



# Flintworks — Privacy Policy

Version 1.0 | Effective: March 1, 2026 | flintworks.ai

## Privacy Policy

Version 1.0 | Effective: March 1, 2026

### Table of Contents

---

1. Introduction
2. Data Controller
3. Personal Data We Collect
4. How We Use Your Data
5. Legal Basis for Processing
6. Data Sharing and Third Parties
7. International Data Transfers
8. Data Retention
9. Your Rights
10. Cookies
11. Children's Privacy
12. Jurisdiction-Specific Provisions
13. Changes to This Policy
14. Contact

### 1. Introduction

---

This Privacy Policy describes how we collect, use, store, and protect your personal data when you use our AI assistant management platform (“the Platform”).

Flintworks use a multi-tenant platform that enables businesses to create, deploy, and monitor AI-powered Digital Assistants. This policy applies to all users of the Platform, including account administrators, team members, and end-users who interact with Digital Assistants deployed through our service.

By using the Platform, you acknowledge that you have read and understood this Privacy Policy.

---

## 2. Data Controller

---

The data controller responsible for your personal data is:

- **Entity:** Flintworks
  - **Contact:** [privacy@flintworks.ai](mailto:privacy@flintworks.ai)
- 

## 3. Personal Data We Collect

---

We collect and process the following categories of personal data:

### 3.1 User Account Information

When you create an account on the Platform, we collect:

- Email address (used as your login identifier)
- First name and last name
- Password (stored as a secure hash, never in plain text)
- Authentication method (local, LDAP, SAML, or OAuth2)

### 3.2 Company Information (Client Account)

When registering an organization, we collect:

- Company name
- Corporate email address
- Authentication configuration preferences

### 3.3 End-User Contact Data

When end-users interact with Digital Assistants deployed through the Platform, we may collect:

- Channel session identifiers (e.g., WhatsApp, WebChat)
- Conversation metadata

### 3.4 AI Conversation and Workflow Data

To provide and improve the Platform's services, we process:

- Complete prompts sent to AI models
- AI model responses

- Model name and provider used
- Token usage and associated costs
- Workflow execution data and routing information

### 3.5 Technical and Security Data

- API keys (for platform authentication)
- Timezone preferences

### 3.6 Demo Request Data

When requesting a demo, we collect:

- Name, email address, and company name
- Message content
- Email verification code

Data Category	Examples	Purpose
User Account	Email, name, password hash	Authentication, account management
Company	Company name, corporate email	Multi-tenant organization
End-User Contacts	Channel session ID, metadata	Conversation tracking
AI Conversations	Prompts, responses, tokens, costs	Service delivery, monitoring
Technical	API keys, timezone	Security, user preferences
Demo Requests	Name, email, company, message	Sales and onboarding

## 4. How We Use Your Data

We use the personal data we collect for the following purposes:

- **Platform Operation and Authentication:** To provide, maintain, and secure your access to the Platform, including user authentication and session management.
- **AI Conversation Processing:** To process conversations with AI models on behalf of our clients and their end-users.
- **Digital Assistant Improvement:** Conversation data may be used to improve the quality of prompts and knowledge bases (RAG) for Digital Assistants. This does **not** involve training third-party AI models — data remains within the Flintworks platform.
- **Security and Abuse Prevention:** To detect, prevent, and respond to security incidents, fraud, and abuse of the Platform.

- **Aggregated Analytics:** To generate aggregated, anonymized metrics for service improvement. Individual users cannot be identified from these metrics.
- **Communication:** To respond to your inquiries, demo requests, and provide service-related notifications.

---

## 5. Legal Basis for Processing

---

We process your personal data based on the following legal grounds:

- **Contract Performance:** Processing necessary to provide the Platform services you have requested.
- **Legitimate Interest:** Processing for security, fraud prevention, and service improvement, where our interests do not override your rights.
- **Consent:** Where required by applicable law, we obtain your consent before processing (e.g., demo requests, marketing communications).
- **Legal Obligation:** Processing necessary to comply with applicable laws and regulations.

---

## 6. Data Sharing and Third Parties

---

We do **not** sell your personal data. We do **not** use third-party analytics or tracking tools. We do **not** display third-party advertisements.

We share data only in the following circumstances:

### AI Model Providers (LLM)

Conversation data is sent to third-party AI model providers for processing. The specific provider depends on the Digital Assistant configuration:

- **Consumer-facing assistants:** Flint selects the provider (currently Anthropic/Claude).
- **Custom assistants:** The client selects their preferred provider (Anthropic, OpenAI, Google, etc.).

