

Document reference: G-02 | Region: Global | Version: [TBD] | Effective date: [TBD]

WORKING DRAFT - PUBLICATION CONTROL: This document is drafted for the RedTree launch. Do not publish until the Global Compliance Matrix confirms the related launch implementation. Any text marked 'TBD BEFORE PUBLICATION' must be resolved and removed before release.

1. Scope and controller

This Global Privacy Policy explains how personal data is handled in connection with the RedTree website, application and services. Regional privacy appendices provide additional rights and legal information for the EU/EEA, United Kingdom, United States and India.

Controller: SIMG SASU, 37 avenue du Roule, , . Contact: contact@thesimg.com | +33 (0)1 59 58 01 53.

2. RedTree privacy principles

- RedTree does not sell personal data.
- RedTree does not use personal data for behavioural advertising or cross-context behavioural advertising.
- RedTree does not disclose personal data to third parties for their own independent marketing or unrelated commercial purposes.
- Personal data is disclosed to processors/service providers only where technically necessary to provide, secure, administer or support the service, or where the user initiates a connected service.
- RedTree does not use cookies, trackers, tracing technologies or analytics in the confirmed launch design.
- User content remains the user's content; SIMG processes it only as necessary to provide the requested RedTree functions and comply with law.

3. Categories of data

Category	Examples
Account and identity	Email address, display name, Firebase UID, authentication method. Passwords are handled by Firebase Authentication and are not stored by SIMG in readable form.
Subscription	Plan/feature access information, subscription identifiers, billing cycle, status,

Category	Examples
n and payment records	payment/webhook records. Full card details are handled by the payment provider, not stored by RedTree.
User content	Files, folders, filenames, notes, annotations, images, audio, transcriptions, text, metadata, structure/organisation, chat messages and other content deliberately imported, created or selected by the user.
AI context	Relevant file/folder names, dates, truncated or other text content made available to the AI feature, annotations, chat history and user messages, depending on the requested task and production implementation.
Technical/security data	Service events and diagnostic/security logs necessary to operate and protect RedTree. No separate analytics or crash-reporting system is currently used.
Connected-service data	Google Sign-In data and, when the user initiates Drive backup/sync, files and metadata needed for that function.

4. Purposes

- Create and manage RedTree accounts and authentication.
- Provide local, cloud, sync, backup, AI, transcription and other requested functionality.
- Manage subscriptions, payments, feature access and customer support.
- Protect the security, integrity and availability of RedTree and investigate technical failures or abuse.
- Comply with accounting, tax, legal and regulatory obligations and establish or defend legal claims.

The applicable legal bases differ by jurisdiction and are explained in the relevant regional privacy appendix.

5. Technical providers and disclosures

Provider / category	Purpose / data flow
Google Firebase / Google Cloud	Firebase Authentication; Firestore app data; Firebase Storage user backups; Cloud Functions; limited Firebase Hosting for payment redirect.
Google Sign-In / Google Drive	Authentication and optional user-initiated Drive backup/sync using the drive.file scope.

Provider / category	Purpose / data flow
API	
OpenAI API	AI processing of relevant user-selected or task-relevant context to return the requested analysis or intelligence.
Stripe	Payment processing, subscription and renewal management, invoicing and tax calculation. For users in the European Economic Area the contracting entity is Stripe Payments Europe, Limited, an Irish company.
PayPal	A payment method offered within the Stripe checkout. PayPal account credentials are not disclosed to RedTree.
SEPA Direct Debit	A payment method offered for euro-area subscriptions, routed through Stripe. The mandate and bank details are handled by Stripe.
Android / Google speech recognition	Voice-to-text processing when the user activates transcription.
Hostinger	Public RedTree website hosting.

OneDrive and Dropbox are not integrated in the confirmed launch architecture. Analytics and crash reporting are None unless the Global Compliance Matrix is updated before release.

6. Artificial intelligence

AI features operate only on a scope the user explicitly designates at the moment of the request. They do not run in the background, do not process the environment as a whole, and act on no initiative of their own. Within that scope, RedTree AI is designed to process sufficiently rich user context to perform the task requested by the user. The privacy boundary is purpose and subsequent use, not an artificial reduction of useful context. Data may therefore be sent to OpenAI where reasonably necessary to perform the requested AI function.

RedTree will not opt user content into voluntary model-training or data-sharing programmes, and does not authorise OpenAI to use RedTree customer content for advertising or unrelated independent exploitation. OpenAI states that API customer content is not used to train its models by default unless the customer opts in.

TBD BEFORE PUBLICATION: confirm the final production OpenAI retention setting, including whether Zero Data Retention is approved/used and which API endpoints are deployed.

7. Storage and locations

RedTree uses local device storage plus Google Firebase/Google Cloud services and optional user-initiated Google Drive backup. Cloud Functions are currently deployed in us-central1.

TBD BEFORE PUBLICATION: confirm the production Firestore and Firebase Storage regions and reflect them here and in the transfer register.

8. Retention and deletion

Retention depends on the type of data, the user's actions, contractual needs, legal obligations and technical backup cycles. Cancellation, downgrade or feature deactivation does not automatically delete user data. The Retention & Deletion Policy contains the operational rules.

9. Security

RedTree uses HTTPS/TLS for service communications. Google-hosted Firestore, Firebase Storage and Google Drive provide encryption at rest as part of their services. On-device SQLite metadata and preferences are not separately encrypted in the confirmed current build; a security review remains a launch/P2 control in the Compliance Matrix.

10. Rights and requests

Depending on the user's location, privacy law may provide rights of access, correction, deletion, portability/export, objection, restriction, withdrawal of consent or complaint. Requests can be submitted through the RedTree Data Rights page or to contact@thesimg.com. Identity or account-control verification may be required where reasonably necessary.

11. Age

RedTree is intended for users aged 18 or over and is not designed as a service for children.

12. No cookies, tracking or advertising

RedTree's confirmed launch design uses no cookies, trackers, tracing technologies, analytics or behavioural advertising. If that production behaviour changes, RedTree will update this Policy and any consent mechanism before activating a technology that legally requires it.

13. Changes and contact

Material changes will be reflected in the version register and, where required, notified to users. Contact: contact@thesimg.com | +33 (0)1 59 58 01 53.

Exporting content to other applications

RedTree lets a user send content to another application or service using the sharing functions of their device. Content sent this way is no longer under SIMG's control and is governed by the terms of the receiving service.