

Data processing agreement

Annex to the terms of the KI-Denkraum

Version of 4 October 2026 · identifier denkraum-avv-2026-10-04 · kidenkraum.com/en/avv/2026-10-04

English translation for information purposes. Only the German version is authoritative: kidenkraum.com/de/avv/2026-10-04

between the **Customer** who takes out a subscription to the KI-Denkraum (controller) and **lennartgehl.com GmbH**, Hans-Henny-Jahnn-Weg 53, 22085 Hamburg, Local Court (Amtsgericht) Hamburg HRB 173152, represented by the managing director Lennart Maximilian Gehl (**provider**, processor).

§ 1 Conclusion of the contract and scope

(1) This agreement is an annex to the Terms of the KI-Denkraum (§ 17(2) of the Terms). The Customer and the provider agree to it when a subscription is taken out, without a separate declaration being required. The version valid at the time of purchase is authoritative; the provider stores which version applied.

(2) The agreement applies to the extent that the provider processes personal data of Users on behalf of the Customer. That is the case as soon as the Customer creates a team in the KI-Denkraum, and for as long as the team exists. Users are the natural persons to whom the Customer gives personal access through the team, including the persons with the role of owner or admin.

(3) The agreement is available at kidenkraum.com as a page and as a PDF and can be saved and printed (electronic form under Art. 28(9) GDPR).

(4) For processing on behalf of the Customer, this agreement takes precedence over the Terms. In all other respects, the definitions of the Terms apply.

§ 2 Subject matter, nature, purpose and duration

(1) The subject matter is the provision of personal access to the KI-Denkraum for the Users authorised by the Customer within the scope of a team's subscription. This includes:

1. invitations to the business email addresses that owners or admins enter;
2. team management: membership, roles (owner, admin, member), seats, invitation status and the log of these operations;
3. the administration of the invited Users' accounts, to the extent it serves team access: registration, sign-in, password, downloading their own data, deleting the account;
4. the associated emails, in particular invitation, confirmation of the address and password reset;
5. the personal saved list and ratings of episodes, to the extent the Platform stores them in a User's account, as well as the search.

(2) Nature of the processing: collecting, storing, organising, matching, displaying to the User and to owners and admins, sending by email, deleting.

(3) The data serve exclusively the services under paragraph 1. The Platform does not transmit them to any AI model; if the search uses an AI model, it passes only the entered search term to it via Amazon Web Services in the EU, without reference to the account and without storage by the operator of the model (Annex 2). For support and operations, for example when clarifying an enquiry or an error, the provider may use an AI model via Amazon Web Services in the EU (Annex 2), and only in a separate working session set up for that

purpose; AWS does not store the data in the process and does not pass them on to the developer of the model. The provider does not use the data for training AI models or for advertising.

(4) The processing lasts as long as the team's subscription; § 10 applies beyond that.

§ 3 Data subjects and types of data

(1) The data subjects are employees of the Customer and other persons authorised by the Customer, in particular freelancers working for it, as well as persons the Customer invites, even before acceptance of the invitation.

(2) The following are processed:

1. account data: name, business email address, name of the business, password (only as a hash); for sign-in with Google additionally the Google identifier and a link to the profile picture;
2. team data: membership of the team, role, time of joining;
3. invitation data: invited address, intended role, inviting person, times of invitation, expiry, acceptance or withdrawal;
4. team management log: who sent, resent or withdrew an invitation, changed a role or removed a member, and when, with the address or identifier of the person concerned;
5. sign-in and log data: times of registration, confirmation and sign-ins, IP address, browser identifier;
6. emails: recipient address, name, content, delivery status;
7. saved list and ratings, to the extent stored in the account: identifier, edition or collection and version of saved episodes and use cases, rating of an episode, each with its time;
8. search terms: only for the duration of the search; the Platform does not store them against the account, as part of the requested address they remain in the technical logs of the hosting provider for up to 30 days.

(3) Special categories of personal data (Art. 9 and 10 GDPR) are not covered. The Customer also does not enter such data in free-text fields, such as the name of the team.

