, legal, or compliance justification.

8.1 Retention Governance

VMENTORZ shall maintain an internal Data Retention Matrix that specifies:

- Categories of data processed;
- Applicable retention duration or retention triggers;
- Legal or operational basis for retention;
- Deletion or anonymisation protocol.

Retention periods may vary depending on the category of data and applicable legal or operational requirements and shall be defined and managed through the internal Data Retention Matrix maintained by VMENTORZ.

The Data Retention Matrix shall be reviewed periodically and updated in accordance with regulatory developments, infrastructure changes, and business needs.

8.2 User-Initiated Deletion Requests

Where a Data Principal exercises a lawful right to deletion or erasure:

- Requests shall be reviewed in accordance with applicable law;
- Data shall be deleted or anonymised unless retention is required for legal compliance, fraud prevention, dispute resolution, regulatory obligations, or enforcement of rights;
- Actions taken shall be documented internally where feasible.

8.3 Sensitive / Health Data Retention

Sensitive / Health Data shall be retained with heightened caution, given the potential impact of misuse or breach.

Retention of session notes and other health-related data shall be:

- Limited to continuity of care requirements;
- Subject to legal defence considerations;
- Evaluated in light of user inactivity or account closure;
- Governed by the internal Data Retention Matrix.

If proprietary audio/video session recording infrastructure is implemented in future, separate retention controls for recordings shall be defined within the Data Retention Matrix.

8.4 Secure Deletion & Anonymisation

Upon expiry of retention triggers:

- Personal Data shall be securely deleted; or
- Irreversibly anonymised where continued retention of anonymised insights is operationally justified.



Deletion and anonymisation processes shall be implemented in a manner proportionate to infrastructure capability and commercially reasonable security safeguards.

9. Data Sharing & Disclosure Controls

VMENTORZ shall share Personal Data only where necessary, lawful, and proportionate to defined operational, legal, regulatory, or service-related purposes.

Data sharing shall be purpose-bound and limited to the minimum data required to achieve the intended objective.

9.1 Sharing for Service Delivery

Personal Data may be shared:

- With Mentors for the purpose of session delivery, continuity of care, and professional engagement;
- With authorised internal personnel responsible for operational support, compliance, security, risk management, or customer experience.

Access shall remain restricted in accordance with role-based permissions defined under this Policy.

9.2 Sharing with Service Providers & Vendors

Personal Data may be shared with third-party Data Processors, including but not limited to:

- Cloud infrastructure providers;
- Payment processors;
- Communication platforms;
- Technology vendors;
- Analytics and infrastructure service providers.

Such sharing shall be governed by written agreements requiring:

- Confidentiality obligations;
- Processing strictly under documented instructions;
- Implementation of reasonable security safeguards;
- Prompt notification of any suspected or confirmed data breach.

Vendor access shall be limited to what is necessary for service provision.

9.3 Sharing with Affiliates & Related Entities

Personal Data may be shared with group entities, affiliates, or related healthcare initiatives operated by or associated with VMENTORZ where:

- Such sharing supports continuity of care, operational integration, lawful business expansion, or service enhancement;
- The sharing remains consistent with the original purpose of collection or is otherwise permitted under applicable law;
- Appropriate contractual and security safeguards are implemented.

Such sharing shall remain subject to this Policy and applicable data protection standards.

9.4 Regulatory & Legal Disclosure

Personal Data may be disclosed to regulatory authorities, law enforcement agencies, courts, or other governmental bodies where:

- Required under applicable law;
- Necessary to comply with lawful directives;
- Required to protect or enforce legal rights;
- Necessary to address emergency situations involving risk to life, health, or safety.



Disclosures shall be limited to what is legally required or reasonably necessary in the circumstances.

9.5 Restrictions & Permitted Commercial Use of Data

Personal Data shall not be disclosed, transferred, or commercially exploited in identifiable form except where permitted under applicable law and supported by a lawful basis for processing.

Nothing in this Policy restricts VMENTORZ from using, analysing, or commercialising Anonymised Data or Aggregated Data, provided such data does not identify any individual and cannot reasonably be re-identified.

Sensitive / Health Data shall be subject to heightened scrutiny prior to any external disclosure and shall not be shared externally in identifiable form without lawful basis and appropriate safeguards.

