

TETRIX LABS LIMITED

JOROMI AI

PRIVACY POLICY

This Privacy Policy explains how Tetrix Labs collects, uses, discloses, retains, and protects personal data in connection with JOROMI AI, its Enterprise AI Operating System.

Enterprise Privacy Policy

Prepared for Enterprise Customers, Regulators, and Compliance Review

Effective Date: 14th July 2026

1. Introduction

Tetrix Labs (“Tetrix Labs,” “we,” “us,” or “our”) develops and operates JOROMI AI, an Enterprise AI Operating System that unifies AI models, autonomous agents, workflow automation, enterprise search, knowledge management, document intelligence, business intelligence, analytics, governance, and cloud infrastructure into a single governed platform (the “Services” or the “Platform”). This Privacy Policy (the “Policy”) explains how we collect, use, disclose, retain, transfer, and protect personal data in connection with the Platform, our websites, our developer tools, and our related enterprise services.

Privacy is treated as a design requirement of JOROMI AI, not an afterthought. Because the Platform processes enterprise, government, and regulated-industry data at scale — including data generated through AI agents, workflow automation, and retrieval-augmented generation — we apply the following commitments across the Platform:

- **Privacy by Design:** Data protection principles are incorporated into the architecture and default configuration of every module, from the AI Agent Studio to the Governance Center.
- **Security by Design:** Technical and organizational safeguards are built into the Platform's infrastructure, identity, and access control layers rather than layered on after deployment.
- **Responsible AI:** AI processing on the Platform is governed by defined policies covering human oversight, transparency, explainability, and model governance, as described in Section 7 (AI Processing).
- **Data Governance:** Enterprise customers retain control over their organizational data through workspace-level configuration, retention policies, and administrative controls, as described in Section 15 (Enterprise Administration).
- **Transparency:** This Policy is written to be understood by the enterprise procurement teams, compliance officers, regulators, and individual users who rely on it, without sacrificing legal precision.
- **Enterprise Trust and Accountability:** We maintain internal accountability structures, documented data processing records, and contractual commitments — including Data Processing Agreements — to support enterprise customers' own compliance obligations.

Who This Policy Covers

This Policy applies to personal data processed by Tetrix Labs in connection with JOROMI AI. It does not govern the content, policies, or practices of third-party websites, applications, or integrations that enterprise customers may connect to the Platform, which are governed by those third parties' own terms and privacy notices.

2. Scope

This Policy applies to personal data processed by Tetrix Labs in the course of operating JOROMI AI and related services, across the following categories of individuals:

Category	Description
----------	-------------

Enterprise Customers	Organizations that have entered into an agreement with Tetrrix Labs to access JOROMI AI, and the individuals within those organizations who administer or configure the Platform.
Business Users	Employees, contractors, and agents of an enterprise customer who use the Platform under that organization's tenant.
Website Visitors	Individuals who visit our public websites, including prospective customers and members of the public.
Trial Users	Individuals who register for a trial, demonstration, or evaluation of the Platform.
API Developers	Individuals and organizations who access JOROMI AI through the API Platform or Developer Platform.
Marketplace Users	Individuals and organizations who publish, distribute, or install agents, workflows, or connectors through the AI Marketplace.
Partners	Technology, implementation, and channel partners who collaborate with Tetrrix Labs on the deployment or distribution of the Platform.
Vendors, Contractors, and Consultants	Individuals engaged by Tetrrix Labs to support the development, operation, or delivery of the Platform.
Event Attendees	Individuals who register for or attend webinars, conferences, or other events hosted or sponsored by Tetrrix Labs.
Job Applicants	Individuals who apply for employment or engagement with Tetrrix Labs, where applicable and subject to separate recruitment privacy notices.

Where an enterprise customer deploys JOROMI AI to process personal data belonging to its own employees, customers, or other individuals ("Customer Data"), that enterprise customer — not Tetrrix Labs — is generally responsible for providing appropriate notice to those individuals, as described further in Section 18 (Data Controllers and Processors).

