

Data processing agreement

Created on 16 October 2026

This data processing agreement under Art. 28 GDPR supplements the [terms and conditions](#) and applies to any use of HORAKA in which personal data is processed on behalf of the customer.

Parties

Controller (hereinafter “client”) is the customer who created the workspace, with the details in their account.

Processor (hereinafter “contractor”) is:

giant Computer Systems

Owner Marc Breuer

Am Altengraben 23

90768 Fürth

Germany

Email: info@horaka.com

Preamble

The client uses HORAKA to record, evaluate and bill working time for clients and projects, alone or with team members. The client alone decides on the purposes and means of this processing and is the controller within the meaning of Art. 4 (7) GDPR. The contractor processes the data exclusively on the client's behalf.

This agreement does not cover data the contractor processes for its own purposes, in particular the client's own master, contract and billing data. In that respect the contractor is a controller in its own right and its [privacy policy](#) applies.

§ 1 Subject matter and duration

1.1 The subject matter is the operation of HORAKA for the client's workspace: storing and processing time entries and master data, managing team member accounts, calculating rounding, breaks and amounts, creating reports and exports, sending emails and notifications, and providing the API and the webhooks and connections set up by the client.

1.2 The duration of this agreement corresponds to the term of the contract for use. It ends without notice upon final deletion of the data under § 9.

§ 2 Nature and purpose of processing, types of data, data subjects

2.1 Nature of processing: collecting, recording, storing, organising, adapting, reading, querying, using, transmitting to recipients determined by the client, restricting and erasing.

2.2 Purpose: recording, evaluating and billing working time for the client.

2.3 Types of data:

- Team member accounts: name, email address, role, language, time zone, sign in data (password as a hash, two factor authentication and passkeys where used);
- Time entries: start, end, duration, breaks, project, activity, notes, tags, hourly rates, amounts and billing status;
- Master data: the client's clients, projects and activities, including names and notes stored there;
- Logs: activity log (who changed what and when), webhook delivery logs, technical identifiers of devices, tokens and push subscriptions;
- Contents of imports and exports created by the client.

2.4 Categories of data subjects: the client and its team members, their clients and contact persons, where the client records them in master data or notes.

2.5 The contractor does not process this data for its own purposes. In particular, it is not used for advertising or to train artificial intelligence systems.

§ 3 Right to issue instructions

3.1 The contractor processes the data only on documented instructions from the client. The instructions result from this agreement, the terms and the settings the client makes in HORAKA; the latter are individual instructions in electronic form.

3.2 The client issues further instructions in text form to the address above. Verbal instructions must be confirmed in text form without delay.

3.3 If the contractor considers an instruction unlawful, it informs the client without delay. It may suspend execution until the client confirms or changes the instruction.

3.4 Processing outside the instructions only takes place if the contractor is required to do so by Union or Member State law; in that case it informs the client of the legal requirement before processing unless that law prohibits it.

§ 4 Obligations of the contractor

4.1 The contractor commits the persons authorised to process the data to confidentiality, unless they are already subject to a statutory duty of confidentiality. The commitment continues after their activity ends.

4.2 The contractor keeps a record of all categories of processing activities under Art. 30 (2) GDPR.

4.3 The contractor informs the client without delay if a supervisory authority takes action against it that concerns the processing on behalf of the client.

4.4 The contractor has not appointed a data protection officer; the requirements of Art. 37 GDPR and § 38 BDSG are not met. The contact for all data protection matters is the address above.

§ 5 Technical and organisational measures

5.1 The contractor takes the measures described in Annex 1 under Art. 32 GDPR and maintains them for the duration of the agreement.

5.2 The measures may be adapted in the course of technical development as long as the level of protection is not reduced. Significant changes are documented.

§ 6 Sub processors

6.1 The client hereby gives general authorisation to engage further processors. The sub processors engaged at the time the contract is concluded are listed in Annex 2 and are hereby approved.

6.2 If the contractor intends to engage a further sub processor or to replace an existing one, it informs the client in text form at least four weeks in advance. The client may object to the change within two weeks for an important data protection reason; in that case either party may terminate the contract for use as of the date of the change.

6.3 The contractor commits each sub processor to data protection obligations equivalent to those of this agreement and remains responsible to the client for its conduct.

6.4 Services to which the client itself has data transmitted (such as webhooks, API access, EARLY) and ancillary services in which third parties have no access to the data processed on behalf of the client do not count as sub processing.

§ 7 Support for the client

7.1 The contractor supports the client with suitable technical and organisational measures in responding to requests from data subjects for access, rectification, erasure, restriction, data portability and objection. For this purpose HORAKA provides in particular the workspace data export, the per account data copy, editing and deleting entries and accounts, and deletion of the workspace.

7.2 If a data subject contacts the contractor directly, the contractor forwards the request to the client without delay and does not answer it itself.