10. AI Governance & Data Usage Controls

VMENTORZ may deploy artificial intelligence (AI), machine learning models, or automated systems to support platform functionality, including but not limited to:

- Mentor recommendations;
- User matching;
- Assessment interpretation support;
- Operational analytics;
- Fraud detection and risk management;
- Customer experience enhancement.

AI systems are intended to support service delivery and operational efficiency and do not replace independent professional judgment exercised by Mentors.

10.1 Nature & Scope of AI Systems

AI tools deployed by VMENTORZ:

- Shall not autonomously provide clinical diagnosis or treatment decisions;
- Shall operate within clearly defined purpose limitations;
- Shall be subject to human oversight where appropriate;
- Shall not override independent professional judgment of Mentors.

AI outputs are assistive in nature and may require contextual interpretation. AI outputs are probabilistic and may contain inaccuracies, incomplete interpretations, or contextual limitations. AI systems shall not be treated as determinative, authoritative, or independently sufficient for clinical, diagnostic, or therapeutic decision-making.

10.2 Data Usage for AI Training & Improvement

VMENTORZ may use Personal Data for the purpose of improving AI systems, provided that:

- Such use is supported by a lawful basis for processing;
- Sensitive / Health Data is subject to heightened safeguards;
- Data is anonymised or aggregated where feasible;
- Use of identifiable Personal Data is limited to what is reasonably necessary and proportionate.

AI training shall not involve identifiable Sensitive / Health Data for commercial deployment without appropriate legal basis and safeguards.

10.3 Anonymisation & Aggregation Controls

Where data is used for AI development, analytics, or research:

- VMENTORZ shall prioritise the use of Anonymised Data or Aggregated Data;
- Reasonable measures shall be implemented to prevent re-identification;
- Outputs derived from anonymised data shall not be used to reconstruct identifiable profiles.

10.4 Bias & Risk Awareness



VMENTORZ acknowledges that AI systems may present risks including:

- Bias in recommendation patterns;
- Inaccurate or incomplete outputs;
- Limitations based on training datasets.

AI systems shall be periodically reviewed for performance, consistency, and risk indicators where feasible.

10.5 Future AI Expansion

As AI capabilities evolve, VMENTORZ shall:

- Review data usage practices;
- Evaluate regulatory requirements;
- Update governance controls where necessary;
- Align AI deployment with ethical, legal, and operational considerations.

10.6 – AI Limitations & Risk Allocation

AI systems deployed by VMENTORZ are designed to support operational and service functions and may produce errors, inconsistencies, or unintended outputs.

VMENTORZ shall not rely solely on AI-generated outputs for critical decisions affecting user health or safety without appropriate human review.

Mentors remain responsible for exercising independent professional judgment in all service-related decisions.

11. Session Data Handling Protocol

Session-related data represents highly sensitive information and shall be subject to enhanced governance controls.

11.1 Current Session Infrastructure

At present:

- VMENTORZ does not centrally record audio or video sessions.
- Sessions may be conducted through third-party communication platforms.
- Recording functionality, if enabled, is subject to the policies and consent mechanisms of the external platform used.

VMENTORZ does not automatically initiate or enforce recording of sessions under the current operational model.

11.2 Recording Restrictions

No session shall be recorded without the knowledge and consent of all participating parties.

Users and Mentors are responsible for ensuring compliance with applicable laws and platform standards if recording is initiated through third-party tools.

VMENTORZ shall not be responsible for unauthorised recordings initiated outside authorised Platform infrastructure.

11.3 Session Notes

Session notes may be created by Mentors and/or users for the purpose of:

- Continuity of care;
- Progress tracking;
- Professional documentation.

Session notes stored within the Platform shall:

- Be treated as Sensitive / Health Data;
- Be subject to role-based access controls;
- Not be accessible to unauthorised personnel.

Mentors are responsible for ensuring that notes:

- Are proportionate and professionally appropriate;
- Do not contain excessive or unrelated Personal Data;



- Are not exported, downloaded, or stored outside authorised systems without lawful basis.

11.4 Future Recording Infrastructure

If VMENTORZ introduces proprietary audio/video infrastructure in future:

- Session recording shall require explicit, informed consent;
- Recording shall not be enabled by default without appropriate transparency;
- Recordings shall be classified as Highly Sensitive Data;
- Enhanced access restrictions and retention controls shall apply;
- Recording retention periods shall be defined in the Data Retention Matrix.