3. Definitions

For the purposes of this Policy, the following terms have the meanings set out below. Capitalized terms not defined in this Policy have the meanings given to them in the applicable customer agreement.

Term	Definition
Personal Data / Personal Information	Any information relating to an identified or identifiable natural person, used interchangeably in this Policy to reflect terminology used across applicable data protection laws.

Sensitive Data	Categories of personal data subject to heightened protection under applicable law, including data revealing racial or ethnic origin, health data, biometric data, financial account credentials, and government identifiers.
Customer Data	Data, content, and materials — including documents, prompts, records, and workflow inputs — submitted to or processed by the Platform by or on behalf of an enterprise customer.
Term	Definition
Enterprise Data	Customer Data together with configuration, workspace, and administrative data associated with an enterprise customer's tenant.
AI Data	Data generated or processed in connection with AI functionality on the Platform, including Prompts, AI Output, retrieval results, and agent execution records.
Processing	Any operation performed on personal data, including collection, recording, storage, use, disclosure, and deletion.
Controller	The entity that determines the purposes and means of processing personal data.
Processor	The entity that processes personal data on behalf of, and under the instructions of, a Controller.
Subprocessor	A third party engaged by a Processor to assist in processing personal data on behalf of a Controller.
Services / Platform	JOROMI AI and its constituent modules, including the AI Agent Studio, Enterprise Workflow Automation, Enterprise Search, Knowledge Management, Document Intelligence, Business Intelligence, Analytics, Governance Center, Compliance Center, Risk Intelligence, Identity & Access Management, Secure Collaboration, API Platform, Cloud Infrastructure, and Developer Platform.
Cookies	Small data files placed on a device by a website or application, as further described in Section 9 (Cookies).
Metadata	Data describing other data, such as the time, source, size, or type of a file, message, or transaction.
Usage Data	Data generated through interaction with the Platform, including login events, feature usage, session duration, and navigation patterns.
Prompt	Any instruction, query, or input submitted by a user to an AI model or AI agent on the Platform.

AI Output	Any content, recommendation, decision, or result generated by an AI model or AI agent in response to a Prompt or workflow trigger.
Model	An AI or machine learning model made available through the Platform, whether developed by Tetrix Labs or a third-party model provider.
Workspace	A logically segregated environment within the Platform associated with a particular enterprise customer or team.
Tenant	The isolated instance of the Platform, including configuration, data, and access controls, provisioned for a particular enterprise customer.
Authorized User	An individual authorized by an enterprise customer to access the Platform under that customer's account.

4. Categories of Data Collected

We collect and process the following categories of data in connection with the Platform. The specific categories applicable to a given individual depend on how they interact with the Platform — for example, as a business user, a website visitor, or an API developer.

Identity and Contact Data

- Identity Data — name, job title, employer, and professional role
- Contact Data — email address, business address, and telephone number
- Authentication Data — credentials, single sign-on identifiers, and multi-factor authentication data

Business and Enterprise Data

- Business Data — organization name, industry, business size, and commercial relationship details
- Enterprise Knowledge Bases — documents and records an enterprise customer uploads or connects to the Platform's Knowledge Layer
- Workflow Data — process configurations, triggers, approvals, and execution records within Enterprise Workflow Automation
- Agent Configurations — roles, permissions, and settings assigned to AI agents built in the AI Agent Studio

AI Interaction Data

- Prompt Data — the content of Prompts submitted by users to AI models and agents
- AI Conversation History — records of interactions between users and conversational AI features
- Uploaded Documents — files submitted for Document Intelligence, search indexing, or knowledge management
- API Requests and API Responses — data transmitted through the API Platform, including payloads and response content

