

Privacy Policy

Your data stays with you — local-first and non-custodial

Last updated: September 3, 2026

TrustLayer is a decentralized identity protocol. Identity keys are generated and encrypted (AES-GCM) inside your browser and never transmitted to us. This policy describes the limited data processed server-side and your rights over it.

1. What we never do

We never request, store, or transmit your wallet private keys or seed phrases.

We never take custody of your funds. TrustLayer is fully non-custodial.

We never sell, rent, or share personal data with advertisers or data brokers.

We never install software on your device without your explicit consent through an official store.

2. What we process

Public wallet address (for trust-score lookups and delivery of on-chain entitlements).

Public handle and display name that you choose.

Anonymised interaction proofs — cryptographic hashes only, no personal content.

For token acquisition flows only: full name, email, declared country and detected IP country, encrypted at rest.

Aggregated, non-identifying request metrics and error traces used to keep the service healthy.

3. Legal bases

Where GDPR or an equivalent regime applies, we rely on: contract performance (operating the account and delivering requested protocol services); legitimate interests (security, abuse and Sybil prevention, service reliability); legal obligation (sanctions screening, record retention); and consent where separately requested.

4. Wallet signatures

When you connect a wallet we request a standard EIP-191 signature to prove ownership of the address. This signature does not authorise any transaction, transfer, or approval — it is read-only authentication equivalent to "Sign-In with Ethereum".

5. Cookies and tracking

We do not use third-party advertising cookies, fingerprinting, or cross-site tracking pixels. Local browser storage is used to hold your encrypted identity and app preferences on your own device.

6. Processors and transfers

We use a managed database/auth provider, edge hosting, an email/notification provider, and AI providers for content generation. Personal data is not used to train third-party models. Where data is transferred internationally we rely on the processor's standard contractual clauses.

7. Retention

Retention periods are set out in the Data & Proof Retention Policy. On-chain proofs are permanent and immutable and cannot be deleted, including following a deletion request.

8. Your rights

Subject to applicable law you may request access, rectification, erasure of server-side records, restriction, portability, and objection, and may withdraw consent where consent is the basis.

Requests: mdtawhidrahman507@gmail.com. We respond within 30 days. You may also complain to your local supervisory authority.

9. Children

The Service is not directed to persons under 18. We do not knowingly process data of minors; if you believe we have, contact us and we will delete it.

10. Security and breach

All server-side tables enforce row-level security; sensitive fields are encrypted at rest and reachable only through admin-role paths with step-up verification. In the event of a personal-data breach we will notify affected users and, where required, regulators without undue delay.

11. Contact

Privacy questions: mdtawhidrahman507@gmail.com.