This is a convenience translation. Only the German version is legally binding. German version: knotenhirn.dev/site/avv.pdf

Data processing agreement

under Art. 28 GDPR · As of October 2026

Controller (Auftraggeber): the customer who uses Knotenhirn for their team

Processor (Auftragnehmer): Michael Schwarz, Kirchplatz 3, 01728 Bannewitz, Germany, email knotenhirn@michael-schwarz.dev

§ 1 Subject matter and scope

1. The processor operates Knotenhirn, a hosted service for a team's shared notes, which are read and edited in the browser and by AI agents via the Model Context Protocol (MCP). If the controller's team stores personal data in Knotenhirn, the processor processes them on the controller's behalf.
2. This agreement applies to every team that uses Knotenhirn, including during the free trial. It supplements the general terms and conditions (AGB) at knotenhirn.dev/agb (English translation: knotenhirn.dev/en/terms) and takes precedence over them in matters of data protection.
3. It applies as long as the processor processes the team's data, that is also after the end of a subscription, until the data have been deleted under § 9.

§ 2 Nature, purpose, data and data subjects

Annex 1 describes the nature and purpose of the processing, the types of data and the categories of data subjects.

§ 3 Instructions

1. The processor processes the data only on documented instructions from the controller, unless Union law or German law requires it to process them otherwise. In that case, it informs the controller of that legal requirement before processing, unless the law prohibits this.
2. Instructions are this agreement, the AGB and the settings and actions that admins and members of the team make in Knotenhirn. The controller gives further instructions by email.
3. If the processor considers an instruction unlawful, it informs the controller without undue delay.

§ 4 Confidentiality

The processor operates Knotenhirn itself. If it engages further persons who gain access to the data, it commits them to confidentiality beforehand, unless they are under a statutory obligation of confidentiality. The processor accesses the team's content only if this is necessary for operation, troubleshooting or at the controller's request.

§ 5 Security of processing

1. The processor takes the technical and organisational measures under Art. 32 GDPR described in Annex 2.

2. It may adapt the measures to the state of the art as long as the level of protection does not decrease.

§ 6 Subprocessors

1. The controller agrees to the use of the subprocessors named in Annex 3.
2. If the processor intends to engage a further subprocessor or to replace one, it informs the controller by email at least four weeks in advance. The controller can object until the change on important grounds relating to data protection law. If the parties cannot agree, the controller can terminate the contract for Knotenhirn with effect from the time of the change.
3. The processor imposes obligations on subprocessors that correspond to this agreement.

§ 7 Assistance to the controller

1. The processor assists the controller in responding to requests from data subjects under Chapter III GDPR. Notes can be read, changed, exported and deleted in Knotenhirn itself. If a data subject contacts the processor directly, the processor forwards the request to the controller.
2. It also assists the controller with the obligations under Art. 32 to 36 GDPR, as far as it has the necessary information.

§ 8 Personal data breaches

If the processor becomes aware of a breach of the security of the controller's personal data, it notifies the controller without undue delay, if possible within 48 hours, by email to the team's admins. The notification contains, as far as known, the information under Art. 33(3) GDPR. The processor immediately takes the measures necessary to secure the data and to mitigate possible consequences.

§ 9 Return and deletion

1. The controller can receive its team's data as Markdown during and after the contract (AGB § 9).
2. After the end of the contract, the processor deletes the team's data completely on the controller's instruction, unless there is a statutory obligation to retain them, and confirms the deletion by email. If an admin dissolves the team in the admin area, the data are deleted immediately. The data disappear from the backups after 14 days at the latest.

§ 10 Evidence and audits

1. On request, the processor makes available to the controller the information necessary to demonstrate compliance with this agreement.
2. After timely notice, the controller can audit compliance itself or through an auditor bound to confidentiality. Audits take place during normal business hours, do not disrupt operation unnecessarily and cover the subprocessors' data centres only through their evidence and certificates.

§ 11 Place of processing

The processor processes the data in the European Union. The application, the database and the backups are located in Germany; the AI functions use only the EU endpoint of Google Vertex AI. A transfer to a third country takes place only under § 6 and subject to the conditions of Art. 44 et seq. GDPR. Google Cloud EMEA Limited belongs to a group based in the USA; Google is certified under the EU-US Data Privacy Framework.