No recording shall be used for AI training, analytics, or commercial deployment in identifiable form without lawful basis and appropriate safeguards.

11.5 Incident Escalation

Any suspected misuse, unauthorised access, or improper handling of session-related data shall be escalated in accordance with the Data Breach Response & Incident Management framework under this Policy.

11.6 Compliance Review Authority

VMENTORZ reserves the right to review compliance with data handling obligations under this Policy, including adherence to access controls, storage restrictions, and authorised use of session-related data.

Such review shall be limited to data protection and security compliance and shall not constitute clinical evaluation of professional practice.

Where specialised review is required, VMENTORZ may engage competent external professionals or advisors to assess compliance with applicable data protection standards.

Failure to cooperate with lawful compliance review may result in corrective action, including suspension or termination of Platform access.

12. Data Breach Response & Incident Management

VMENTORZ shall implement a structured and proportionate approach to identifying, managing, and responding to data security incidents, including Personal Data breaches.

An “Incident” for the purpose of this Policy includes any actual or suspected event that compromises the confidentiality, integrity, or availability of Personal Data.

12.1 Incident Identification & Reporting

All employees, contractors, Mentors, and service providers who become aware of a suspected or actual data incident shall report the matter without undue delay to the designated Data Protection Lead or authorised internal contact.

Examples of reportable incidents include:

- Unauthorised access to user data;
- Accidental disclosure of Personal Data;
- Loss or compromise of devices containing data;
- Suspicious system activity;
- Unauthorised recordings or exports of session-related data.

Failure to report a known incident may result in disciplinary action.

12.2 Initial Assessment & Containment

Upon receiving notice of an incident, VMENTORZ shall:

- Conduct a preliminary assessment of the nature and scope of the incident;
- Identify affected systems and categories of data;



- Take reasonable steps to contain further exposure;
- Preserve relevant logs or evidence where feasible.

Containment measures shall be proportionate to the severity and scale of the incident.

12.3 Risk Evaluation

The Data Protection Lead (or designated authority) shall assess:

- The sensitivity of the affected data;
- The number of affected Data Principals;
- The likelihood of harm;
- Potential regulatory obligations;
- Reputational and operational impact.

Sensitive / Health Data incidents shall be treated as high priority.

12.4 Regulatory & User Notification

Where required under applicable law, VMENTORZ shall notify:

- The relevant regulatory authority;
- Affected Data Principals.

Notification shall be made within legally prescribed timelines and shall include information reasonably necessary to describe:

- The nature of the breach;
- Categories of data involved;
- Remedial steps taken;
- Recommended precautions for affected individuals (where applicable).

12.5 Corrective Action & Remediation

Following containment, VMENTORZ shall take reasonable steps to:

- Remediate identified vulnerabilities;
- Strengthen safeguards where necessary;
- Update internal controls to prevent recurrence;
- Review vendor obligations where relevant.

Remedial actions shall be proportionate to operational scale and infrastructure capability.

12.6 Documentation & Incident Register

VMENTORZ shall maintain an internal record of material data incidents, including:

- Date and nature of the incident;
- Impact assessment;
- Containment measures taken;
- Notifications issued (if any);
- Corrective actions implemented.

The Incident Register shall be retained for governance and compliance purposes.

12.7 Lessons Learned & Control Improvement

Following resolution of a significant incident, VMENTORZ shall conduct a structured review to:

- Identify root causes;
- Evaluate adequacy of existing safeguards;
- Determine improvements to technical or organisational controls;
- Update policies or procedures where necessary.



Security controls shall evolve in response to operational learnings and emerging risks.

13. Security Safeguards Framework

VMENTORZ shall implement reasonable technical and organisational safeguards designed to protect Personal Data against unauthorised access, disclosure, alteration, loss, destruction, or misuse.

Security measures shall be proportionate to:

- The sensitivity of the data processed;
- The scale of operations;
- The evolving threat landscape;
- Infrastructure capability and commercial feasibility.

Security controls shall evolve in alignment with operational growth and may progressively align with recognised industry security standards as the Platform scales.

