Data Retention and Disposal Policy

How long Splits retains user data, and how it is securely disposed of.

Effective	May 19, 2026	**Version**	1.0
Organization	Splits	**Owner**	Mustafa Alhelawe, Founder
Contact	privacy@splitshq.com	**Review cadence**	Annual

---

1. Purpose and Scope

This Data Retention and Disposal Policy describes how Splits handles the retention, deletion, and disposal of personal and financial information collected through the Service. It applies to all production data systems operated by Splits and to backups maintained by its vendors.

2. Principles

- Retain only what is necessary to deliver the Service or meet legal obligations.
- Delete user data promptly upon account deletion or when retention windows expire.
- Honor user requests for access, correction, and deletion in accordance with applicable law (including GDPR and CCPA where applicable).
- Maintain documented retention windows for each data category.

3. Data Categories and Retention Windows

The retention windows below apply to active production data. Backup retention is described separately in Section 6.

Data category	Retention while account is active	Retention after account deletion
User account record (email, display name)	Life of account	Deleted within 7 days of account deletion; backups age out per Section 6.
Friendships, splits, ledger entries, notifications	Life of account; users may delete individual records	Deleted within 7 days of account deletion.
MFA factors and registered passkeys	Life of account; user may remove individual factors at any time	Deleted with account.
Plaid items, accounts, and transactions	Until the user disconnects the institution	Plaid access token revoked immediately on disconnect or account deletion; local rows deleted at the same time.
Push notification subscriptions	Life of account; user may revoke	Deleted with account.

Data category	Retention while account is active	Retention after account deletion
	per-device	
Operational logs (Vercel, Supabase)	Rolling 30-day window	Rolled out of log retention within 30 days regardless of account status.
Database backups	30-day point-in-time recovery window	Backups expire on a rolling basis after 30 days.

4. Deletion Triggers

4.1 User-Initiated Account Deletion

Users can request deletion of their account at any time from the in-product Settings area. Upon confirmation, Splits initiates deletion of the user's record and all data linked to it. Cascade deletes propagate through related tables (linked Plaid items, accounts, transactions, ledger entries authored by the user, friendships, payment records, MFA factors, and registered passkeys). Plaid access tokens associated with the user are revoked through the Plaid API before the corresponding rows are deleted.

4.2 Plaid Disconnect

When a user disconnects an institution from within the Service, the corresponding Plaid item is removed and the associated access token is revoked. Historical transaction records sourced from that item are retained only as needed to preserve historical ledger integrity for the counterparties involved, and are otherwise deleted within 30 days.

4.3 Inactivity Purge

Accounts that have been inactive for 36 months may be deactivated and queued for deletion. Affected users receive at least 30 days' advance notice by email.

4.4 Legal Holds

If Splits receives a valid legal hold or law-enforcement preservation request, the affected data is preserved despite the schedule above, and the user is notified to the extent permitted by law.

5. Deletion Methods

Deletion is performed via SQL DELETE statements operating under foreign-key cascade relationships defined in the database schema. Once a row is deleted from the primary database, the underlying storage is overwritten in the normal course of Postgres operations. Splits does not maintain shadow copies of deleted user data outside of the backup window described below.

6. Backup Retention

Splits relies on Supabase's managed backup infrastructure. Point-in-time recovery is enabled with a 30-day window. Data deleted from the primary database may persist in backups until those snapshots age out of the 30-day window. No new backups will reference deleted user data.

7. User Rights

Users may exercise the following rights with respect to their personal information, in accordance with applicable law:

- Access: request a copy of the personal information Splits holds about them.
- Correction: request that inaccurate information be corrected.
- Deletion: request deletion of their account and associated data (subject to legal-hold exceptions).
- Portability: request a structured copy of their data.
- Objection / restriction: request that processing of their data be limited.

Requests may be submitted from within the application or by emailing privacy@splitshq.com. Splits responds within 30 days, with one extension of up to 60 additional days where the request is complex.

8. Vendor Disposal

Splits' primary vendors maintain their own data deletion procedures. When Splits terminates use of a vendor, it requests deletion of any data the vendor holds on its behalf and retains the vendor's confirmation.

9. Policy Review

This Policy is reviewed at least annually and updated when retention requirements, data categories, or vendors change materially. Current version v1.0, effective May 19, 2026.