Talken — Privacy Policy

Last updated: 25 August 2025

This Privacy Policy describes how **Talken** ("Talken", "we", "us", or "our") handles information in connection with our website (**talken.me**), the Talken application, and auxiliary experiences such as whitelist/early-access flows run via our Discord bot (collectively, the "Services").

We designed Talken as a **privacy-first, end-to-end encrypted chat** built on top of **Quai Network**. By default, message contents are encrypted on the client and **stored on-chain as encrypted payloads**. We cannot decrypt your messages; only you (and the intended recipient) hold the keys.

If you do not agree with this Policy, please do not use the Services.

1) What we (do not) see

- **Message contents:** Encrypted end-to-end. We **cannot** read them. Encrypted payloads may be stored **on-chain** and are **immutable**.

- **Public blockchain data:** Your wallet address, on-chain timestamps, transaction/hash metadata are **public by design** and visible to anyone (including block explorers and indexers).

- **Whitelist / early access (Discord bot):** If you choose to participate, we may collect the **Discord handle** and **wallet address** you submit **voluntarily** to manage allowlists, eligibility, and access ("Whitelist Data").

- **Basic operational logs:** Like most Internet services, we may receive limited technical data (e.g., coarse event logs, device/browser type, and similar diagnostics) to secure the Services and prevent abuse. We do **not** sell personal data or build marketing profiles.

2) Legal bases for processing

Depending on your location (e.g., GDPR/UK GDPR/CCPA):

- **Consent** — for Whitelist Data and optional communications. By submitting data in whitelist/early-access flows, **you consent** to its processing for access management and UX (you can withdraw consent any time).

- **Legitimate interests** — to secure and operate the Services (e.g., anti-abuse, rate limiting, diagnostics).

- **Contract necessity** — to deliver features you request (e.g., enabling allowlisted access).

3) How we use information

- To **operate** the Services (including allowlist gating and eligibility checks).

- To **communicate** essential updates (e.g., service notices, testnet information).

- To **secure** and **debug** (fraud/abuse prevention, reliability).

- To **improve UX** (e.g., streamline early-access flows).

We do **not** use message contents for analytics or advertising (we can't decrypt them).

4) Sharing

We do not sell personal data. We may share limited information with:

- **Vendors/Processors** that help us run the Services (e.g., hosting, incident tooling), bound by contractual safeguards.

- **Public blockchains** (by your transactions) — on-chain data is public and outside our control.

- **Wallet providers** (e.g., Pelagus) you choose to use — governed by their policies.

- **Legal/Compliance** — when required by law or to defend rights and security.

5) Retention

- **On-chain encrypted message payloads** may persist **indefinitely**; we cannot alter or delete them.

- **Whitelist Data** is retained **no longer than necessary** for early-access operations, then deleted or anonymized. If you withdraw consent earlier, we will delete it sooner where feasible.

- **Operational logs** are kept for a limited time necessary for security and reliability, then minimized or aggregated.

6) Your choices & rights

Depending on your jurisdiction, you may have rights to **access**, **correct**, **delete**, **port**, or **object** to certain processing, and to **withdraw consent**.

Limitations: On-chain data and encrypted message payloads may be technically and legally **immutable**. Where we cannot delete or alter on-chain data, we will explain the limitation.

To exercise rights or ask questions, contact: **talken.me@protonmail.com**.

7) Children

The Services are not directed to children. We do not knowingly collect personal data from users **under 13** (or **under 16 in the EEA/UK**). If you believe a child has provided us data, contact us; we will take appropriate steps.

8) Security

- **E2EE by default**: message contents are encrypted client-side; keys remain with users.

- We implement reasonable organizational and technical safeguards.

  No system is perfectly secure. **You are responsible** for safeguarding your data, devices, wallets, seed phrases, private keys, funds, etc.

9) International transfers

We may process data in countries other than your own. By using the Services, you understand your data may be transferred internationally where local laws may differ.

10) Third-party services

Your use of third-party tools (e.g., **Pelagus wallet**, **Discord, Quai Network**) is governed by their terms and privacy policies. We are not responsible for their practices.

11) Communications

We may send essential service messages (e.g., security, testnet notices). Marketing/optional messages are sent **only with consent**, and you may **unsubscribe** at any time.

12) Changes

We may update this Policy periodically. We will post the new effective date above. Continued use indicates acceptance.

13) Contact

Data Controller: **Talken**

Email: **talken.me@protonmail.com**