Homericly — Data Retention and Deletion Policy

Live online: https://homericly.com/data-retention — always the canonical version.

Owner: Founder / Engineering Lead — roofing@homericly.com **Monitored security channel:** security@homericly.com (group address, always watched) **Last reviewed:** 2026-06-05 **Review cadence:** Quarterly, or on any change to applicable privacy laws (GDPR, CCPA, state-level US privacy laws).

1. Purpose

Define how long Homericly retains each class of data, when and how it is deleted, and how a user can request deletion under GDPR / CCPA.

2. Principles

- **Collect only what is necessary** to operate the feature.
- **Retain only as long as necessary** for that feature, billing,

audit, or legal obligation.

- **Delete promptly** once the retention period elapses or the user

requests deletion.

- **Audit log of deletions** is itself retained — the act of deletion

is a privileged operation that must remain provable.

3. Data classes and retention windows

Class	Examples	Retention	Deletion trigger
Bank-feed data	Plaid items, accounts, transactions	Active until user disconnects, then 24 months for reconciliation, then purged	User disconnect + 24-month sweep
Customer / contact PII	Names, emails, phones, addresses in the CRM	Active for the life of the relationship + 12 months	Customer-record deletion request OR 12 months past last activity
Financial records	Invoices, payments, expenses, GL journals	7 years (US tax retention norm)	Aged-out sweep at year-end
Audit log	`audit_log` table	Indefinite	Never deleted; redacted-not-removed on individual user-data deletion requests

Class	Examples	Retention	Deletion trigger
Telemetry / analytics	Plausible events, PostHog events	Plausible: 12 months. PostHog: 12 months.	Provider's own retention sweep
AI generation logs	Prompts, completions for content, design, agent runs	90 days	Daily sweep
Email / SMS	Outbound message bodies, delivery status	90 days (status), 30 days (bodies)	Daily sweep
Backups	Supabase point-in-time recovery	7 days (Hobby) / 28 days (Pro)	Provider-managed rolling window
Session tokens	Auth sessions, OAuth refresh tokens	Sliding 30-day expiry; rotated on sign-in	Auto-expire + revoke on sign-out
Secrets / API keys	Vendor credentials in Vercel env	Until rotation	Manual on incident or vendor rotation

4. User-initiated deletion (GDPR Art. 17 / CCPA §1798.105)

Any user — portal end-customer or contractor — may request deletion of their personal data by emailing `privacy@homericly.com`.

Within 30 days the operator:

1. Confirms identity (account email match + magic-link verification).
2. Disconnects any third-party integrations bound to the user

(Plaid items, Composio connected accounts, Stripe customer when applicable).

1. Soft-deletes the user record (sets `deleted_at`) and rotates the

user's auth tokens to terminate live sessions.

1. After a 30-day grace window (to allow reversal on a mistaken

request), runs the hard-delete sweep which:

- Removes the user's PII rows from `customers`, `portal_users`,

`leads`, message logs.

- Redacts the user's identifiers in the `audit_log` (replaces

name/email with a stable hash) but keeps the event records — the fact that an action happened cannot be denied.

- Removes generated AI artifacts attributable to the user (review

drafts, content cards, image generations).

1. Records the deletion in the audit log + emails the requester a confirmation.

Exception: data the operator is legally obliged to retain (tax records, anti-fraud records on a confirmed chargeback) is retained under the relevant exemption and the user is informed.

5. Account closure

When an organization terminates its Homericly subscription:

- 12-month read-only grace window (the org's data remains accessible through export tools but no new writes are accepted).
- After the grace window, the org's data is purged with the same sweep above. The `audit_log` is redacted, not removed.
- The organization's Stripe customer record is preserved (Stripe is the regulated party for payment-history retention).

6. Automated sweeps

- **Daily** — AI generation logs (>90 days), message bodies (>30 days), message statuses (>90 days).
- **Monthly** — Plaid transactions belonging to disconnected items past the 24-month window.
- **Quarterly** — CRM contacts past the 12-month inactivity window.
- **Year-end** — Financial records past the 7-year window.

Each sweep records the number of rows removed and the run timestamp to the audit log.

7. Third-party data minimization

- Plaid: only `Transactions`, `Auth`, `Balance` products are enabled.
- Stripe: customers + payment methods + subscriptions. No card data ever transits Homericly servers (Stripe Elements / Checkout only).
- Composio: only the toolkits a user has explicitly connected. Per-org spend caps prevent runaway data egress.
- AI providers: prompts contain only the minimum context required;

customer PII is not pasted into model prompts unless the user has enabled the relevant AI feature for that customer.

8. Notifications and right-to-know

The publicly published Privacy Policy (`homericly.com/privacy-policy`) lists the data classes above and the operator's contact email. Notice-of-collection is provided at the point of data entry (e.g., the Plaid Link consent screen, the portal sign-up screen).

9. Compliance posture

- **GDPR** Art. 5 (storage limitation), Art. 17 (right to erasure):

satisfied by sections 3, 4.

- **CCPA** §1798.105 (right to delete), §1798.130 (notice): satisfied

by sections 4, 8.

- **Plaid SPQ** Q11 (defined and enforced retention policy reviewed

periodically): satisfied by sections 3, 6, plus the quarterly review cadence stated above.

10. Review

This policy is re-read every quarter. Material changes require a postmortem-style note in `docs/policies/CHANGELOG.md` so the review trail is preserved.