Data Retention and Disposal Policy

Folio · Zero One O · Version 1.0 · Effective August 2026

1. Purpose and scope

Folio is an iOS application that helps small business owners understand their financial position. It retrieves bank and credit card data through Plaid on the user's instruction. This policy defines how long that data is kept, how it is disposed of, and who is accountable for enforcing both.

It covers all consumer data processed by Folio, including data retrieved from the Plaid API, and applies to production systems operated by Zero One O as well as data held by our sub-processors.

2. Retention schedule

Data category	Retention period	Basis
Account records (email, name, password hash)	Life of the account	Required to operate the service
Financial account and transaction data retrieved via Plaid	Life of the account	The product's core function is historical analysis
Plaid access tokens	Until the institution is disconnected or the account is deleted	Required to sync the accounts the user connected
User-generated content (categories, tags, notes, costing data)	Life of the account	User-owned records
Session and refresh tokens	30 days, or until sign-out or revocation	Authentication
One-time sign-in codes	10 minutes, then invalid; row removed with the account	Multi-factor authentication
Sign-in metadata (IP address, user agent)	Life of the account	Security monitoring and abuse detection
Encrypted database backups	30 days (30 retained daily backups), then automatically overwritten	Disaster recovery

We do not retain consumer financial data after an account is deleted, other than in encrypted database backups, which are overwritten automatically within 30 days.

3. Disposal

3.1 User-initiated deletion

A user deletes their account from within the app (Me tab), confirming with their password. Deletion is immediate and performs, in order:

- Revocation of every Plaid Item via **/item/remove**, ending our authorization at the user's financial institutions
- Deletion of the user record, which cascades to transactions, bank accounts, credit cards, categories, tags, vendor rules, sessions, trusted devices and one-time codes

Revocation is performed before deletion, while the access tokens still exist. Each revocation is attempted independently so that a failure at the provider cannot prevent the user's account from being deleted.

3.2 Partial deletion

A user may disconnect an individual financial institution without deleting their account. This revokes the corresponding Plaid Item and stops further retrieval, while leaving previously imported history in place under the user's control.

3.3 Backups

Cloud SQL retains 30 daily backups, encrypted at rest, which expire automatically. Deleted records are therefore purged from backups within 30 days of deletion. Records are not restored selectively; they age out with the backup containing them.

4. Enforcement

- Deletion is implemented in application code and executed automatically, not as a manual administrative task.
- Referential integrity constraints (ON DELETE CASCADE) ensure dependent records cannot survive the parent account.
- Provider access tokens are held server-side only and are never exposed to the client application.
- Access to production data is restricted to authorized personnel using multi-factor authentication.

5. Legal and regulatory alignment

This policy is intended to meet applicable data privacy requirements, including the right to deletion under the California Consumer Privacy Act and, where applicable, the GDPR right to erasure. Users may request access, correction, export or deletion of their personal information; export and deletion are available directly in the application, and other requests are handled on contact.

6. Review

This policy is reviewed at least annually, and additionally whenever a change ships that affects data handling — a new sub-processor, a new category of stored data, or a change to what deletion removes. The review confirms that the documented retention periods still match system behaviour.

7. Ownership and contact

This policy is owned by the operator of Folio, who is accountable for its enforcement and review. Questions or data requests: **privacy@zerooneo.com**.