Providers are selected based on security standards and responsible data handling practices. Data may be processed on the provider's servers (generally located in the United States).

We implement and continuously improve **data masking techniques** on sensitive information before it is processed by AI service providers, so that personally identifiable data is not exposed to third parties in plain text.

## Hosting Infrastructure

Our servers are located in San José, Costa Rica. Data is stored and transmitted with industry-standard encryption (TLS/HTTPS in transit, disk-level encryption at rest).

---

## 7. International Data Transfers

---

Our primary servers are located in **San José, Costa Rica**. However, when AI conversations are processed by third-party model providers, data may be transferred to servers in the United States or other jurisdictions where these providers operate.

We ensure that any such transfers are conducted with appropriate safeguards, including contractual commitments from providers to protect your data in accordance with applicable privacy laws.

---

## 8. Data Retention

---

We retain your personal data for as long as necessary to fulfill the purposes described in this policy:

- **Account data:** Retained for the duration of your account and for a reasonable period thereafter for legal compliance.
- **Conversation data:** Retained according to the client account's configuration and applicable data retention requirements.
- **Demo request data:** Retained for up to 12 months after the request, unless a business relationship is established.
- **Security logs:** Retained for up to 24 months for security and compliance purposes.

You may request deletion of your data at any time by contacting us (see Section 14).

---

## 9. Your Rights

---

Depending on your jurisdiction, you may have the following rights regarding your personal data:

- **Access:** Request a copy of the personal data we hold about you.
- **Rectification:** Request correction of inaccurate or incomplete data.
- **Deletion:** Request deletion of your personal data.
- **Portability:** Request your data in a structured, commonly used format.
- **Restriction:** Request that we limit the processing of your data.

- **Objection:** Object to certain types of data processing.
- **Withdraw Consent:** Where processing is based on consent, you may withdraw it at any time.

To exercise any of these rights, contact us at [privacy@flintworks.ai](mailto:privacy@flintworks.ai). We will respond within the timeframe required by applicable law.

---

## 10. Cookies

---

The Platform uses only **strictly functional cookies** required for proper operation:

- **sessionid** : Session management cookie for authenticated users.
- **csrftoken** : Security cookie for cross-site request forgery protection.

We do **not** use advertising cookies, analytics cookies, or any third-party tracking cookies. Because our cookies are strictly necessary for the Platform to function, no cookie consent banner is required.

---

## 11. Children's Privacy

---

The Platform is not intended for use by individuals under the age of 18. We do not knowingly collect personal data from minors. If you believe we have inadvertently collected data from a minor, please contact us immediately at [privacy@flintworks.ai](mailto:privacy@flintworks.ai), and we will promptly delete such data.

---

## 12. Jurisdiction-Specific Provisions

---

### 12.1 Costa Rica (Law 8968 / PRODHAB)

If you are located in Costa Rica, your personal data is protected under Law 8968 — Protection of Individuals Regarding the Processing of Their Personal Data. You have the right to access, rectify, delete, and object to the processing of your data. Complaints may be filed with the Agency for the Protection of Citizens' Data (PRODHAB).

### 12.2 Brazil (LGPD)

If you are located in Brazil, your data is protected under the Lei Geral de Proteção de Dados (LGPD). You have the rights of confirmation, access, correction, anonymization, portability, deletion, information about sharing, and the right to revoke consent. You may contact the National Data Protection Authority (ANPD) if you believe your rights have been violated.

### 12.3 Mexico (LFPDPPP)

If you are located in Mexico, your data is protected under the Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP). You have ARCO rights (Access, Rectification, Cancellation, and Opposition). To exercise these rights, contact us at [privacy@flintworks.ai](mailto:privacy@flintworks.ai).

### 12.4 United States (CCPA/CPRA)

If you are a California resident, the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) grant you additional rights, including the right to know what personal data we collect, the right to delete, and the right to opt-out of the sale of personal data. We do **not** sell personal data. To exercise your rights, contact us at [privacy@flintworks.ai](mailto:privacy@flintworks.ai).

### 12.5 Canada (PIPEDA)

If you are located in Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) governs how we handle your personal data. You have the right to access your personal information, challenge its accuracy, and withdraw consent. Complaints may be filed with the Office of the Privacy Commissioner of Canada (OPC).

---

## 13. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, or legal requirements. When we make material changes, we will notify you by updating the date at the top of this page and, where appropriate, providing additional notice (such as an email notification or an in-platform alert).

We encourage you to review this policy periodically.

---

## 14. Contact

If you have any questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us:

### Contact Information

- Email: [privacy@flintworks.ai](mailto:privacy@flintworks.ai)