Technical and Security Data

- Device Information — device type, operating system, and unique device identifiers
- Network Information — IP address, connection type, and approximate location derived from network data
- Browser Data — browser type, version, and language settings
- Security Data — access logs, authentication attempts, and security event records
- Integration Metadata — identifiers and configuration data associated with connected third-party systems

Usage and Diagnostic Data

- Usage Data — feature interactions, session activity, and navigation patterns
- Diagnostic Information and Crash Reports — technical data generated when the Platform encounters an error
- Telemetry — performance and operational data collected to monitor Platform health
- Audit Logs and Compliance Records — records of user, agent, and administrative activity retained for governance and audit purposes

Commercial and Support Data

- Billing Data and Payment Information — invoicing details and payment card or bank data, processed via our payment processors
- Customer Support Records — correspondence, tickets, and related records arising from support requests
- Marketing Preferences — communication preferences and consent records
- Event Registrations — registration and attendance data for webinars, conferences, and similar events

Cookies and Analytics

- Cookies and similar tracking technologies, as described in Section 9 (Cookies)
- Analytics Data — aggregated and individual usage statistics collected through analytics tools

Sensitive Data

Enterprise customers are responsible for configuring the Platform appropriately and obtaining any legally required consents or authorizations before submitting Sensitive Data to the Platform. Tetrix Labs does not request Sensitive Data as a condition of providing the Services and applies heightened access controls to any Sensitive Data that customers elect to process on the Platform.

5. Sources of Data

We collect data from the following sources:

- **Directly from Users:** Data provided when registering for an account, configuring a Workspace, submitting a Prompt, uploading a document, or contacting support.
- **From Enterprise Customer Organizations:** Data provided by an enterprise customer's administrators in the course of provisioning, configuring, and managing a Tenant, including data about Authorized Users.
- **Through Integrations and APIs:** Data received from connected ERP, CRM, HR, finance, productivity, and data warehouse systems that an enterprise customer configures to work with the Platform.
- **From Devices:** Technical data automatically collected from the devices used to access the Platform.
- **Through Cookies and Similar Technologies:** Data collected through cookies and tracking technologies deployed on our websites and, where applicable, within the Platform interface.
- **From Service Providers:** Data received from vendors that support our operations, such as identity verification, payment processing, and analytics providers.
- **From Public Sources:** Publicly available business information, such as company registries, used to support account verification and enterprise onboarding.
- **From Customer Administrators:** Access permissions, role assignments, and account status information configured by an enterprise customer's designated administrators.

6. How Data Is Used

We process personal data for the following purposes, each grounded in a lawful basis as described in Section 8 (Legal Bases):

1. Providing AI inference, enterprise search, and knowledge retrieval functionality
2. Operating AI agents and executing multi-step agent workflows
3. Executing and orchestrating Enterprise Workflow Automation processes
4. Authenticating users and verifying identity for account access
5. Administering Tenants, Workspaces, and user permissions
6. Detecting, investigating, and preventing fraud and abuse of the Platform
7. Monitoring for security threats and responding to security incidents
8. Maintaining and improving Platform performance, reliability, and functionality
9. Complying with applicable legal, regulatory, and contractual obligations
10. Managing customer support requests and resolving technical issues
11. Optimizing and personalizing the Platform experience for Authorized Users
12. Generating aggregated and de-identified insights to improve product quality
13. Communicating with customers, prospects, and event attendees regarding the Services
14. Processing billing, invoicing, and payment transactions
15. Enforcing our terms of service, this Policy, and applicable agreements

7. AI Processing

Because JOROMI AI is an AI-native platform, this section describes in detail how data is processed by AI models, agents, and related functionality, and the governance controls that apply to that processing.

Prompt Processing and AI Inference

When a user submits a Prompt, the Platform transmits the relevant content — together with any retrieved knowledge context — to the applicable Model for inference. The resulting AI Output is returned to the user and, depending on Workspace configuration, may be logged for audit, quality, and governance purposes.

