SHFA AI
Privacy and Data Privacy Policy

Los Angeles, USA / Remote
Version: 1.0
Effective Date: Apr 29, 2026
Owner: Thanas Papa, Primary Compliance Owner and Security Owner
Reviewer / Approver: Michael Abehsera, Executive Approver
Status: Final

Introduction

SHFA AI LLC (“SHFA AI,” “Company,” “we,” “us,” or “our”) provides AI automation services through an AI-enabled software platform. This Privacy and Data Privacy Policy describes how SHFA AI collects, uses, stores, protects, shares, retains, and deletes personal data and customer-provided data processed through the SHFA AI platform, website, and related services.

This Policy serves as SHFA AI’s external-facing privacy policy and internal data privacy governance policy.

Scope

This Policy applies to personal data and customer-provided data processed by SHFA AI in connection with:

* The SHFA AI website and related forms or communications.

* The SHFA AI AI automation platform.

* User accounts, authentication, and administrative activity.

* Chat messages, user prompts, conversation history, AI outputs, metadata, and customer-provided datasets.

* Internal personnel, support, compliance, security, and vendor-management activities where personal data is processed.

This Policy applies to SHFA AI employees, contractors, administrators, and other authorized personnel who access or process personal data or customer-provided data on behalf of SHFA AI.

Company and Service Description

SHFA AI LLC is an IT company based in Los Angeles, USA that provides AI automation services. SHFA AI operates an AI-enabled software platform that allows users to interact with AI agents using natural language in order to query data sources such as databases and CSV data. The platform includes a user interface, backend request handling, AI agent processing, and user data storage and retrieval.

The service is designed to support controlled user access, secure data handling, and role-based administrative operations. SHFA AI uses managed cloud and software vendors to operate the platform. Render is used for application hosting and deployment, Supabase is used for database and authentication services, GitHub is used for source code management, and OpenAI is used for AI model inference.

Roles and Responsibilities

The following roles are responsible for privacy and data protection governance:

* Primary Compliance Owner and Security Owner: Thanas Papa, thanas@shfa.ai.

* IT Owner: Irvi Rrika, irvi@shfa.ai.

* HR / People Owner: Michael Abehsera, michael@shfa.ai.

* Executive Approver: Michael Abehsera, michael@shfa.ai.

The Security Owner is responsible for maintaining privacy and data security controls, reviewing privacy-relevant incidents, and coordinating compliance evidence. The IT Owner is responsible for technical implementation of system access, infrastructure, and data protection controls. The HR / People Owner is responsible for personnel-related privacy obligations where applicable. The Executive Approver is responsible for final approval of policy changes and major privacy governance decisions.

Types of Data Processed

SHFA AI may collect and process the following categories of data:

* Authentication data, including email address, first name, and last name.

* Account and profile information submitted by users or administrators.

* Chat messages, prompts, uploaded content, conversation history, and other customer-provided inputs.

* AI-generated outputs and related chat metadata.

* Customer-provided data needed to deliver AI automation services, including data submitted for natural-language query workflows.

* Application and system event data, including authentication events, administrative actions, access events, system errors, and operational activity.

* Support and business communications, including emails or messages exchanged with SHFA AI.

* Billing, contractual, and customer relationship information, where applicable.

SHFA AI does not intentionally require users to submit sensitive personal data unless the processing is expressly agreed, necessary for the requested workflow, or otherwise permitted under applicable law and contractual terms. Customers are responsible for ensuring that data submitted to the platform is lawful, accurate, and appropriate for the intended use.

Purpose of Processing

SHFA AI processes data for the following purposes:

* To provide, operate, maintain, and improve the AI automation platform.

* To authenticate users and manage account access.

* To process user prompts, customer-provided data, and workflow requests.

* To generate AI-assisted responses and automation outputs.

* To provide customer support and respond to inquiries.

* To maintain security, detect unauthorized activity, troubleshoot errors, and monitor operational performance.

* To manage vendors, subprocessors, contracts, compliance evidence, and internal controls.

* To comply with legal, regulatory, audit, accounting, and contractual obligations.

* To protect the rights, property, security, and availability of SHFA AI, customers, users, and third parties.

Legal Bases and Lawful Processing

Where applicable, SHFA AI processes personal data based on one or more lawful grounds, including:

* Performance of a contract or steps necessary before entering into a contract.

* Legitimate business interests, including service operation, security monitoring, fraud prevention, and product administration.

* Compliance with legal or regulatory obligations.

* Consent, where required by applicable law or where SHFA AI requests consent for a specific processing activity.

SHFA AI will apply privacy requirements according to the applicable contractual and legal context, including privacy requirements that apply based on customer location, data subject location, and the nature of the data processed.

Customer Data Ownership

Customer-provided data belongs to the customer or user. SHFA AI acts as a processor or service provider for customer-provided data where it processes such data on behalf of customers to deliver the AI automation service. SHFA AI uses customer-provided data only as necessary to provide the service, maintain security, comply with obligations, and perform activities authorized by the customer or applicable agreement.

SHFA AI does not sell customer-provided data. SHFA AI does not use customer data to train internal AI models.

AI Model Usage

SHFA AI uses third-party AI model providers, including OpenAI, to process user prompts and deliver AI automation functionality. Data shared with AI model providers is limited to what is necessary to provide the service and is handled according to applicable provider terms and contractual commitments.

