Data & Proof Retention Policy

What TrustLayer stores, where, and for how long

Last updated: September 3, 2026

TrustLayer is local-first and non-custodial. Identity keys are generated and encrypted (AES-GCM) inside the user's browser and never transmitted. This document describes the limited data processed server-side and the retention period applied to each category.

1. Data we never collect

Wallet private keys, seed phrases, or recovery phrases.

Custody of user funds — the protocol is fully non-custodial.

Advertising identifiers, third-party tracking pixels, or fingerprinting data.

2. Local-only data (user device)

Encrypted identity keypair, local proof queue, offline vouch drafts, and messenger history are stored in browser storage under AES-GCM encryption.

Retention: controlled entirely by the user. Clearing site data or exporting the 12-word recovery phrase is the only migration path; TrustLayer cannot restore it.

3. Public protocol data (on-chain / proofs)

Public wallet address, public handle, display name, vouch proofs, badge mints and trust-score snapshots.

Proof hashes are anchored to Base mainnet and to Merkle roots. Retention: permanent and immutable — on-chain records cannot be deleted or amended, including on account deletion requests.

4. Compliance & audit records

compliance_log: every geo-check, self-certification, purchase acceptance, block and jurisdiction mismatch event. Retention: minimum 5 years, no automated purge.

Admin audit log: privileged administrative actions, including badge grants/revocations and treasury operations. Retention: minimum 5 years.

5. KYC / presale intake

Collected only for token acquisition flows: wallet address, full name, email, declared country and detected IP country.

Personally identifiable fields are encrypted at rest with pgcrypto and are decryptable only through an admin-role RPC guarded by a rotating admin secret.

Retention: minimum 5 years, encrypted, in line with financial record-keeping expectations.

6. Operational telemetry

Aggregated, non-identifying request metrics and error traces used to keep the read edge and cron jobs healthy.

Retention: 30 days rolling, then discarded.

7. Access control

All server-side tables enforce row-level security. Sensitive tables are reachable only by service-role code paths or by admin-role holders verified through a separate roles table and TOTP step-up.

Encryption-key rotation requires export under the current secret, rotation of the secret, and a re-encryption backfill.

8. User rights

Users may export their identity and proof set at any time from the app, and may delete all local data from their device.

Requests regarding server-side records: mdtawhidrahman507@gmail.com. Note that immutable on-chain proofs cannot be erased.