13.1 Technical Safeguards

Where technically and commercially feasible, VMENTORZ shall implement safeguards including:

- Encryption of data in transit;
- Secure cloud hosting infrastructure;
- Firewall and access control mechanisms;
- Authentication and credential protection controls;
- Segmentation of systems handling Sensitive / Health Data where practicable;
- Regular system updates and patch management practices.

Future enhancements may include encryption of data at rest, infrastructure hardening, environment segregation (production and non-production), and advanced monitoring controls as operational maturity increases.

13.2 Organisational Safeguards

VMENTORZ shall implement organisational controls including:

- Role-based access policies;
- Confidentiality obligations for employees, contractors, and Mentors;
- Defined data handling procedures;
- Vendor due diligence and onboarding controls;
- Documented review processes for new data categories or platform features.

Access to Sensitive / Health Data shall be restricted strictly on a need-to-know basis.

13.3 Vendor & Cloud Security Governance

Where third-party infrastructure providers are engaged:

- Providers shall be selected based on security capability, reputation, and reliability;
- Data processing agreements shall define security, confidentiality, and breach notification obligations;
- Cloud configurations shall be secured in accordance with provider best practices and internal risk assessment.

VMENTORZ shall periodically review vendor risk exposure in proportion to operational scale.

13.4 Secure Development & Change Management

New platform features affecting Personal Data shall undergo internal review to assess:

- Data minimisation alignment;
- Access control implications;
- Security risk exposure;



- Compliance impact.

Changes involving Sensitive / Health Data shall be reviewed by the Data Protection Lead prior to deployment.

13.5 Progressive Security Maturity

VMENTORZ recognises that cybersecurity risks evolve over time.

As operational scale increases, the Company may:

- Formalise security governance frameworks;
- Adopt structured risk assessment methodologies;
- Pursue alignment with recognised security certifications;
- Implement advanced monitoring and audit controls.

Security enhancements shall be implemented progressively in alignment with business growth, risk profile, and regulatory expectations.

14. Cross-Border Data Transfers

VMENTORZ may process, store, or access Personal Data using cloud infrastructure, technology platforms, or service providers that operate across multiple jurisdictions.

Personal Data may therefore be transferred to, stored in, or processed in locations outside India where such transfer is necessary for:

- Service delivery;
- Infrastructure management;
- Operational continuity;
- Analytics and system improvement;
- Lawful business expansion into new geographies;
- Disaster recovery or redundancy mechanisms.

14.1 Legal Basis & Regulatory Compliance

Cross-border transfers shall be undertaken:

- In accordance with the Digital Personal Data Protection Act, 2023, and any rules or notifications issued thereunder;
- Subject to lawful basis for processing;
- In compliance with any government restrictions on designated jurisdictions.

If specific countries or territories are restricted by regulatory notification, VMENTORZ shall take reasonable steps to ensure compliance with such requirements.

14.2 Safeguards for International Processing

Where Personal Data is processed outside India, VMENTORZ shall:

- Enter into written agreements with Data Processors requiring confidentiality and security safeguards;
- Require vendors to implement reasonable data protection controls;
- Apply role-based access restrictions;
- Use encryption and security controls proportionate to data sensitivity.

Sensitive / Health Data shall be subject to heightened review prior to cross-border processing.

14.3 Global Infrastructure & Multi-Region Operations

As VMENTORZ expands into additional geographies, Personal Data may be processed within regional infrastructure to support:



- Local service delivery;
- Compliance with jurisdiction-specific requirements;
- Improved performance and user experience.

Cross-border processing may also occur through:

- Cloud redundancy mechanisms;
- Backup and disaster recovery configurations;
- Global network routing;
- Vendor support operations.

All such processing shall remain subject to this Policy.

15. Children's Data Protection Framework

VMENTORZ recognises that Personal Data relating to children requires heightened protection due to the potential vulnerability of minors.

For the purpose of this Policy, a "Child" shall mean an individual below the age threshold prescribed under applicable law.

15.1 Lawful Processing & Guardian Consent

Where services are provided to a Child:

- Personal Data shall be processed only with verifiable consent of a parent or lawful guardian, in accordance with applicable law;
- Guardian consent mechanisms shall be proportionate to the operational model of the Platform;
- VMENTORZ shall take reasonable steps to verify age and guardian authority where applicable.

No processing of a Child's Personal Data shall occur in the absence of lawful basis.

