

Technische und organisatorische Maßnahmen

Anlage 1 zum AVV des KI-Denkraums

Stand vom 9. Oktober 2026 · Kennung denkraum-tom-2026-10-09 · kidenkraum.com/de/tom/2026-10-09

Anlage 1 zum Auftragsverarbeitungsvertrag des KI-Denkraums (kidenkraum.com/de/avv, § 6 Abs. 2): die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Stand 9. Oktober 2026.

Der Anbieter darf die Maßnahmen weiterentwickeln, solange das Schutzniveau nicht sinkt, und teilt wesentliche Änderungen in Textform mit. Jeder Stand bleibt unter seinem Datum abrufbar.

1. Rechenzentren

- Der Anbieter betreibt keine eigenen Server. Datenbank und Anmeldung laufen bei Supabase in Rechenzentren von Amazon Web Services in Frankfurt am Main (Region eu-central-1), die Serverfunktionen der Anwendung bei Vercel ebenfalls in Frankfurt am Main.
- Zertifizierungen: Supabase SOC 2 Type 2, Vercel SOC 2 Type 2, Amazon Web Services für die Region Frankfurt unter anderem ISO 27001 und BSI C5.

2. Zugang und Zugriff

- Jeder Nutzer hat ein persönliches Konto. Einladungen gehen nur an geschäftliche Adressen; Adressen allgemeiner E-Mail-Anbieter lehnt der Server ab.
- Die Adresse wird per Link bestätigt, über die Einladung oder über eine Bestätigungsmail, deren Link eine Stunde gilt.
- Passwörter speichert Supabase Auth nur als Hash (bcrypt).
- Einladungslinks enthalten einen zufälligen Schlüssel mit 256 Bit, gelten sieben Tage, in Teams nach Einzelvertrag 30 Tage, längstens bis zum Ende der Laufzeit, und lassen sich nur mit dem Konto der eingeladenen Adresse annehmen. In Teams nach Einzelvertrag tritt das Konto der eingeladenen Adresse mit der Anmeldung bei.
- In der Teamverwaltung sehen und ändern nur Inhaber und Admins Mitglieder, Einladungen und Einzellizenzen ihres Teams; der Server prüft Rolle und Teamzugehörigkeit bei jeder dieser Aktionen. Die Geschäftsführung des Anbieters sieht Konten und Teams in ihrer Verwaltung, legt dort Teams nach Einzelvertrag an, lädt für sie ein, ändert ihre Laufzeit und ihre Einzellizenzen und setzt ihren Inhaber; andere Teams ändert sie nur auf Weisung (§ 5 AVV).
- Zeilenrechte in der Datenbank (Row Level Security) begrenzen jeden Zugriff aus dem Browser: Ein Nutzer liest nur sein eigenes Profil und die Mitgliedschaften seines Teams; Einladungen und Protokoll lesen nur Inhaber und Admins dieses Teams. Team, Mitgliedschaften und Einladungen ändert nur der Server.
- Der Dienstschlüssel mit Vollzugriff auf die Datenbank liegt nur auf dem Server. Datenbankfunktionen mit erhöhten Rechten, etwa die Suche eines Kontos nach E-Mail-Adresse, kann nur der Server aufrufen.
- Schutz vor automatisierten Angriffen: Cloudflare Turnstile auf Formularen, die ohne Anmeldung ein Konto anlegen oder eine Mail auslösen (etwa Registrierung und „Passwort vergessen“), Ratenbegrenzungen für Registrierung, Anmeldung und weitere Formulare.
- Scheidet eine Person mit Zugang aus, werden ihre Zugänge entzogen und die Schlüssel erneuert, die sie kannte.

- Administrative Zugänge zu Supabase, Vercel, Postmark, Cloudflare, Stripe und GitHub hat nur die Geschäftsführung, jeweils mit Zwei-Faktor-Anmeldung.

