



admin@tuwa.io

Privacy Policy

Last Updated: October 14, 2026

This Privacy Policy describes how FOP Tkach Oleksandr ("we," "us," or "our") collects, uses, and protects your information when you use the unified TUWA ecosystem, which includes the main site tuwa.io, the showcase at demo.tuwa.io, the Quasar dashboard at quasar.tuwa.io, the Custom Styles editor at custom-style.tuwa.io, the documentation at docs.tuwa.io and stories.tuwa.io, and our open-source npm packages (Orbit Utils, SIWX, Satellite Connect, Pulsar, Nova UI Kit, the TUWA SDK and the Quasar SDK).

1. Open Source Ecosystem & Transparency

The core logical layers of TUWA are open-source and publicly available on [GitHub](https://github.com). Our npm packages (@tuwaio/orbit-*, @tuwaio/satellite-*, @tuwaio/pulsar-*, @tuwaio/nova-*, @tuwaio/siwx-*, @tuwaio/sdk and the network add-ons) run in your own app and send no data to us. Quasar Community Edition runs on your own servers and sends no data to us either. We encourage you to review our [Documentation](#) to fully understand how data flows within these headless and UI-agnostic modules.

2. Core Principle: Self-Custody

TUWA is built for self-custody and keeps data on your device where it can. We NEVER ask for, access, or store your private keys. You maintain full sovereignty over your digital assets at all times.

3. Data Collection & Usage

To provide the ecosystem's features, we collect limited, specific data:

- **Registration & Notifications:** We collect your email address strictly for authentication, account management, and sending necessary operational notifications.
- **Wallet Sign-In:** If you sign in to the Quasar dashboard with a wallet (SIWX), we store its public address to identify your account.
- **Web3 Synchronization:** We collect public wallet addresses and transaction metadata to synchronize your on-chain history across devices via the Quasar cloud layer.
- **Billing Information:** Quasar Cloud is in public beta and free of charge, so we do not collect billing or payment details.

We do not sell your personal data to third parties.

4. API Keys & Infrastructure

We utilize robust RPC infrastructure to process blockchain requests. Organizations can provide their own provider settings for their apps: custom RPC endpoints, Alchemy or QuickNode keys, and Pimlico or Gelato keys. Quasar Cloud reads the transactions of an organization's apps only through the RPC providers that the organization sets up, and tracks sponsored (ERC-4337) and relayed transactions only with the app's own Pimlico key or bundler URL and its own Gelato key. Any custom RPC endpoints and API keys you provide are encrypted at rest in our database (AES-256-GCM) and decrypted only by the Quasar engine when it calls your provider. When you provide them, the Quasar engine sends that provider the data its request needs, such as a transaction hash or a wallet address, under your own agreement with the provider.

5. Data Storage and Protection

Most Web3 operations occur locally on your client device using Local Storage (for example, by Pulsar and Satellite Connect). Any data transmitted to Quasar Cloud is protected using industry-standard security measures, including transport layer security (TLS) and access controls that scope every record to its organization.

6. Your Privacy Rights

You may request access to and correction or deletion of personal data associated with your account, subject to applicable law, including legal retention obligations and exceptions (Regulation (EU) 2016/679, Articles 15 and 17). Where the law gives you these rights, you may also ask us to restrict or stop processing, object to processing based on our legitimate interests, and receive your data in a portable format. To exercise these rights, please contact us at admin@tuwa.io. Immutable on-chain data cannot be deleted by us.

7. Additional Privacy Information

For personal data within the scope of applicable data-protection law, this section gives our purposes and legal bases, retention periods, recipients and international transfers, and how to complain to a supervisory authority (Regulation (EU) 2016/679, Articles 13 and 14).

Controller and contact. FOP Tkach Oleksandr, Ukraine, admin@tuwa.io. We have not appointed a data protection officer; write to the same address with any data protection question.

Purposes and legal bases.

