

Document reference: G-04 | 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 Do not publish until the Global Compliance Matrix confirms the related launch implementation.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. Purpose

This Policy describes how RedTree handles retention, recovery and deletion of account data and user content. It supplements the Global Privacy Policy.

2. Core rules

- Subscription cancellation is not account deletion.
- Downgrade or feature deactivation does not automatically delete user data.
- Where data becomes inaccessible because a feature/storage entitlement ends, RedTree provides at least 30 days for recovery/export before deletion can occur.
- Account deletion removes or anonymises data that no longer has a lawful retention purpose, subject to legal, accounting, security and claims-related retention.
- Deletion must be traceable without retaining deleted user content.

3. Local files

Files stored on the user's device remain under the user's control and are deleted when the user deletes them through the device/RedTree functionality. Local SQLite metadata and preferences are also subject to the account/content deletion design implemented at launch.

4. Firebase Storage and Google Drive backups

Firebase Storage backups and optional Google Drive backups are user-initiated. In the confirmed current implementation they are retained until the user deletes them; no automatic expiry is configured.

File deletion is intended to remove corresponding cloud copies on sync where the integration supports it. Backups may otherwise persist until explicitly deleted. The UI must explain any exception clearly.

5. Account deletion

At launch, account deletion must be available in-app and through a public web request mechanism. After verification where necessary, RedTree will delete or anonymise the account and associated data that is not required to be retained.

TBD BEFORE PUBLICATION: P1 implementation of in-app deletion and final deletion propagation/timing must be confirmed by dev.

6. Data export

At launch, RedTree must provide a genuine user-data export capability. Where downgrade/cancellation makes data inaccessible, the export/recovery window is at least 30 days.

TBD BEFORE PUBLICATION: P1 user-data export implementation, formats and scope must be confirmed by dev.

7. Processor and system propagation

Deletion must propagate, where legally and technically required, across Firestore, Firebase Storage, connected Google Drive data under RedTree control, relevant payment/subscription records and other processors. Data retained under a legal obligation must be isolated from normal service use.

TBD BEFORE PUBLICATION: final propagation map and processor-specific deletion mechanisms.

8. Payment and accounting records

Subscription IDs, payment/webhook records and accounting evidence may be retained for the periods required or permitted by tax, accounting, fraud-prevention and legal-claims rules. Full card details are handled by the payment provider and are not stored by RedTree.

9. Logs

Cloud Functions write diagnostic/error logs to Google Cloud Logging. Retention is set at the platform level. TBD BEFORE PUBLICATION: record the exact retention value applied in production.

10. AI processing retention

RedTree sends relevant context to OpenAI only to perform requested AI functionality. TBD BEFORE PUBLICATION: confirm the production OpenAI API retention/ZDR configuration and any endpoint-specific persistence before stating a final external retention period.

11. Security and backup residues

Deleted data may persist temporarily in technical backups or logs until their normal rotation/deletion, where such copies cannot reasonably be selectively edited. Restored backups must preserve or reapply valid deletion decisions where technically required.

12. Requests and proof

RedTree may request reasonable identity or account-control verification before executing a deletion or export request. SIMG may retain minimal evidence that a deletion request was executed, provided that evidence does not reconstruct deleted content.

13. Contact

contact@thesimg.com | +33 (0)1 59 58 01 53

Implementation status

TBD BEFORE PUBLICATION: in-app account deletion, deletion propagation to backups, and automatic backup expiry are not implemented as of 1 September 2026. The retention periods stated above must be confirmed against the deployed configuration before this policy is published, and the exact Cloud Logging retention value recorded.