

Data Processing Addendum

Last Updated: October 14, 2026

This Data Processing Addendum ("DPA") forms part of the [Terms of Service](#) between FOP Tkach Oleksandr ("TUWA," "we," "us," or "our") and the organization that uses Quasar Cloud ("Customer"). It applies to personal data that we process on the Customer's behalf when we provide Quasar Cloud ("Customer Personal Data").

1. Roles

- The Customer is the controller of Customer Personal Data, or a processor acting for its own controller. We are its processor, or its sub-processor in the second case.
- This DPA does not cover personal data that we process as a controller, such as the accounts of the Customer's team members, billing and security records. Our [Privacy Policy](#) describes that processing.

2. Details of Processing

Subject matter	Providing Quasar Cloud to the Customer
Duration	While the Customer uses Quasar Cloud, and until the deletion described in Section 10
Nature and purposes	Receiving, storing and tracking the transactions that the Customer's apps sync to Quasar Cloud; showing their history; sending webhooks to the Customer's endpoints
Data subjects	The users of the Customer's apps whose transactions the apps sync
Categories of data	Public wallet addresses; transaction hashes and the metadata the app sends with them (such as titles, descriptions and payloads); transaction statuses; webhook payloads and delivery logs

Special categories	None are intended. The Customer must not send special categories of personal data or data relating to criminal convictions and offences in transaction metadata
--------------------	---

3. AML Screening

AML screening of the senders of incoming transactions is not available in Quasar Cloud. Before we offer it, we will update this DPA and tell the Customer under Section 7.

4. Instructions

We process Customer Personal Data only on the Customer's documented instructions. These Terms, this DPA, the Customer's settings in the Quasar dashboard and the Customer's API requests are its instructions. We inform the Customer if, in our opinion, an instruction infringes data protection law, and we may refuse to follow it. If the law requires us to process Customer Personal Data otherwise, we tell the Customer before we do, unless that law prohibits it.

5. Confidentiality

Everyone we authorize to process Customer Personal Data is bound by confidentiality.

6. Security

We implement the technical and organizational measures in Annex B. We may update them, but not in a way that lowers the overall protection of Customer Personal Data.

7. Sub-processors

- The Customer gives us a general authorization to use the sub-processors in Annex C.

- We tell the Customer about a new or replaced sub-processor by email to the owners of its organization at least 30 days before it starts processing Customer Personal Data. The Customer may object on reasonable data protection grounds within that period, and we will discuss the objection with it in good faith. If we cannot resolve the objection, the Customer may stop using Quasar Cloud before the new sub-processor starts processing its data, after exporting the data of its apps (Section 10).
- We impose on each sub-processor data protection obligations that are no less protective than this DPA, and we remain responsible to the Customer for its performance.
- **Providers that the Customer sets up.** Quasar Cloud reads the transactions of the Customer's apps only through providers that the Customer sets up for an app: a custom RPC endpoint, Alchemy or QuickNode keys, a Pimlico key or a bundler URL sent with a transaction, and a Gelato key. The Customer obtains these endpoints and keys from its own accounts with those providers, chooses them and contracts with them; they are not our sub-processors. On the Customer's instruction, we send them only the data each request needs, such as a transaction hash, a user operation hash or a task ID, through the endpoint and with the credentials that the Customer gave us, and we keep those credentials encrypted (Annex B). The Customer is responsible for its agreement with each such provider, including any data protection terms and transfer safeguards it requires.

8. Assistance

- **Requests of data subjects.** We forward to the Customer any request we receive about Customer Personal Data and do not answer it ourselves unless the Customer instructs us to. The Customer can find, export and delete the data of its apps in the Quasar dashboard; we help with anything these tools do not cover.
- **Security, impact assessments and consultations.** We give the Customer reasonable assistance with its obligations under Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to us.

9. Personal Data Breaches

We notify the Customer without undue delay after we become aware of a personal data breach that affects Customer Personal Data. The notice describes, as far as we know at the time, the nature of the breach, the categories and approximate number of data subjects and records concerned, its likely consequences and the measures taken or proposed. We provide further information as it becomes available.

10. Deletion and Return

- The Customer can export the data of its apps and delete an app or its organization in the Quasar dashboard at any time.
- When the Customer deletes an app or its organization, we delete the related Customer Personal Data: transactions, webhook endpoints and delivery logs. Deleting large volumes of data may take some time.
- At the end of the services for the Customer's organization (Terms of Service, Section 5), the Customer chooses between return and deletion: until the end date it can export the organization in the Quasar dashboard, or, where its access was closed without notice, ask us for the export file within 30 days after the closing. We delete the remaining Customer Personal Data 30 days after the end date.
- Webhook delivery logs are also deleted automatically after 3 months.
- Deleted data can remain in our encrypted database backups for up to 7 days, after which the backups are overwritten.
- We keep Customer Personal Data longer only where the law requires us to, and we do not return it where the law forbids it.

11. Audits

We make available to the Customer the information necessary to demonstrate compliance with this DPA, including this DPA, the description of our security measures, our sub-processor list and answers to reasonable security questionnaires. We also allow audits, including inspections, by the Customer or an auditor it mandates who is bound by confidentiality, on at least 30 days' notice, during business hours and at the Customer's cost. Where the information above or a remote review of

documents is enough, the audit is done that way. An on-site inspection takes place no more than once in any 12 months, unless a personal data breach, a supervisory authority or reasonable grounds to suspect a breach of this DPA require another one.