(4) Reading behaviour is not covered: the provider does not analyse on a user-related basis which Content a User accesses, searches for or downloads, and shows owners and admins none of it. Such accesses appear only in the technical logs of the hosting. The saved list and ratings (paragraph 2 no. 7) are visible only to the User themselves, never to owners or admins. Aggregated analyses with which the provider improves the selection and presentation of the Content are carried out under its own responsibility (§ 4(1) no. 7).

§ 4 Distinction from the provider's own responsibility

(1) This agreement does not cover processing for which the provider itself is responsible:

1. performance of the contract and billing with the Customer, including checkout, payment, invoices and the number of seats booked;
2. the account of the person who orders the subscription for the Customer, to the extent it serves the performance of the contract;
3. records of the confirmation of business status (Unternehmereigenschaft) and of the acceptance of the Terms and this agreement;
4. the security of the Platform as a whole and the prevention of abuse, such as analysing technical logs to detect attacks and blocking abusive access;

5. the fulfilment of legal obligations, such as retention obligations;
6. the trial and accounts outside a team, such as an account that already existed before the invitation and an account after the end of team membership (§ 10(3));
7. aggregating the saved list and ratings into totals without reference to individual persons, never per team or Customer and only across at least ten Users; the totals contain no personal data.

(2) This distinction does not narrow the processing on behalf of the Customer. Invitations, team management and the Users' accounts remain processing on behalf of the Customer, to the extent they serve team access, even if the provider needs information from them for a purpose under paragraph 1. In that case it uses only what is necessary for that purpose; Stripe, for example, receives from team management only the number of seats, no names or addresses. The measures under Annex 1 remain an obligation under this agreement.

(3) The privacy policy of the KI-Denkraum applies to the processing under paragraph 1.

§ 5 Instructions

(1) The provider processes the data only on documented instructions from the Customer, including with regard to a transfer to a third country. If the law of the European Union or of Germany requires it to process the data otherwise, it informs the Customer of that requirement beforehand, unless the law prohibits such information.

(2) The Customer's instructions are the Terms, this agreement, the Users' entries in the saved list, ratings and search and the settings that owners and admins make in team management: inviting, resending or withdrawing invitations, changing roles, removing members. The Customer also instructs the provider to enable every User to download their data and delete their account on the account page.

(3) Further instructions are issued by the Customer's legal representatives or the owner of the team in text form (Textform, e.g. by email) to hallo@kidenkraum.com. The provider documents them. An instruction that goes beyond the agreed scope of services it treats as a request for an amendment of the contract.

(4) If the provider considers an instruction to be unlawful, it points this out to the Customer without undue delay. It may suspend execution until the Customer confirms or changes the instruction.

§ 6 Confidentiality and security

(1) The provider uses only persons who have committed themselves to confidentiality or are subject to a statutory obligation of confidentiality, and gives them only the access their task requires. The obligation continues after the end of the contract.

(2) The provider implements the technical and organisational measures under Art. 32 GDPR described in Annex 1. It may develop them further as long as the level of protection does not decrease, and communicates material changes in text form.

(3) The contact for data protection is the management at hallo@kidenkraum.com. The provider has not designated a data protection officer because there is no obligation to do so (Art. 37 GDPR, § 38 of the German Federal Data Protection Act (BDSG)).

§ 7 Sub-processors

(1) The Customer grants general authorisation to engage sub-processors (Art. 28(2) GDPR). Those engaged at the time of conclusion of the contract are listed in Annex 2; the current list is available at /en/avv (Annex

2).

(2) Before the provider engages or replaces a sub-processor, it informs the Customer at least 30 days in advance in text form, by email to the owner of the team.

(3) The Customer may object to the change in text form on objective grounds under data protection law within 14 days of receipt of the information. The parties then seek a solution. If that fails, the Customer may end the team's subscription by extraordinary termination (außerordentliche Kündigung), effective at the time the change takes effect; the provider refunds fees paid in advance pro rata in accordance with § 10(8) of the Terms.

