Privacy and Security Policy

RiskaVaire GRC Platform

Company: Vardaan Data Sciences PVT LTD

Product: RiskaVaire - Governance, Risk & Compliance Platform

Address: Aurum, 1st Floor, Plot No 57, Jayabheri Enclave, Gachibowli Hyderabad-500032 INDIA

Email: info@vardaanglobal.com

Phone: +91 40-35171118, +91 40-35171119

Effective Date: 25/08/2025

Version: 1.0

1. Introduction and Scope

This Privacy and Security Policy governs the collection, use, processing, storage, and protection of personal and organizational data within the RiskaVaire Governance, Risk & Compliance (GRC) platform. This policy applies to all users, administrators, and stakeholders who access or interact with the RiskaVaire system.

Scope: This policy covers all data processed through RiskaVaire modules including Policy Management, Compliance Management, Audit Management, Incident Management, and Risk Management functionalities.

2. Data Collection and Processing

2.1 Types of Data Collected

Personal Data:

- User account information (username, email, phone number)
- Professional information (department, business unit, role, location)

- Authentication credentials and Multi-Factor Authentication data
- User activity logs and system interaction records

Organizational Data:

- Policy documents and frameworks
- Compliance records and audit findings
- Incident reports and risk assessments
- Business unit and departmental information
- Financial impact assessments and cost analyses

2.2 Data Collection Methods

Data is collected through:

- User registration and profile management
- Document uploads and AI-assisted content extraction
- System-generated logs and automated data capture
- Manual data entry through forms and interfaces
- Integration with external systems and frameworks

2.3 Legal Basis for Processing

Data processing is conducted based on:

- Contractual necessity for service provision
- Legitimate business interests in GRC management
- Compliance with legal and regulatory obligations
- User consent where explicitly provided

3. Data Security Measures

3.1 Technical Safeguards

Access Controls:

- Role-based access control with 22 predefined roles and customizable permissions
- Multi-Factor Authentication (MFA) for enhanced security
- Least-privilege access principles across all modules

Data Protection:

- End-to-end encryption for data in transit and at rest
- Secure API endpoints with authentication tokens
- Regular security patches and system updates

System Security:

- Network segmentation and firewall protection
- Intrusion detection and prevention systems
- Regular vulnerability assessments and penetration testing
- Security monitoring and incident response capabilities

3.2 Operational Safeguards

Access Management:

- Regular access reviews and privilege audits
- Segregation of duties for sensitive operations
- Audit trails for all user activities and data modifications

Data Handling:

- Secure data transmission protocols
- Controlled data export and download functions
- Data anonymization and pseudonymization where applicable
- Secure deletion procedures for obsolete data

4. Data Retention and Disposal

4.1 Retention Periods

- **User Account Data:** Retained for the duration of active subscription and more years as mentioned in the End user licensing agreement
- **Policy and Compliance Data, System Logs, Incident Reports, Audit Records:** Retained per regulatory requirements and organizational policies

4.2 Secure Disposal

Data disposal includes:

- Secure deletion using industry-standard methods
- Certificate of destruction for physical media

- Verification of complete data removal
- Documentation of disposal activities

5. User Rights and Controls

5.1 Data Subject Rights

Users have the right to:

- Access their personal data and processing activities
- Rectify inaccurate or incomplete information
- Request data portability in standard formats
- Withdraw consent where applicable
- Lodge complaints with supervisory authorities

5.2 User Controls

Profile Management:

- Update personal and business information
- Manage notification preferences (email, WhatsApp, platform alerts)
- Change passwords with email verification
- Request role changes through approval workflows

Data Access:

- View personal data through profile sections
- Download reports and documents as permitted by role
- Access audit trails of personal data processing

6. Third-Party Integrations and Sharing

6.1 Data Sharing

Data may be shared with:

- Authorized third-party service providers for platform functionality
- External auditors as required for compliance verification
- Regulatory bodies as mandated by law
- Business partners with explicit user consent

6.2 Third-Party Security

All third-party integrations must:

- Maintain equivalent security standards
- Sign data processing agreements
- Undergo regular security assessments
- Provide transparency in data handling practices

7. Incident Management and Breach Response

7.1 Security Incident Response

In case of security incidents:

- Immediate containment and impact assessment
- Notification to affected users within 72 hours
- Regulatory reporting as required by law
- Forensic investigation and remediation measures
- Post-incident review and system improvements

7.2 Data Breach Procedures

- **Detection:** Automated monitoring and manual reporting mechanisms
- **Assessment:** Impact evaluation and risk classification
- **Containment:** Immediate steps to prevent further data exposure
- **Notification:** Timely communication to users and authorities
- **Recovery:** System restoration and security enhancement