Retrieval-Augmented Generation and Enterprise Knowledge Retrieval

Where Retrieval-Augmented Generation (RAG) is used, the Platform retrieves relevant content from an enterprise customer's connected Enterprise Knowledge Bases and provides it to the Model as context for generating a response. Retrieval respects the access permissions configured within the customer's Tenant, so that results reflect only the data a given user is authorized to access.

AI Memory

Certain agent and copilot features may retain contextual information across a session, or across sessions where configured by an enterprise customer, to support continuity in multi-step tasks. AI Memory settings are configurable at the Workspace level, including retention duration and scope.

AI Agent Execution

AI agents built through the AI Agent Studio may take actions within connected enterprise systems, subject to the permissions and guardrails configured by the enterprise customer. Agent activity is logged in the Governance Center and subject to the human oversight and approval controls described in Section 15 (Enterprise Administration).

Human Review

Enterprise customers may configure human-in-the-loop approval gates for sensitive agent actions or AI-generated decisions. Tetrix Labs personnel do not routinely review Customer Data or AI Output, except as necessary to provide support requested by the customer, to investigate suspected abuse or security incidents, or as required by law.

Hallucination Limitations and Customer Responsibility

AI Output is generated probabilistically and may contain inaccuracies, omissions, or content that does not reflect the underlying source data (commonly referred to as “hallucination”). Enterprise customers and Authorized Users are responsible for reviewing AI Output before relying on it for decisions with legal, financial, medical, or other significant consequences, and JOROMI AI provides explainability and source-citation features to support that review.

AI Transparency and Human Oversight

The Platform's Governance Center maintains a registry of Models in use, tracks model version and approval status, and logs AI and agent activity to support transparency and auditability, consistent with the AI governance principles described in the JOROMI AI Enterprise Product Profile.

Model Training Commitment
Enterprise customer data — including Prompts, Customer Data, and AI Output — is never used to train public or general-purpose AI models unless the customer has explicitly agreed to such use in writing. Where an enterprise customer's Model is fine-tuned on its own data, that fine-tuned Model and its underlying data remain within the customer's Tenant and are not used to train models made available to other customers.

8. Legal Bases for Processing

Where applicable data protection law requires a lawful basis for processing personal data, we rely on the following bases, which may vary by jurisdiction and processing activity:

Framework	Lawful Bases Relied Upon
EU GDPR	Performance of a contract, compliance with a legal obligation, legitimate interests (including Platform security and product improvement), and consent where required, such as for certain cookies and marketing communications.
UK GDPR	The same lawful bases as under the EU GDPR, as implemented under the UK's domestic data protection framework.
Nigeria Data Protection Act (NDPA)	Consent, performance of a contract, compliance with legal obligations, and legitimate interests, consistent with the lawful bases recognized under the NDPA.
California Consumer Privacy Act (CCPA/CPRA)	Processing as necessary to provide the Services requested, and other purposes disclosed at or before collection, subject to applicable consumer rights described in Section 14.
Brazil LGPD	Performance of a contract, compliance with legal obligations, legitimate interests, and consent where required under the LGPD.
Other Applicable Laws	Where other data protection laws apply, we rely on the equivalent lawful bases available under those laws, applied consistently with the principles described in this section.

9. Cookies

We and our service providers use cookies and similar tracking technologies on our websites and, in limited cases, within the Platform interface, for the following purposes:

- **Necessary Cookies:** Required for core website and Platform functionality, such as authentication and session management. These cannot be disabled without affecting functionality.
- **Functional Cookies:** Support user preferences, such as language and display settings, to improve the user experience.
- **Analytics Cookies:** Collect aggregated information about how visitors use our websites, helping us understand and improve performance.
- **Performance Cookies:** Measure load times, error rates, and other technical metrics to support Platform reliability.

Where required by applicable law, we obtain consent for non-essential cookies through a consent management mechanism presented at first visit. Users may adjust cookie preferences at any time through our cookie settings tool or their browser controls; disabling certain cookies may limit website or Platform functionality.

