

Data Deletion and Retention Policy

456Labs Inc. (Invoicefinito)

Effective date: June 20, 2026 | Version 1.0 | Next scheduled review: June 2027

1. Purpose

This Data Deletion and Retention Policy (“Policy”) defines how **456Labs Inc.** (“456Labs”, “we”, “us”, “our”) retains, deletes, and anonymizes personal information collected through **Invoicefinito** (the “Services”), including our mobile applications and website. It is designed to align with applicable data protection laws, including the EU/UK General Data Protection Regulation (GDPR), the California Consumer Privacy Act as amended by the CPRA (CCPA/CPRA), and the Personal Information Protection and Electronic Documents Act (PIPEDA) where relevant to our users in Canada.

2. Scope

This Policy applies to:

- Personal information we process about registered users of Invoicefinito.
- Data stored in our production systems, including Google Firebase (Authentication, Cloud Firestore, Cloud Storage, Cloud Functions) and integrated processors such as Plaid (optional bank connections) and Stripe (subscriptions and optional payment acceptance).
- Deletion requests initiated in the app and other privacy-related requests as described below.

This Policy supplements our [Privacy Policy](#) and user-facing [account deletion](#) instructions. If there is a conflict, this Policy governs retention and deletion practices; the Privacy Policy governs broader privacy disclosures.

3. Principles

- **Data minimization:** we retain personal information only for as long as necessary for the purposes described in our Privacy Policy or as required by law.
- **User control:** users can delete their account in the app and disconnect optional integrations (such as bank connections) without contacting support.
- **Security:** deletion is enforced through authenticated server-side processes, access controls, and scheduled purge jobs.
- **Transparency:** retention periods and deletion steps are published to users and reviewed periodically.

4. Retention schedule

The table below summarizes default retention periods for major categories of personal information while an account is active and after deletion is requested.

Data category	While account is active	After deletion request
Account & authentication (email, profile, sign-in metadata)	Retained while the account exists	Deactivated immediately on in-app deletion; authentication record permanently deleted on hard purge (see Section 5)
Business data (clients, invoices, expenses, time entries, projects, settings)	Retained while the account exists	Retained during 30-day grace period; permanently deleted on hard purge
Files (invoice PDFs, receipt images)	Retained while the account exists	Retained during grace period; storage prefix deleted on hard purge
Bank connection summaries & imported transactions (Plaid, optional)	Retained while connected or until account deletion	Disconnect removes Plaid access and connection credentials; all bank data deleted on hard purge
Subscription / billing entitlement records	Retained while needed to provide the subscription	Deleted on hard purge; store receipts may remain with Apple/Google
Encrypted backups & replicas	Per cloud provider cycles	Residual copies may persist up to 90 days after primary deletion
Aggregated or de-identified analytics	May be retained indefinitely	Not reasonably identifiable; not subject to erasure requests
Records required by law (tax, fraud, disputes)	As required by applicable law	Retained only for the legally required period and limited to compliance purposes

5. Account deletion process (enforced)

Account deletion is available only through the authenticated in-app flow described below. Users must sign in to delete their account.

5.1 In-app deletion

1. An authenticated user initiates deletion at **Settings** → **Account** → **Delete account**.
2. Our backend marks the user document with `status: deleted`, records the deletion reason (optional), and sets a **purgeAfter** timestamp **30 calendar days** in the future.
3. The user is signed out. Access to app data is blocked during the grace period except to restore the account or sign out.
4. If the user signs in within 30 days, they may tap **Restore account**, which clears the deletion marker.
5. A scheduled server job runs daily and permanently deletes accounts whose grace period has elapsed (“hard purge”).

5.2 Hard purge (permanent deletion)

On hard purge, we enforce deletion of:

- The Firebase Authentication user record.
- The entire Firestore subtree under `users/{uid}` (recursive delete), including clients, invoices, expenses, time entries, bank transactions, and related subcollections.
- All objects in Cloud Storage under `users/{uid}/`.
- Server-side Plaid items and access tokens; Plaid access is revoked via API where possible.
- Associated Stripe Connect accounts where configured, on a best-effort basis.

6. Partial deletion — bank connections

Users with an optional Plaid bank connection may disconnect a bank at **Settings** → **Bank connections** → **Disconnect** without deleting their Invoicefinito account. This enforces:

- Revocation of Plaid access for that item.
- Deletion of server-side Plaid credentials and the connection summary document.
- Cessation of future transaction imports for that bank.

Previously imported transactions remain until the user deletes their full account or those records are removed during hard purge.

7. Legal bases and user rights

Depending on jurisdiction, users may have rights to access, correct, delete, restrict, or port personal information. Account deletion is performed in the app as described in Section 5. For other privacy requests (for example, access or correction), contact hello@invoicefinito.com. We may request information to verify identity before acting on a request. If you need help signing in so you can use in-app deletion, contact us at the same address.

We do **not** sell personal information. We do not use Plaid data for purposes unrelated to providing the Services described in our Privacy Policy.

8. Exceptions and limitations

- **Third-party copies:** we cannot delete information the user shared outside our systems (for example, an invoice PDF sent by email).
- **App store billing:** Apple and Google maintain their own purchase records for subscriptions.
- **Legal holds:** we may delay deletion where required to comply with law or defend legal claims.
- **Global configuration:** non-personal app configuration shared across all users is not deleted with an individual account.

9. Governance and enforcement

- Deletion logic is implemented in audited server code (Cloud Functions) and is not bypassable by client applications.
- Firestore security rules deny client access to sensitive collections (including server-only Plaid token storage).
- Production access is limited to authorized 456Labs personnel with multi-factor authentication on cloud consoles.
- Material changes to retention or deletion behavior require updates to this Policy, the Privacy Policy, and the public deletion page before or concurrent with deployment.

10. Policy review

456Labs reviews this Policy at least **annually** and upon any material change to data practices, product features (including new integrations), or applicable law. The “Last updated” / review date is revised with each review. Owners: product and engineering leadership, with privacy inquiries directed to hello@invoicefinito.com.

Approved by: 456Labs Inc.

Contact: hello@invoicefinito.com

Public references:

- <https://invoicefinito.com/privacy.html>
- <https://invoicefinito.com/delete-account.html>
- <https://invoicefinito.com/data-deletion-retention-policy.html>