§ 12 Final provisions

1. Liability is governed by Art. 82 GDPR; otherwise the provisions of the AGB apply.
2. The processor announces changes to this agreement by email at least six weeks in advance; AGB § 11 applies accordingly.
3. If a provision is invalid, the rest of the agreement remains valid.
4. German law applies. The agreement is available in electronic form (Art. 28(9) GDPR). Anyone who needs a signed copy writes to knotenhirn@michael-schwarz.dev.

Annex 1: Subject matter of the processing

Nature and purpose

Storing, organising, searching and providing a team's notes in the browser and via MCP, including the history of every change, search by meaning, the automatic topics, the hints about similar notes and the overview of knowledge gaps.

Types of data

- Contents of the notes, titles, groups and links, with all personal data the team stores in them
- History of the notes: who changed what, when and by which channel (browser or MCP)
- Names and email addresses of the team members, their roles and group visibilities
- Search queries of AI agents via MCP, for the overview of knowledge gaps (at most 60 days)
- Embeddings, that is number vectors computed from note texts and search queries

Special categories of personal data (Art. 9 GDPR) are not intended. If the team stores them nevertheless, the controller is responsible for ensuring that this is permitted.

Data subjects

- Members of the team
- Persons about whom notes contain something, for example customers, contacts, suppliers or employees of the controller

This agreement does not cover data that the processor processes as a controller in its own right, for example for sign-in, billing via Stripe or cancellations. For these, the privacy policy at knotenhirn.dev/datenschutz (English translation: knotenhirn.dev/en/privacy) applies.

Annex 2: Technical and organisational measures (Art. 32 GDPR)

Confidentiality

- **Physical access:** The servers are located in a data centre of Hetzner Online GmbH in Nuremberg that is certified to ISO/IEC 27001. Hetzner provides physical access control, video surveillance and access logs.
- **Access to the server:** Sign-in only with an SSH key; passwords are disabled. After five failed attempts, fail2ban blocks the address for one hour. Two firewalls (Hetzner Cloud Firewall and firewalld) let only SSH, HTTP and HTTPS through. The key for automatic deployments may only run the installation command.
- **Access to Knotenhirn:** Knotenhirn has no passwords of its own. People sign in via Microsoft or Google. AI agents sign in via OAuth with a person's account; every request carries an access token that Knotenhirn checks.
- **Data access:** Admins manage members and roles. Groups determine who sees which notes. An AI agent sees only what the person whose account it is connected with may see.
- **Separation:** In the database, every team is separated from all others by Row Level Security; the rules also bind the owner of the tables. Automated tests check the separation. The application accesses the database with its own database user without administrative rights.
- **Pseudonymisation:** The overview of knowledge gaps names no names or email addresses. Links for confirming a cancellation are stored only as a hash value.

Integrity

- **Transmission:** All connections are encrypted with TLS (HTTPS, certificates from Let's Encrypt); HSTS commits browsers to this. A Content Security Policy lets the browser run only the application's own scripts and forbids embedding in other sites; further security headers prevent MIME sniffing and limit the referrer. The database is reachable only in the server's internal network, not from the internet. The AI functions call only the EU endpoint of Google Vertex AI; the service key for this is readable only by the application.
- **Input:** For every change to a note, Knotenhirn records who made it, when and by which channel. Earlier versions can be viewed and restored.

Availability and resilience

- The database is backed up daily; the backups are kept for 14 days. In addition, Hetzner backs up the whole server daily.
- Deleted notes first remain in the team's recycle bin.
- The operating system installs security updates automatically. Application and database run in separate containers with memory limits and restart by themselves after an error.

Review and data protection by default

- Knotenhirn uses no analytics, tracking or advertising tools. The public pages load nothing from third-party servers. They set a cookie only when a person chooses a language themselves: “knotenhirn_sprache” contains only the chosen language (de or en) and expires after one year.
- Automated tests run on every change to Knotenhirn's code.
- The processor reviews the measures with every major change and at least once a year.

Annex 3: Subprocessors

Company	Service	Place of processing
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany	Servers, data centre and backups	Germany (Nuremberg)
Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Ireland	Google Vertex AI: embeddings from note texts and search queries, suggestions for topic names from note titles	European Union (EU endpoint)