3. Trennung

- Die Teams sind über die Zeilenrechte und die serverseitige Prüfung der Teamzugehörigkeit voneinander getrennt.
- Test- und Produktivbetrieb nutzen getrennte Datenbanken und Schlüssel.

4. Übertragung und Integrität

- Alle Verbindungen zur Plattform und zu den Diensten laufen verschlüsselt über TLS; HSTS legt Browser dauerhaft auf HTTPS fest.
- Supabase und Vercel verschlüsseln gespeicherte Daten mit AES-256.
- Das Protokoll der Teamverwaltung hält jede Änderung mit Zeitpunkt und handelnder Person fest.
- Änderungen am Code laufen über Pull Requests mit automatischen Pflichtprüfungen (Unit-Tests, End-to-End-Tests, Codequalität) und einer automatischen Durchsicht. Bekannte Sicherheitslücken in Abhängigkeiten meldet GitHub automatisch.

5. Verfügbarkeit

- Ratenbegrenzung und Bot-Schutz verringern das Risiko einer Überlastung.
- Supabase sichert die Datenbank täglich und bewahrt die Sicherungen sieben Tage auf.

6. Datensparsamkeit und Löschung

- Keine Analyse-, Werbe- oder Trackingdienste, keine nutzerbezogene Auswertung des Leseverhaltens. Gespeicherte Einträge und Bewertungen sieht nur der Nutzer selbst; zusammengefasst werden sie nur zu Summen ohne Bezug zu einzelnen Personen (§ 4 Abs. 1 Nr. 7 AVV).
- Keine Öffnungs- und Klickverfolgung in Mails.
- KI-Unterstützung im Support nur in einer getrennten Arbeitssitzung über Amazon Bedrock in der EU (ohne Speicherung bei AWS); deren Verlauf wird beim Beenden gelöscht. In allen anderen Arbeitssitzungen verhindert eine technische Sperre Abfragen personenbezogener Daten.
- Nutzt die Suche ein KI-Modell, gibt sie ihm über Amazon Bedrock in der EU nur den Suchbegriff weiter, ohne Kennung des Kontos; AWS speichert ihn nicht. Die Anwendung schreibt Suchbegriffe in keine eigenen Protokolle.
- Suchbegriffe stehen als Teil der aufgerufenen Adresse nur in den technischen Protokollen des Hostings und laufen dort mit ihnen aus (höchstens 30 Tage); die Anwendung speichert sie nicht zum Konto.
- E-Mail-Adressen stehen in Anwendungsprotokollen nur gekürzt.
- Ratenbegrenzungen zählen im Arbeitsspeicher und werden nicht gespeichert.
- Datenexport und Kontolöschung durch den Nutzer selbst (§ 9 Abs. 1 AVV).
- Feste Löschfristen: Einladungen 30 Tage nach ihrem Ende, Protokoll der Teamverwaltung nach zwölf Monaten, Teamdaten 30 Tage nach Ende des Abos oder Einzelvertrags (§ 10 AVV).
- Protokolle bei den Diensten laufen automatisch aus: bei Vercel nach höchstens 30 Tagen, die Anmeldeprotokolle bei Supabase nach sieben Tagen, Nachrichten und Zustelldaten bei Postmark nach 45 Tagen.

7. Organisation und Überprüfung

- Unterauftragsverarbeiter nur mit Vertrag nach Art. 28 DSGVO (Liste der Dienstleister, Teil A).
- Meldeweg für Sicherheitsvorfälle: hallo@kidenkraum.com, Bewertung durch die Geschäftsführung, Meldung an den Kunden nach § 9 Abs. 3 AVV.
- Zugang zu den Daten hat nur die Geschäftsführung. Kommen weitere Personen hinzu, verpflichtet der Anbieter sie vor dem ersten Zugang schriftlich auf Vertraulichkeit und weist sie in den Datenschutz ein.
- Die Endgeräte der Geschäftsführung sind verschlüsselt.
- Der Anbieter überprüft diese Maßnahmen mindestens einmal im Jahr und passt sie an.