# Privacy Policy

**Effective Date:** October 22nd, 2025

## Overview

Fundamental Research Labs is an AI research company working to build multi-agent systems. This Privacy Policy explains how we collect, use, disclose, and safeguard your personal data when you use **Shortcut**, our product and related services.

## Scope

This Privacy Policy applies to users of **Shortcut** via our websites, applications, and integrations.

## Information We Collect

### Personal Information

- Name
- Contact details (email)
- Account information required to create and manage your Shortcut account

### Automatically Collected Information

- IP address, browser type, and device information
- Session data (browser-level retention to enable core functionality, e.g. file retrieval) • Usage analytics (For Pro and Max users)

### Information from Other Sources

- Authentication data from OAuth providers (e.g., Google OAuth)

## Consent

By using Shortcut, you consent to the collection and processing of your data as described. If you do not agree, please discontinue use of the service.

## How We Use Your Information

We use your data for:

- **Service Delivery:** Authentication, session management, and enabling product features • **Communication:** Transactional updates, incident notifications, and service alerts •

**Customer Support:** Troubleshooting and addressing user inquiries

- **Security & Fraud Prevention:** Monitoring via real-time threat detection, anomaly logging, API call monitoring, and rate limiting

- **Legal & Compliance:** SOC 2 Type I, Type II adherence

- **Business Continuity:** Backups, disaster recovery, and failover across availability zones

**Data Sharing**

We may share your personal data only under these conditions:

- **Service Providers:** Third-party hosting, deployment, and AI model API vendors (all SOC 2 or equivalent certified, vetted for security compliance)

- **Enterprise Integrations:** With business partners under contractual obligations • **Legal Authorities:** If required by law or to comply with regulations • **Mergers/Acquisitions:** As part of a legitimate transaction

- **With Consent:** When explicitly authorized

**Data Transfers**

- All data is currently processed in **US-based data centers**

- Customers will be notified in advance of any changes in data location.

- We enforce strict security requirements for all vendors including relevant certifications and contractual data protection obligations

**Data Retention & Deletion**

- **User session data:** Retained for Pro/Max Users

- **AI model API calls:** Retained by providers up to 30 days (for safety monitoring)

- **Enterprise customers:** Zero Data Retention agreements, internally and with base LLM • **Customer data:** Pro/Max Opt-In Retention for Feedback

**Security Safeguards**

We implement multiple layers of protection:

- **Encryption:** AES-256 encryption at rest; TLS for data in transit .

- **Authentication:** Username/password with scrypt hashing, CSRF protection, rate

limiting, encrypted session management

• **Enterprise Options:** Google OAuth and SAML integration (on request) . • **Monitoring & Logging:** Real-time threat detection, audit trails

• **Backups & Recovery:** Daily automatic backups via third-party provider

• **Service Continuity:** Automatic failover across multiple APIs, load balancing, and dedicated incident response team

**Data Subject Rights**

You have the right to:

• Access your data

• Request correction

• Request deletion (“Right to be Forgotten”)

• Restrict processing

• Data portability

• Object to processing (including marketing)

• Withdraw consent

Requests may require identity verification.

**Cookies & Tracking**

Shortcut uses cookies for functionality and analytics. Non-essential cookies require your consent, which can be managed in your browser settings.

**Children**

Shortcut is **not directed at children under 16**. If we discover personal data has been collected from a child without parental consent, we will delete it promptly.

**Compliance**

Shortcut complies with SOC 2 Type I standards. We are in progress on our SOC 2 Type II audit.

**Updates to this Policy**

We may update this policy periodically. Any changes will be posted with a new effective date.

Continued use of Shortcut indicates acceptance.

## Google API Services User Data

This section outlines how Shortcut accesses, uses, stores, and shares user data received from Google APIs. Our use and transfer of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements.

**Data Accessed**: To provide its core functionality, Shortcut accesses the following specific data from your Google Account:

- **Google User Profile** (*userinfo.email*, *userinfo.profile*): We access your name and email address as provided by Google OAuth
- **Google Sheets** (*spreadsheets.currentonly*): We access, read, and write to the content of the single, active spreadsheet in which you are using the Shortcut add-on. We do not access any other files in your Google Drive
- **Google Apps Script** (*script.container.ui*, *script.external_request*): We use these scopes to display the add-on sidebar interface within Google Sheets and to connect to our external AI servers

**Data Usage**: We use this Google user data *only* for the following purposes:

- **Service Delivery**: Your name and email are used to create and manage your Shortcut account, authenticate you, and personalize the user interface
- **Core App Functionality**: Content from your active Google Sheet is read and sent to our AI service to process the command you initiated (e.g., "summarize this column"). The AI-generated result is then written back into your active sheet. This data is used solely to perform the task you request
- **Communication**: We use your email to send transactional updates and service alerts. We do not use your Google user data for advertising

**Data Sharing**: We may share Google user data *only* under these limited conditions:

- **Service Providers**: To perform the add-on's core function, we send the relevant data (e.g., text from your sheet) to our third-party AI model API vendors
- **Legal Requirement**s: We may disclose data if required by law or to comply with regulations
- We do not sell or share your Google user data with any other third parties for advertising or any other purpose

**Data Storage & Protection**: We handle all Google user data securely using multiple layers of protection:

- **Encryption**: All data, including Google user data, is encrypted in transit using TLS and at rest using AES-256 encryption
- **Secure Authentication**: We use Google OAuth for secure sign-in, and all user sessions are encrypted

**Data Retention & Deletion**: Our retention policy for Google user data is as follows:

- **Google Sheet Data**: We do not permanently store the content of your Google Sheets
- **Account Data**: We retain your Google-provided account information (name, email) for as long as you have an active Shortcut account
- **Deletion Process**: You have the right to request the deletion of your personal data at any time ("Right to be Forgotten"). To request data deletion, please email your request to privacy@fundamentalresearchlabs.com. We will verify your identity and promptly delete your personal account information from our systems

**Contact Us**

For questions, concerns, or data subject rights requests:

privacy@fundamentalresearchlabs.com