12. International Transfers

- **Flows.** The Customer's apps send Customer Personal Data to Quasar Cloud, whose servers are in the Netherlands and which we operate from Ukraine. We send Customer Personal Data to the sub-processors in Annex C. Providers that the Customer sets up receive data on its instruction (Section 7).
- **Standard contractual clauses.** Where the Customer is subject to the GDPR and transfers Customer Personal Data to us, and our processing of that data is not itself subject to the GDPR, the standard contractual clauses approved by Commission Implementing Decision (EU) 2021/914 apply to that transfer: Module Two where the Customer is a controller, and Module Three where the Customer is a processor. The Customer is the data exporter and we are the data importer. We conclude the clauses with such a Customer, with their annexes completed and signed by both parties, before it sends Customer Personal Data to Quasar Cloud. Until data processing is set up for an organization, Quasar Cloud does not accept Customer Personal Data from its apps.
- **Options in the clauses.** Clause 7 (docking clause) applies. Under Clause 9(a), Option 2 (general written authorisation) applies, with the notice period in Section 7. The optional language in Clause 11(a) does not apply. The competent supervisory authority is determined under Clause 13(a). Under Clause 17, Option 1 applies and the clauses are governed by the law of Ireland. Under Clause 18, disputes are resolved by the courts of Ireland.
- **Annexes of the clauses.** Annex I.A: the details of the parties that the Customer gives when it concludes the clauses, and Annex A of this DPA. Annex I.B: Annex D of this DPA. Annex I.C: the supervisory authority under Clause 13. Annex II: Annex B. Annex III: Annex C.
- **If our processing becomes subject to the GDPR.** If our processing of Customer Personal Data becomes directly subject to the GDPR under its Article 3(2), we will tell the Customer before that happens. The parties will then reassess the transfer and put in place the safeguard that the law requires before transfers continue; the clauses above do not by themselves cover that case.

- **Our sub-processors.** The safeguards for our transfers to sub-processors are listed in Annex C.

13. Liability and Precedence

Each party's liability under this DPA is subject to the limitations in the Terms of Service, to the extent permitted by applicable law. If this DPA conflicts with the Terms of Service, this DPA prevails; where standard contractual clauses apply and conflict with this DPA, the clauses prevail.

14. Term

This DPA applies for as long as we process Customer Personal Data.

Annex A. Parties

- **Customer (controller or processor):** the organization named in the Customer's Quasar Cloud account; contact: the owners of that organization.
- **TUWA (processor):** FOP Tkach Oleksandr, Ukraine; contact: admin@tuwa.io.

Annex B. Security Measures

- **Encryption.** TLS for every connection to Quasar Cloud. Stored secrets, such as provider API keys and webhook secrets, are encrypted with AES-256-GCM. Database backups are encrypted (libsodium) before they leave our servers.
- **Access control.** Every record is scoped to its organization. Organizations have owner, admin and member roles. Accounts can use two-factor authentication and passkeys. Access to the servers is limited to the people who operate Quasar Cloud.
- **Webhooks and outbound requests.** Webhooks are signed (HMAC-SHA256). Webhook delivery and the Customer's RPC endpoints are protected against server-side request forgery. The API has rate limits.
- **Monitoring.** Services are monitored with alerts. Error monitoring excludes cookies, request identity headers and account data. Deleted organizations and their removed members are recorded.

- **Development and release.** Dependencies are updated regularly. Release images are scanned for vulnerabilities, signed (cosign) and published with a software bill of materials; a rollback deploys only images whose signature is verified. Operations follow written runbooks, including for incidents and restoring backups.

Annex C. Sub-processors

Providers that the Customer sets up for its apps are not sub-processors (Section 7).

Sub-processor	Service	Data it receives	Location of processing	Transfer safeguard
HostHatch, LLC	Servers of Quasar Cloud	All Customer Personal Data, stored on our servers	The Netherlands (Amsterdam)	None needed for storage in the European Economic Area; the standard contractual clauses in HostHatch's data processing addendum cover any access from outside it
Cloudflare, Inc.	Network and security; storage of encrypted backups (R2)	Data passing through its network; encrypted backups	Global network	EU-U.S. Data Privacy Framework, with the standard contractual clauses of Cloudflare's data processing addendum as a fallback
Functional Software, Inc. (Sentry)	Error monitoring	Technical error details, which can include a transaction hash or a wallet address	United States	EU-U.S. Data Privacy Framework

Annex D. Description of the Transfer (Annex I.B of the Clauses)

Categories of data subjects	The users of the Customer's apps whose transactions the apps sync
-----------------------------	---

Categories of personal data	Public wallet addresses; transaction hashes and the metadata the app sends with them; transaction statuses; webhook payloads and delivery logs
Sensitive data	None required or intended. Quasar Cloud does not need special categories of personal data or data relating to criminal convictions and offences, and the Customer must not send them in the free-text fields of its transactions, such as titles, descriptions and payloads (Section 2). If the Customer's integration sends other categories of data or needs other retention periods than this Annex describes, the Customer tells us before the transfer, and we agree a description that fits it
Frequency of the transfer	Continuous, whenever the Customer's apps sync transactions
Nature of the processing	Receiving, storing and tracking transactions; showing their history; sending webhooks
Purpose of the transfer and further processing	Providing Quasar Cloud to the Customer (Section 2)
Retention	While the app that sent the data exists; webhook delivery logs for up to 3 months; deleted data remains in encrypted backups for up to 7 days (Section 10)
Transfers to sub-processors	As listed in Annex C, for the duration of the processing