(4) The provider binds each sub-processor by contract to the data protection obligations of this agreement, to the extent they apply to that sub-processor's service, as a rule through that sub-processor's data processing agreement. The provider is liable to the Customer for the performance of those obligations (Art. 28(4) GDPR).

§ 8 Transfers to third countries

(1) If a sub-processor processes data outside the EU and the EEA or accesses them from there, this happens only under the conditions of Art. 44 to 49 GDPR: on the basis of the adequacy decision for the EU-US Data Privacy Framework (Implementing Decision (EU) 2023/1795) for certified recipients, or of standard contractual clauses (Implementing Decision (EU) 2021/914). Annex 2 states the basis for each service.

(2) If a basis ceases to apply, the provider switches the transfer to another safeguard or ends it, and informs the Customer.

§ 9 Assistance and personal data breaches

(1) The provider assists the Customer with appropriate technical and organisational measures in relation to the rights of data subjects (Art. 12 to 22 GDPR). Owners and admins can remove members and withdraw invitations; every User can download their data and delete their account. If a User asks the provider for an export or the deletion of their account, the provider does so in accordance with § 5(2). Other requests concerning team management it forwards to the Customer without undue delay.

(2) With the obligations under Art. 32 to 36 GDPR, the provider assists the Customer with the information available to it.

(3) The provider notifies the Customer of a personal data breach affecting data processed on behalf of the Customer without undue delay after becoming aware of it, where possible within 48 hours. The notification is sent by email to the owner of the team and contains, as far as known, the information under Art. 33(3) GDPR; missing information the provider supplies subsequently. It takes measures without undue delay to remedy the breach and mitigate its effects. The Customer notifies the supervisory authority and the data subjects; the provider does so only on instruction or on the basis of its own legal obligation.

(4) For assistance that goes beyond the functions of the Platform and a minor effort, the provider may demand reasonable remuneration, unless the assistance is due to a breach of its own obligations.

§ 10 Deletion and return

(1) During the term, the provider deletes a member's team membership as soon as owners or admins remove the member, and an invitation 30 days after its acceptance, withdrawal or expiry; an invitation expires after seven days (§ 9(4) of the Terms). Entries in the team management log it deletes twelve months after they are

created. It deletes entries of the saved list and ratings as soon as the User removes them or deletes their account.

(2) After the end of the team's subscription, the provider deletes the team data, the invitations and the team management log within 30 days. If the Customer requests their return in text form before the end, the provider first hands over a list of the members and invitations in a common machine-readable format. Copies in backups are overwritten in the regular cycle. Data the provider must retain by law it blocks until the retention period expires. On request it confirms the deletion in text form.

(3) The provider does not delete the Users' accounts when team membership ends. When it ends, by removal from the team or with the end of the team's subscription, the account continues to exist with access to the preview until the User deletes it (§ 10(8) of the Terms). From then on, the provider processes the account data as well as the saved list and ratings under its own responsibility, as with any account outside a team; the privacy policy provides information about this.

§ 11 Evidence and audits

(1) On request, the provider makes available to the Customer the information necessary to demonstrate compliance with the obligations under Art. 28 GDPR, primarily by way of documents: this agreement with its annexes, written information such as answers to questionnaires, and the contracts, certificates and audit reports of the sub-processors, to the extent they make them available for passing on.

(2) If the documents are insufficient in an individual case, the Customer may audit the provider on site, itself or through an auditor bound to confidentiality who is not a competitor of the provider. The Customer announces the audit at least 30 days in advance in text form. It takes place during normal business hours and at most once per calendar year, except where there is a specific reason such as a personal data breach, and must not disrupt operations disproportionately. The Customer bears the costs, including, to the extent reasonable, the provider's effort; this does not apply if the audit reveals a material breach by the provider.

(3) The provider does not operate its own servers. The Customer assesses the data centres on the basis of the sub-processors' certificates and audit reports.

(4) The powers of the supervisory authorities remain unaffected.