15.2 Heightened Safeguards

Personal Data of Children shall be treated as Highly Sensitive Data and shall be subject to:

- Restricted access controls;
- Enhanced monitoring where feasible;
- Careful limitation of data collection to what is necessary for service delivery.

Profiling or behavioural tracking of Children for unrelated commercial purposes shall not be undertaken.

15.3 Therapeutic Confidentiality Considerations

VMENTORZ acknowledges that, in certain therapeutic contexts, Mentors may conduct sessions with minors in a private or confidential setting, consistent with professional standards.

While guardian consent is required for lawful processing, Mentors retain independent professional judgment in determining appropriate session structure, including private discussion where clinically justified.

VMENTORZ does not interfere in clinical methodology but expects compliance with applicable child protection and mandatory reporting laws.

15.4 Mandatory Reporting & Risk Escalation

Where information disclosed during sessions indicates risk of harm, abuse, exploitation, or threat to life or safety:

- Mentors shall comply with applicable mandatory reporting obligations;
- Appropriate escalation procedures may be triggered;
- Disclosure to competent authorities may be undertaken where required by law.

Such actions shall be documented in accordance with the Incident Management Framework.

15.5 Platform Limitations



VMENTORZ operates as a technology facilitation platform and does not independently supervise live session interactions.

Responsibility for lawful and ethical therapeutic conduct rests with the licensed Mentor providing services.

However, VMENTORZ reserves the right to take corrective action where conduct violates applicable law, platform standards, or child protection obligations.

16. Audit & Compliance Monitoring

VMENTORZ shall maintain oversight mechanisms to monitor compliance with this Policy and applicable data protection laws.

Audit and compliance activities shall be proportionate to operational scale, risk profile, and regulatory requirements.

16.1 Internal Compliance Review

The Data Protection Lead (or designated authority) shall periodically review:

- Data handling practices;
- Access control configurations;
- Incident management documentation;
- Vendor compliance posture;
- Retention matrix alignment.

Internal reviews may include structured self-assessments, documentation verification, or system access review.

16.2 Trigger-Based Review

Additional compliance reviews may be conducted:

- Following a material data incident;
- Upon regulatory inquiry;
- Prior to major infrastructure changes;
- Before launching significant new features involving Personal Data;
- Where systemic risk indicators are identified.

16.3 External Assessment

Where operational scale, regulatory expectations, or business requirements necessitate enhanced oversight, VMENTORZ may engage qualified external professionals to conduct:

- Security assessments;
- Compliance reviews;
- Certification audits;
- Infrastructure evaluations.

External assessment shall be implemented progressively in alignment with business growth and resource capability.

16.4 Corrective & Preventive Actions

Where non-compliance or control weaknesses are identified, VMENTORZ shall:

- Document findings;
- Define corrective actions;
- Assign responsibility for remediation;
- Monitor implementation progress.

Repeated or serious violations may result in disciplinary or contractual action.

16.5 Documentation & Governance Records

VMENTORZ shall maintain internal documentation sufficient to demonstrate compliance efforts, including:

- Policy versions;
- Incident records;



- Retention matrix updates;
- Review logs where applicable.

Documentation shall be retained proportionate to governance needs.

17. Training & Awareness

VMENTORZ recognises that effective data protection requires awareness and accountability across the organisation. Training and awareness measures shall be proportionate to operational scale and data sensitivity.

17.1 Employee & Contractor Training

Employees and contractors handling Personal Data shall receive appropriate guidance regarding:

- Data protection obligations;
- Secure data handling practices;
- Access control responsibilities;
- Incident reporting requirements;
- Confidentiality expectations.

Training may be delivered through structured sessions, internal briefings, documented guidance materials, or onboarding processes.

17.2 Mentor Awareness

Mentors operating on the Platform shall be informed of their data protection obligations through:

- Engagement agreements;
- Code of Conduct;
- Platform usage guidelines.

Where appropriate, VMENTORZ may provide guidance materials relating to secure data handling and confidentiality. Mentors remain independently responsible for compliance with applicable data protection laws and professional standards.

17.3 Ongoing Awareness & Updates

Where significant changes are made to:

- Data processing practices;
- Security controls;
- Regulatory requirements;
- Platform infrastructure;

VMENTORZ may communicate relevant updates to affected personnel.