Activity	Data	Legal basis
Your Quasar account: sign-up, sign-in, two-factor authentication, passkeys, linked wallets, your profile	Email address, password hash, 2FA and passkey data, public wallet addresses; the name and the Telegram and Discord usernames you choose to add to your profile	Performance of our contract with you
Keeping accounts and services secure: sessions, rate limits, abuse prevention, blocking re-registration of a deleted email for 30 days	Session tokens, IP addresses in request logs, email address of a deleted account	Our legitimate interest in secure services and in preventing abuse

Activity	Data	Legal basis
Managing the access of teams: who lost access to an organization and who deleted one, to investigate incidents and disputes about that access	Email address of a removed member, the account that deleted an organization, the dates	Our legitimate interest, and the organization's, in managing access to its organization and in investigating incidents and disputes
Complying with sanctions: checking an organization or person reported to us as subject to sanctions	Names, email addresses, wallet addresses and organization details of the case, the lists checked and the result	Our legal obligations under sanctions law, and our legitimate interest in complying with it
Providing Quasar Cloud to your organization: apps, API keys, webhook endpoints, usage and quota	Names and settings of your organization and apps, usage records, the members of the organization and their roles	Performance of our contract where you are the party to it (for example, as a sole proprietor); otherwise our legitimate interest, and your organization's, in providing and using the service your organization signed up for
Operational emails: verification, security notices, quota notices	Email address	Performance of our contract with you
Error monitoring of the Quasar dashboard and engine	Technical error details; we turn off the collection of cookies, request identity headers and account data	Our legitimate interest in reliable services
Answering requests and legal claims	Your messages and the data needed to answer them	Our legitimate interests and legal obligations

Our role for your apps. When an organization syncs its users' transactions to Quasar Cloud, that organization decides what is processed and is the controller of that data. We process it on the organization's behalf under our [Data Processing Addendum](#). Its users should contact the organization first; we will help it answer.

Retention.

- Account data: until you delete your account. After deletion, we keep the email address for 30 days to block re-registration and then remove it.

- Records of removed members and deleted organizations: 12 months after the removal or deletion.
- Records of sanctions checks: 5 years after the case is closed, unless the law requires a different period.
- Transactions and webhook endpoints: while the app that sent them exists; they are deleted together with the app or its organization.
- Webhook delivery logs: up to 3 months, and together with the app or its organization if that is earlier.
- Error reports: up to 90 days.
- Backups: deleted data can remain in our encrypted database backups for up to 7 days.

Recipients and processors. We share personal data only with providers that help us run the ecosystem, and only the data each one needs:

- HostHatch: the servers of Quasar Cloud (production and staging) in Amsterdam, the Netherlands.
- Cloudflare: network, security and DNS for every site; storage of backups and files (R2).
- Vercel: hosting of tuwa.io, the documentation sites, demo.tuwa.io, custom-style.tuwa.io and stories.tuwa.io.
- Resend: delivery of emails.
- Sentry (Functional Software): error monitoring of the Quasar dashboard and engine.
- Alchemy: blockchain reads of the Quasar dashboard, such as the ENS name of the wallet you connect.

Providers that an organization sets up for its apps, such as its own RPC endpoint or its Alchemy, QuickNode, Pimlico or Gelato key, receive data on that organization's instruction and under its own agreement with them (Section 4). We may also disclose data where the law requires it.

International transfers. We are established in Ukraine and collect your data directly from you. The Quasar Cloud servers are in the Netherlands. Several providers above are established or process data in the United States or in other countries outside the European Economic Area. Where the GDPR requires a safeguard for such a transfer, these are the safeguards in the providers' terms:

- Cloudflare, Vercel, Resend and Sentry: their certification under the EU-U.S. Data Privacy Framework.
- HostHatch: the standard contractual clauses in its data processing addendum, for any access to our servers from outside the European Economic Area.
- Alchemy: the standard contractual clauses in its data processing addendum.

You can ask us at admin@tuwa.io which safeguard applies to a particular provider.

Complaints. If the GDPR applies to you, you may complain to the data protection supervisory authority of the EU or EEA country where you live or work or where you believe an infringement took place. Separately, compliance with Ukrainian data protection law is supervised by the Ukrainian Parliament Commissioner for Human Rights. We would appreciate the chance to address your concern first at admin@tuwa.io.

Data we do not collect from you. Some data comes from other sources: transactions and wallet addresses that an app syncs to Quasar Cloud, and public blockchain data. If we obtain your personal data from a source other than you, we will also provide applicable information about its source and the timing of notice (Regulation (EU) 2016/679, Article 14).