AI outputs may be probabilistic and may require review. Customers and users are responsible for evaluating outputs before relying on them for legal, financial, medical, safety-critical, or other high-impact decisions.

Data Sharing and Subprocessors

SHFA AI may share data with vendors and subprocessors that support operation of the platform, subject to appropriate access, contractual, and security controls. Known vendors include:

* Render, for application hosting and deployment.

* Supabase, for database and authentication services.

* GitHub, for source code management and change management.

* OpenAI, for AI model inference.

SHFA AI evaluates vendors based on the nature of services provided, data processed, service criticality, and security posture before onboarding. Vendors that process customer or sensitive company data are assessed through the third-party risk management process and are expected to maintain appropriate organizational and technical controls.

Security Controls

SHFA AI implements administrative, technical, and organizational safeguards designed to protect personal data and customer-provided data. These controls include:

* Role-based access control for application and administrative access.

* Least privilege access restrictions for production infrastructure.

* Supabase Row Level Security, where applicable.

* Multi-factor authentication for administrative access where supported.

* Prohibition on shared accounts.

* Encryption in transit using TLS 1.2 or higher.

* Encryption of confidential data at rest using approved cryptographic controls.

* Logging of authentication events, administrative actions, system errors, and operational events.

* Operational monitoring and alerting for significant anomalies.

* Incident response procedures for detection, containment, remediation, and post-incident review.

* Managed database backup and recovery capabilities through Supabase.

Access to Data

Access to personal data and customer-provided data is granted based on job responsibilities and least privilege principles. Users are restricted to data associated with their own accounts unless a different customer-authorized access model applies. Privileged actions are restricted to authorized roles.

Administrative access to production infrastructure is limited to approved personnel. SHFA AI performs formal reviews of user access rights at least quarterly. Unauthorized or unnecessary access identified during review must be revoked promptly. Access to SHFA AI systems and data is revoked promptly upon termination of employment or contract, and involuntary termination access must be revoked within 24 hours.

Data Retention

SHFA AI retains personal data and customer-provided data for as long as SHFA AI has a legitimate business need for its use or as necessary to meet regulatory, legal, audit, security, contractual, or operational requirements. Personally identifiable information is deleted or de-identified as soon as it no longer has a business use, subject to legal holds and other lawful retention requirements.

Customer accounts and customer data are deleted within sixty (60) days of contract termination through manual data deletion processes, unless a separate agreement, legal obligation, security requirement, or documented legal hold requires retention. Customers may request deletion of their data from the platform, subject to applicable contractual, legal, security, backup, and audit requirements. Backups and logs may be retained for a limited period where deletion is not technically immediate, but such data remains subject to access controls and security protections.

Data Subject and Customer Rights

Depending on applicable law, individuals may have rights to:

* Request access to personal data.

* Request correction of inaccurate personal data.

* Request deletion of personal data.

* Request restriction of processing.

* Object to certain processing activities.

* Request portability of personal data.

* Withdraw consent where processing is based on consent.

* Lodge a complaint with a competent supervisory authority.

Customers and users may submit privacy requests using the contact information in this Policy. SHFA AI will respond according to applicable law, identity verification requirements, contractual obligations, and operational constraints.

International Data Transfers

SHFA AI may process and transfer data through cloud infrastructure and vendors located outside the user's jurisdiction. Where required by applicable law, SHFA AI will use appropriate transfer safeguards, contractual terms, vendor due diligence, and technical protections to support lawful international data transfers.

Incident Response and Breach Notification

SHFA AI maintains incident response procedures for identifying, triaging, containing, remediating, and reviewing security incidents. Security-relevant logs and operational monitoring support investigations. If SHFA AI determines that a security incident affects personal data or customer-provided data, SHFA AI will evaluate notification obligations under applicable law and customer agreements.

Legal and executive staff determine whether external breach reporting or communications are required. Breaches are reported to customers, consumers, data subjects, and regulators without undue delay and

in accordance with contractual commitments and applicable law. Personnel may not disclose information regarding incidents or potential breaches to unauthorized third parties without approval from legal and/or executive management.

Privacy by Design and Personnel Responsibilities

SHFA AI personnel must handle personal data and customer-provided data according to this Policy, applicable security policies, contractual obligations, and the principle of least privilege. Employees and applicable third parties with administrative or privileged technical access to SHFA AI production systems and networks complete security awareness training at onboarding and annually thereafter.

Privacy and security considerations are incorporated into system design, vendor onboarding, change management, incident response, and customer support workflows.

Children’s Privacy

The SHFA AI platform is intended for business and professional use. SHFA AI does not knowingly collect personal data from children without appropriate authorization. If SHFA AI becomes aware that it has collected personal data from a child in violation of applicable law or platform terms, it will take appropriate steps to delete or restrict such data.

Changes to this Policy

SHFA AI may update this Policy periodically to reflect changes in services, vendors, legal obligations, or security controls. Material changes are reviewed by the Security Owner and approved by the Executive Approver before publication or formal adoption.

Contact

Privacy and data protection questions may be directed to:

SHFA AI LLC

Los Angeles, USA

Website: https://shfa.ai/

Primary Compliance and Security Contact: Thanas Papa, thanas@shfa.ai