17.4 Progressive Maturity

As the Platform scales, VMENTORZ may implement more structured training programs, periodic refreshers, or role-specific awareness initiatives in alignment with regulatory expectations and operational growth.

18. Disciplinary Measures

Compliance with this Policy is mandatory for all individuals handling Personal Data under the authority of VMENTORZ.

Failure to comply with data protection obligations may result in corrective, disciplinary, or contractual action proportionate to the nature and severity of the breach.

18.1 Employees & Contractors



Where an employee or contractor:

- Accesses Personal Data without authorisation;
- Fails to report a known data incident;
- Misuses, discloses, or mishandles Personal Data;
- Violates access control or confidentiality obligations;

VMENTORZ may take action including:

- Formal warning;
- Temporary suspension of access privileges;
- Mandatory retraining;
- Termination of employment or engagement;
- Legal action where appropriate.

18.2 Mentors / Practitioners

Where a Mentor:

- Accesses data beyond assigned users;
- Exports, copies, or stores data outside authorised systems;
- Fails to comply with data handling obligations;
- Engages in unauthorised recording or disclosure;
- Violates child protection or mandatory reporting requirements;

VMENTORZ may take action including:

- Temporary suspension of Platform access;
- Withholding of pending payouts where contractually permitted;
- Permanent termination of engagement;
- Reporting to appropriate regulatory or professional authorities where required;
- Initiation of legal action where warranted.

Such actions shall be consistent with the Mentor Engagement Agreement and applicable law.

18.3 Vendors & Third Parties

Where a Data Processor or vendor:

- Fails to implement agreed safeguards;
- Breaches confidentiality obligations;
- Delays breach notification;
- Violates contractual data protection terms;

VMENTORZ may:

- Require corrective measures;
- Suspend data access;
- Terminate contractual arrangements;
- Pursue contractual remedies.

18.4 Proportionality & Documentation

Disciplinary measures shall be:

- Proportionate to the severity and impact of the violation;
- Documented where appropriate;
- Implemented in accordance with contractual and legal obligations.

19. Policy Review & Amendments

This Policy shall be reviewed periodically to ensure continued alignment with:



- Applicable laws and regulatory developments;
- Operational practices and infrastructure changes;
- Platform feature enhancements;
- Evolving cybersecurity risks;
- Business expansion into new geographies or service models.

19.1 Review Authority

The Data Protection Lead, in consultation with senior management where appropriate, shall be responsible for initiating and overseeing policy review.

Reviews may be conducted:

- On a periodic basis;
- Following material incidents;
- Upon regulatory developments;
- Prior to significant infrastructure or feature changes;
- Where audit findings indicate required updates.

19.2 Amendments

VMENTORZ reserves the right to amend, update, or revise this Policy as necessary to:

- Reflect changes in law or regulatory guidance;
- Strengthen security safeguards;
- Improve governance controls;
- Adapt to evolving business models.

Amendments shall take effect upon internal approval and documentation.

19.3 Documentation of Revisions

Material revisions to this Policy shall be:

- Documented in the Version Control section;
- Dated and approved by authorised personnel;
- Retained as part of governance records.

20. Version Control & Governance Record

This Policy shall be subject to structured version control and documented governance oversight.

20.1 Version Tracking

Each version of this Policy shall include:

- Version number;
- Effective date;
- Summary of material changes (where applicable);
- Approval authority.

No modification shall be treated as valid unless documented in accordance with this section.

20.2 Governance Record Retention

Previous versions of this Policy shall be retained as part of internal governance documentation for reference, audit, and compliance purposes.

Retention of prior versions shall be proportionate to regulatory and operational needs.

20.3 Approval Authority

This Policy and subsequent amendments shall be approved by authorised leadership of VMENTORZ, including the Data Protection Lead and/or designated senior management.

Approval records may be maintained electronically.



20.4 Policy Accessibility

This Policy is an internal governance document.

Access shall be restricted to authorised personnel and may be shared externally only where:

- Required by law;
- Requested during due diligence;
- Required for vendor, investor, or regulatory review;
- Approved by authorised leadership.

Version History

Version	Effective Date	Summary of Changes	Approved By
1.0	January 29, 2026	Initial internal Data Protection Policy.	VMENTORZ Board / Management