§ 12 Obligations of the Customer

(1) The Customer is responsible for the lawfulness of the processing, in particular for being permitted to invite Users and to provide their data to the provider. It informs the Users about the processing (Art. 13 and 14 GDPR). The provider supports it in that every email to Users refers to the privacy policy of the KI-Denkraum.

(2) The Customer invites only business addresses and removes Users who are no longer to have access, for example after they leave.

(3) If the Customer discovers errors or irregularities in the processing, it informs the provider without undue delay.

(4) The Customer's contact person is the owner of the team, unless the Customer names another person in text form.

§ 13 Liability

(1) Towards data subjects, the parties are liable under Art. 82 GDPR.

(2) As between the Customer and the provider, the liability rules of the Terms (§ 16) also apply to claims under this agreement. Art. 82 GDPR remains unaffected.

§ 14 Term, amendments, final provisions

(1) This agreement applies for the term of the subscription and ends with it, without any notice of cancellation being required. § 6(1) and § 10 continue to apply beyond the end.

(2) The parties agree amendments to this agreement in text form or under the procedure for amendments to the Terms (§ 18). For sub-processors, § 7 applies.

(3) The German version is authoritative; the English version is a translation.

(4) In all other respects, the final provisions of the Terms (§ 19) apply, in particular on applicable law and place of jurisdiction.

Annex 1: Technical and organisational measures

As of 4 October 2026.

1. Data centres

- The provider does not operate its own servers. Database and sign-in run at Supabase in Amazon Web Services data centres in Frankfurt am Main (region eu-central-1), the application's server functions at Vercel, likewise in Frankfurt am Main.
- Certifications: Supabase SOC 2 Type 2, Vercel SOC 2 Type 2, Amazon Web Services for the Frankfurt region including ISO 27001 and BSI C5.

2. Access to systems and data

- Every User has a personal account. Invitations go only to business addresses; the server rejects addresses of general email providers.
- The address is confirmed via a link, through the invitation or through a confirmation email whose link is valid for one hour.
- Supabase Auth stores passwords only as a hash (bcrypt).
- Invitation links contain a random 256-bit key, are valid for seven days and can only be accepted with the account of the invited address.
- Only owners and admins see and change members, invitations and seats; the server checks role and team membership for each of these actions.
- Row-level permissions in the database (Row Level Security) limit every access from the browser: a User reads only their own profile and the memberships of their team; invitations and the log are read only by owners and admins of that team.
- The service key with full access to the database is held only on the server. Database functions with elevated privileges, such as looking up an account by email address, can be called only by the server.
- Protection against automated attacks: Cloudflare Turnstile at registration and password reset, at most five registrations per IP address and minute, rate limits of Supabase Auth for sign-in and registration.
- If a person with access leaves, their access rights are revoked and the keys they knew are renewed.
- Administrative access to Supabase, Vercel, Postmark, Cloudflare, Stripe and GitHub is held only by the management, in each case with two-factor authentication.

3. Separation

- The teams are separated from one another by the row-level permissions and the server-side check of team membership.
- Test and production operation use separate databases and keys.

4. Transfer and integrity

- All connections to the Platform and to the services are encrypted via TLS; HSTS permanently binds browsers to HTTPS.
- Supabase and Vercel encrypt stored data with AES-256.
- The team management log records every change with the time and the acting person.
- Changes to the code go through pull requests with mandatory automated checks (unit tests, end-to-end tests, code quality) and an automated review. Known security vulnerabilities in dependencies are reported automatically by GitHub.

5. Availability

- Rate limiting and bot protection reduce the risk of overload.
- Supabase backs up the database daily and keeps the backups for seven days.