10. Data Sharing

We share personal data only as necessary to provide and support the Services, and only with the categories of recipients described below:

Recipient Category	Purpose of Sharing
Cloud Infrastructure Providers	Hosting, storage, and compute services underlying the Platform's Infrastructure Layer.
AI Infrastructure and Model Providers	Provision of AI inference services for Models made available through the AI Layer, subject to the model training commitment in Section 7.
Payment Processors	Processing of billing and payment transactions for paid Services.
Security Vendors	Threat detection, vulnerability management, and incident response support.
Auditors	Independent verification of security, financial, and compliance controls.
Regulators and Public Authorities	Disclosure where required by applicable law, regulation, court order, or lawful government request.
Legal Advisers	Support in connection with legal proceedings, corporate transactions, or regulatory matters.
Customer-Authorized Integrations	Third-party systems and applications that an enterprise customer configures to connect with the Platform, at that customer's direction.
No Sale of Personal Information Tetrix Labs does not sell personal information, and does not share personal information in exchange for monetary or other valuable consideration in a manner that would constitute a “sale” or “share” under applicable law.	

Where required by law, we enter into data processing agreements or equivalent contractual safeguards with third parties who process personal data on our behalf, obligating them to protect that data consistently with this Policy and applicable law.

11. International Data Transfers

JOROMI AI is deployed globally, and personal data may be transferred to, stored in, and processed in countries other than the country in which it was originally collected, including countries that may not have data protection laws equivalent to those of the origin country. Where such transfers occur, we apply the following safeguards, as applicable:

- **Standard Contractual Clauses (SCCs):** Used for transfers of personal data originating in the European Economic Area to countries not subject to an adequacy decision.
- **UK International Data Transfer Addendum:** Used alongside the SCCs to extend equivalent protections to transfers of personal data originating in the United Kingdom.
- **Adequacy Decisions:** Relied upon for transfers to countries recognized as providing an adequate level of data protection by the relevant regulatory authority.
- **Encryption in Transit:** Applied to data transferred across networks and jurisdictions to protect confidentiality during transmission.
- **Regional Hosting and Data Residency:** Available for enterprise customers with specific data residency requirements, allowing Tenant data to be hosted within a designated region, subject to contractual agreement.
- **Cross-Border Governance Controls:** Access to data across regions is governed by the same Identity & Access Management and audit logging controls that apply within a single region.

12. Security

We maintain a comprehensive information security program designed to protect personal data against unauthorized access, disclosure, alteration, and destruction, incorporating the following measures:

Access and Identity Controls

- Encryption of data in transit (TLS) and at rest
- Zero Trust network architecture with continuous verification
- Multi-factor authentication (MFA) for administrative and user access
- Centralized Identity and Access Management (IAM)
- Role-based access control (RBAC) enforced at the field and module level

Monitoring and Response

- Continuous security monitoring and logging across the Platform
- Formal incident response procedures with defined escalation paths
- Regular penetration testing by qualified internal or third-party assessors
- Ongoing vulnerability management and patch management processes

Resilience and Assurance

- Disaster recovery and business continuity planning, including backup and failover procedures
- Vendor and subprocessor security assessments prior to onboarding
- Secure software development lifecycle (SSDLC) practices applied to Platform engineering
- Periodic internal review of security controls against recognized frameworks

No system can guarantee absolute security. In the event of a security incident affecting personal data, we will notify affected enterprise customers and, where required by applicable law, relevant regulators and individuals, in accordance with our incident response procedures and contractual commitments.

