

Technical and organisational measures

Annex 1 to the DPA of the KI-Denkraum

Version of 9 October 2026 · identifier denkraum-tom-2026-10-09 · kidenkraum.com/en/tom/2026-10-09

English translation for information purposes. Only the German version is authoritative: kidenkraum.com/de/tom/2026-10-09

Annex 1 to the data processing agreement of the KI-Denkraum (kidenkraum.com/en/avv, § 6(2)): the technical and organisational measures under Art. 32 GDPR. As of 9 October 2026.

The provider may develop the measures further as long as the level of protection does not decrease, and communicates material changes in text form. Every version remains available under its date.

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, in teams under an individual contract for 30 days, at most until the end of the term, and can only be accepted with the account of the invited address. In teams under an individual contract, the account of the invited address joins when it signs in.
- In team management, only owners and admins see and change the members, invitations and seats of their team; the server checks role and team membership for each of these actions. The provider's management sees accounts and teams in its administration area, creates teams under an individual contract there, invites for them, changes their term and seats and sets their owner; it changes other teams only on instruction (§ 5 DPA).
- 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. Teams, memberships and invitations are changed only by the server.
- 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 on forms that create an account or trigger an email without a sign-in (for example registration and password reset), rate limits for registration, sign-in and other forms.
- 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 entries and ratings; they are aggregated only into totals without reference to individual persons (§ 4(1) no. 7 DPA).
- 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.
- Search terms appear, as part of the requested address, only in the technical logs of the hosting provider and expire there with them (at most 30 days); the application does not store them against the account.
- 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) DPA).
- 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 or individual contract (§ 10 DPA).
- 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 (list of service providers, part A).
- Reporting channel for security incidents: hallo@kidenkraum.com, assessment by the management, notification of the Customer under § 9(3) DPA.
- 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.