6. Data minimisation and deletion

- No analytics, advertising or tracking services, no user-related analysis of reading behaviour. Only the User sees their saved list and ratings; they are aggregated only into totals without reference to individual persons (§ 4(1) no. 7).
- No open and click tracking in emails.
- AI assistance in support only in a separate working session via Amazon Bedrock in the EU (without storage at AWS); its history is deleted when the session ends. In all other working sessions, a technical block prevents queries of personal data.
- If the search uses an AI model, it passes only the search term to it via Amazon Bedrock in the EU, without the identifier of the account; AWS does not store it. The application does not write search terms to any logs of its own.
- Email addresses appear in application logs only in shortened form.
- Rate limits are counted in memory (the working memory of the server) and are not stored.
- Data export and account deletion by the User themselves (§ 9(1)).
- Fixed deletion periods: invitations 30 days after their end, team management log after twelve months, team data 30 days after the end of the subscription (§ 10).
- Logs at the services expire automatically: at Vercel after at most 30 days, the sign-in logs at Supabase after seven days, messages and delivery data at Postmark after 45 days.

7. Organisation and review

- Sub-processors only with a contract under Art. 28 GDPR (Annex 2).
- Reporting channel for security incidents: hallo@kidenkraum.com, assessment by the management, notification of the Customer under § 9(3).
- Only the management has access to the data. If further persons are added, the provider binds them to confidentiality in writing before their first access and instructs them in data protection.
- The management's devices are encrypted.

- The provider reviews these measures at least once a year and adapts them.

Annex 2: Sub-processors

As of 4 October 2026; DPF status checked on 29 September 2026 in the list at dataprivacyframework.gov.

Sub-processor	Service	Place of processing	Safeguard where a third country is involved
Supabase Pte. Ltd. , 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513	Database, sign-in (Supabase Auth)	Amazon Web Services data centres in Frankfurt am Main (eu-central-1); access for operations and support from Singapore and the USA possible	Standard contractual clauses in Supabase's data processing agreement. There is no adequacy decision for Singapore; Supabase is not certified under the Data Privacy Framework.
Vercel Inc. , 440 N Barranca Ave #4133, Covina, CA 91723, USA	Hosting, delivery, server functions, technical logs	Server functions in Frankfurt am Main, delivery via a global network	EU-US Data Privacy Framework (certified, active), additionally standard contractual clauses
AC PM, LLC (Postmark, a company of ActiveCampaign), 1 N Dearborn Street, Suite 500, Chicago, IL 60602, USA	Sending of emails	USA (data centres of Deft and Amazon Web Services)	EU-US Data Privacy Framework (certified as an affiliated company of ActiveCampaign, LLC, active), additionally standard contractual clauses
Cloudflare, Inc. , 101 Townsend Street, San Francisco, CA 94107, USA	Turnstile: check at registration with an email address, including of invited Users, and at password reset, whether a human is filling in the form (IP address, technical characteristics of the browser)	Cloudflare's global network	EU-US Data Privacy Framework (certified, active), additionally standard contractual clauses
Microsoft Ireland Operations Limited , One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland	Email mailbox hallo@kidenkraum.com for enquiries, instructions and notifications concerning team management	Data centres in the EU; access from the USA not excluded	EU-US Data Privacy Framework (Microsoft Corporation certified), additionally standard contractual clauses
Amazon Web Services EMEA SARL , 38 Avenue John F. Kennedy, L-1855 Luxembourg	AI model (Claude via Amazon Bedrock) for support and operations in individual cases, in a separate working session; once the search uses an AI model, the conversion of the search term (model by Cohere via Amazon Bedrock), without the identifier of the account	Data centres in the EU; no storage of inputs and outputs; the developers of the models have no access	Processing in the EU; AWS data processing agreement with standard contractual clauses, Amazon in the EU-US Data Privacy Framework

Notes:

1. The services use their own sub-processors, such as Amazon Web Services, and publish lists of them.
2. According to its own statements, Cloudflare additionally uses the Turnstile signals under its own responsibility to improve bot detection.

3. Stripe and Google are not sub-processors under this agreement, because the provider conducts billing under its own responsibility and Stripe receives only the number of seats from team management, and because Users choose sign-in with Google voluntarily and Google is itself responsible for it.
4. Cover images are delivered by the provider via its own server; Spotify receives no User data in the process.