13. Retention

We retain personal data for as long as necessary to provide the Services, fulfil the purposes described in this Policy, and comply with applicable legal, regulatory, and contractual obligations, applying the following principles:

- **Customer-Controlled Deletion:** Enterprise customers may configure retention and deletion settings for Customer Data within their Tenant, and may request deletion of Customer Data upon termination of their agreement, subject to the retention exceptions below.
- **Legal Holds:** Data subject to a legal hold, investigation, or litigation will be retained until the hold is lifted, notwithstanding a standard deletion request.
- **Regulatory Retention:** Certain data, such as billing and audit records, may be retained for the periods required by applicable tax, financial, or regulatory obligations.

- **Backup Retention:** Data may persist in encrypted backups for a limited period following deletion from production systems, consistent with our backup and disaster recovery schedules.
-
- **Secure Destruction:** Upon expiry of the applicable retention period, personal data is securely deleted or deidentified in accordance with our data destruction procedures.

14. User Rights

Subject to applicable law and the exceptions and limitations provided therein, individuals may have the following rights with respect to their personal data:

Right	Description
Access	Request confirmation of whether we process personal data about you, and access to that data.
Rectification	Request correction of inaccurate or incomplete personal data.
Erasure	Request deletion of personal data, subject to the retention principles in Section 13.
Restriction	Request that we limit the processing of personal data in certain circumstances.
Portability	Request a copy of personal data in a structured, commonly used, machine-readable format.
Objection	Object to processing based on legitimate interests, including for direct marketing purposes.
Automated Decision Making	Request information about, and in certain cases object to, decisions made solely through automated processing that produce legal or similarly significant effects.
Consent Withdrawal	Withdraw consent at any time, where processing is based on consent, without affecting the lawfulness of processing before withdrawal.
Complaint	Lodge a complaint with a competent data protection authority.

Where an individual's personal data is processed by JOROMI AI as Customer Data on behalf of an enterprise customer, requests to exercise these rights should generally be directed to that enterprise customer in the first instance, as described in Section 18 (Data Controllers and Processors). Where Tetrix Labs is the appropriate party to respond, requests may be submitted using the contact details in Section 21.

15. Enterprise Administration

Enterprise customers access JOROMI AI through administrator accounts with elevated permissions over their Tenant. Enterprise administrators may, consistent with their organization's internal policies and applicable law:

- Create, suspend, and remove Authorized User accounts within their Tenant
- Monitor Authorized User activity, including Usage Data and, where configured, AI Conversation History, for security, compliance, and operational purposes
- Configure data retention, access control, and AI governance policies applicable to their Workspace
- Access organizational Workspaces, Enterprise Knowledge Bases, and workflow configurations associated with their Tenant
- Manage Enterprise Data, including exporting or deleting data associated with their Tenant
- Configure integrations between the Platform and their organization's other enterprise systems

Because enterprise administrators may have visibility into an Authorized User's activity within the Platform, individuals using JOROMI AI under an enterprise account should refer to their employer's internal policies for information about how their activity may be monitored, in addition to this Policy.

16. Third-Party Services

JOROMI AI is designed to integrate with an organization's existing technology stack. Where an enterprise customer connects the Platform to third-party systems, the following applies:

- **Integrations and APIs:** Data exchanged between JOROMI AI and connected ERP, CRM, HR, finance, or other systems is transmitted according to the permissions configured by the enterprise customer.
- **Marketplace Apps:** Agents, workflows, and connectors published by third parties through the AI Marketplace are subject to the applicable third party's own terms and privacy practices, in addition to Marketplace review requirements.
- **External AI Models:** Where an enterprise customer elects to route Prompts to a third-party Model not hosted by Tetrix Labs, that Model provider's own data handling terms may apply to the extent disclosed to the customer.
- **Cloud Services:** Underlying cloud infrastructure providers process data as Subprocessors under contractual terms consistent with this Policy, as described in Section 10.

We encourage enterprise customers and Authorized Users to review the privacy practices of any third-party service connected to the Platform before enabling that integration.