8. AI and Automated Processing

8.1 AI Data Processing

The RiskaVaire platform uses AI for:

- Automated policy and framework content extraction
- Risk analysis and predictive assessments
- Compliance gap identification
- Incident impact analysis and mitigation suggestions

8.2 AI Governance

- Transparency in AI decision-making processes
- Human oversight for critical determinations
- Regular algorithm auditing and bias testing
- User notification of automated processing activities

9. International Data Transfers

9.1 Cross-Border Transfers

When data is transferred internationally:

- Adequate protection measures are implemented
- Standard Contractual Clauses (SCCs) are executed
- Data localization requirements are respected
- Users are informed of transfer destinations and safeguards

9.2 Data Sovereignty

- Data residency options based on customer requirements
- Compliance with local data protection laws
- Regular assessment of international transfer mechanisms

10. Training and Awareness

10.1 Staff Training

All personnel receive:

- Initial privacy and security training
- Regular updates on policy changes
- Role-specific security awareness sessions
- Incident response training and exercises

10.2 User Education

Users are provided with:

- Privacy policy explanations and guides
- Regular security awareness communications

- Self-service privacy management tools

11. Contact Information and Complaints

11.1 Data Protection Officer

For privacy-related inquiries:

- **Email:** info@vardaanglobal.com
- **Phone:** +91 40-35171118
- **Address:** Aurum, 1st Floor, Plot No 57, Jayabheri Enclave, Gachibowli Hyderabad-500032 INDIA

11.2 Complaint Resolution

Users may:

- Contact our Data Protection Officer directly
- Use the platform's built-in support features
- Escalate to relevant supervisory authorities
- Seek legal remedies as provided by applicable law

12. Policy Updates and Notifications

12.1 Policy Changes

- Material changes require 30 days advance notice
- Users will be notified through email and platform notifications
- Continued use constitutes acceptance of updated terms
- Previous versions maintained for reference

12.2 Regular Review

This policy is reviewed:

- Annually or as required by regulatory changes
- Following significant security incidents
- Upon major platform updates or feature additions
- Based on user feedback and compliance requirements

13. Regulatory Compliance

13.1 Applicable Laws

This policy ensures compliance with:

- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- Personal Data Protection Bill (when enacted)
- General Data Protection Regulation (GDPR) for EU users
- Other applicable international privacy laws

14. Law Enforcement and Government Requests

14.1 Compliance with Legal Requests

We may disclose personal or organizational data to law enforcement authorities, regulatory bodies, or government agencies when required by applicable law, regulation, legal process, or enforceable governmental request.

14.2 Safeguards and Transparency

Where legally permissible, we will notify affected users or organizations of such requests prior to disclosure. We will ensure that any disclosure is limited to the minimum information necessary to comply with the request.

14.3 Challenging Unlawful Requests

If we reasonably believe that a request for information is unlawful, overbroad, or not properly authorized, we reserve the right to challenge or refuse such requests, to the extent permitted by law.

15. Liability and Limitations

15.1 Platform Responsibility

We implement industry-standard technical and organizational measures to protect data. However, no system can be guaranteed to be completely secure.

15.2 User Responsibilities

Users are responsible for:

- Maintaining the confidentiality of their login credentials and authentication methods.
- Ensuring accuracy and legality of the data they upload or process through the platform.
- Using the platform in compliance with applicable laws and organizational policies.

15.3 Limitations of Liability

- To the maximum extent permitted by applicable law, Vardaan Data Sciences Pvt. Ltd. shall not be held liable for:
- Loss or damage resulting from unauthorized access due to user negligence (e.g., weak passwords, sharing credentials).
- Incidents or breaches caused by third-party integrations, applications, or services not under our direct control.
- Indirect, incidental, or consequential damages arising from the use or inability to use the platform.

16. Governing Law and Jurisdiction

16.1 Applicable Law

This Privacy and Security Policy shall be governed by and construed in accordance with the laws of India, without regard to its conflict of laws principles.

16.2 Dispute Resolution

Any disputes, controversies, or claims arising from or relating to this Policy shall first be attempted to be resolved amicably through good-faith negotiations.

16.3 Jurisdiction

In the event that disputes cannot be resolved amicably, they shall be subject to the exclusive jurisdiction of the competent courts located in Hyderabad, Telangana, India.

Acknowledgment: By using the RiskaVaire platform, users acknowledge that they have read, understood, and agree to be bound by this Privacy and Security Policy.

Document Control:

- **Prepared by:** Vardaan Data Sciences Legal and Compliance Team
- **Approved by:** Chief Privacy Officer
- **Distribution:** All RiskaVaire Users and Stakeholders