7.3 The contractor supports the client in complying with Art. 32 to 36 GDPR, taking into account the nature of processing and the information available to it.

§ 8 Personal data breaches

8.1 The contractor notifies the client in text form without delay, usually within 24 hours of becoming aware, of any breach of the protection of the client's personal data.

8.2 Where available, the notification contains a description of the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences and the measures taken or proposed.

8.3 Notifying the supervisory authority and informing the data subjects is the responsibility of the client.

§ 9 Return and deletion

9.1 The client can download its data at any time during the term as a full data export (JSON and CSV). This fulfils the return obligation under Art. 28 (3) (g) GDPR.

9.2 If the client requests deletion of the workspace, the contractor permanently deletes all data processed on behalf of the client after 14 days. Copies in backups are overwritten in the regular backup cycle.

9.3 The contractor may keep data subject to a statutory retention obligation (invoices and anonymised billing records) and documentation serving as evidence of proper processing beyond the end of the agreement.

§ 10 Evidence and inspections

10.1 On request, the contractor demonstrates compliance with the obligations of this agreement in a suitable manner, in particular by providing information and the documentation of the technical and organisational measures.

10.2 After prior notice with a reasonable period and during normal business hours, the client may satisfy itself of compliance. Inspections are to be limited to what is necessary and must not disrupt operations disproportionately.

10.3 For inspections that go beyond simple information and are not prompted by a specific reason, the contractor may charge reasonable compensation for the effort.

§ 11 Place of processing

The data processed on behalf of the client is stored and processed on servers in Germany. When delivered through Cloudflare, requests are routed through Cloudflare servers; a transfer to a third country only takes place if the requirements of Art. 44 et seq. GDPR are met, in particular on the basis of the EU standard contractual clauses.

§ 12 Liability

Art. 82 GDPR applies. Between the parties, the liability provisions of the terms also apply.

§ 13 Final provisions

13.1 If this agreement and the terms contradict each other, this agreement takes precedence for processing on behalf of the client.

13.2 The law of the Federal Republic of Germany applies.

13.3 Should any provision of this agreement be invalid, the validity of the remaining provisions remains unaffected.

Annex 1: Technical and organisational measures (Art. 32 GDPR)

Confidentiality

- **Physical access control:** The servers are located in a data centre of Hetzner Online GmbH in Germany. Hetzner as operator of the data centre ensures physical access protection (separation, video surveillance, logging).
- **System access control:** Sign in with email address and password (at least ten characters, stored only as a hash), optional two factor authentication and passkeys; sign in attempts are rate limited. Administrative access to the servers is restricted to the contractor and secured with key based authentication. For web requests the servers are only reachable through Cloudflare.
- **Data access control:** Roles owner, admin and member with graded permissions; every request is checked against the caller's permissions. API tokens carry restricted permissions, can be time limited and revoked and are stored only as a hash.
- **Separation control:** Every record belongs to exactly one workspace; every query is limited to the workspace of the signed in account. Test and production systems use separate databases with separate credentials.
- **Pseudonymisation:** Secrets such as tokens and links are only stored as a hash or encrypted; files are not publicly accessible.

Integrity

- **Transfer control:** Every transfer is TLS encrypted, including between Cloudflare and the servers. Webhooks carry an HMAC signature, target addresses are checked against internal networks. Exports can only be downloaded by the account that created them.
- **Input control:** Changes to entries are stored in the activity log with the time and the account that made them.

Availability and resilience

- Regular backups of the database and files.
- Prompt installation of security updates for the operating system and application.
- Monitoring of the systems and background processing.
- Rate limits per account and token to protect against overload.

Procedures for review and assessment

- **Data protection by default:** no analytics or tracking services; web push notifications only after the person switches them on; reminders can be switched off.
- **Automated deletion routines:** exports and import files after seven days, webhook delivery logs and incoming events after 30 days, deletion markers for syncing after 90 days, workspaces after the deletion notice period.
- **Order control:** sub processors are only engaged under a contract pursuant to Art. 28 GDPR; instructions are given in text form.

Annex 2: Sub processors

Company	Service	Place of processing
---------	---------	---------------------

Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany	Operation of the servers including database, files and backups	Germany
Cloudflare Germany GmbH, Rosental 7, 80331 Munich, Germany	Delivery of the website as a proxy, protection against attacks, protection of sign up (Turnstile)	European Union; additionally EU standard contractual clauses
Stripe Payments Europe, Limited, 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Ireland	Processing of payments and invoices for the subscription; receives the workspace name and the owner's email address and language, no time entries	Ireland; transfer to Stripe, Inc. (USA) on the basis of the EU standard contractual clauses

The contractor sends emails through its own mail server; no further service provider is involved.

The German version of this agreement is authoritative.

Last updated: 15 October 2026