17. Children's Privacy

JOROMI AI is an enterprise platform intended for business use by organizations and their Authorized Users, and is not directed to children. We do not knowingly collect personal data from individuals under the age of 16 (or the applicable minimum age under local law) other than in the ordinary course of an enterprise customer's internal use of the Platform, such as HR-related data processed by an enterprise customer in compliance with its own legal obligations. If

we become aware that we have inadvertently collected personal data from a child in violation of this section, we will take reasonable steps to delete that data.

18. Data Controllers and Processors

The parties' respective roles as Controller and Processor depend on the nature of the data and processing activity involved:

Data Type	Role of Tetrix Labs	Role of Enterprise Customer
Customer Data submitted to the Platform (e.g., Prompts, uploaded documents, workflow inputs)	Processor, acting on the enterprise customer's instructions	Controller, determining the purposes and means of processing
Account and billing data for the enterprise customer relationship	Controller	N/A — provides data as a data subject or on behalf of its personnel
Website visitor and marketing data	Controller	N/A
Employee and HR data processed by an enterprise customer using the Platform	Processor	Controller

Where Tetrix Labs acts as a Processor with respect to Customer Data, our processing is governed by a Data Processing Agreement (DPA) incorporated into the applicable enterprise customer agreement, which sets out the scope, duration, nature, and purpose of processing, together with the customer's instructions and our corresponding obligations. Enterprise customers seeking a copy of our standard DPA should contact us using the details in Section 21.

19. Compliance Framework

Our privacy and security program is designed to support alignment with recognized international data protection and information security frameworks. Except where an independent certification is expressly stated, references below describe our program's design objectives and should not be read as a claim of formal certification.

Framework	Relevance
EU GDPR / UK GDPR	Program designed to support compliance with core data protection principles, lawful processing, and data subject rights.
Nigeria Data Protection Act (NDPA)	Program designed to align with NDPA requirements applicable to our Nigerian operations and customers.
CCPA / CPRA (California)	Program designed to support applicable California consumer privacy rights and disclosure obligations.
Brazil LGPD	Program designed to align with LGPD principles applicable to processing involving Brazilian data subjects.
PIPEDA (Canada)	Program designed to align with Canadian federal privacy principles where applicable.
POPIA (South Africa)	Program designed to align with South African data protection principles where applicable.
ISO 27001 / ISO 27701	Information security and privacy information management practices are designed with reference to these standards.
SOC 2	Internal controls are designed with reference to SOC 2 trust services criteria.
NIST Cybersecurity Framework	Security program structured with reference to the NIST framework's core functions.
AI Governance Best Practices	AI-specific controls described in Section 7 are designed with reference to emerging international AI governance guidance.

Enterprise customers requiring specific compliance documentation, audit reports, or certification evidence as part of their procurement or due diligence process should contact us using the details in Section 21.

20. Policy Updates

We may update this Policy from time to time to reflect changes in our practices, the Platform, or applicable law. Material changes will be communicated through one or more of the following methods, as appropriate: a notice on our website,

an in-Platform notification, or direct communication to enterprise customer administrators. The “Effective Date” at the top of this Policy indicates when it was last revised. Where required by applicable law or by an enterprise customer’s agreement with us, we will provide advance notice of material changes and, where applicable, seek consent before the change takes effect. Continued use of the Platform following the effective date of an updated Policy constitutes acceptance of the changes, to the extent permitted by applicable law.

21. Contact Information

Questions, requests, or complaints regarding this Policy or our data practices may be directed to:

Function	Contact
Privacy Office	[Insert Privacy Office Email Address]
Data Protection Officer	[Insert DPO Name and Email Address, if applicable]
Legal Department	[Insert Legal Department Email Address]
Security Team	[Insert Security Team Email Address / security.txt link]
General Enquiries	[Insert General Contact Email Address]
Website	[Insert Website URL]
Registered Office	[Insert Registered Office Address]

Effective Date: [Insert Effective Date] | Version: [Insert Version Number]

JOROMI AI — The AI Operating System for Modern Enterprises.