Vertrag über Auftragsverarbeitung

nach Art. 28 DSGVO · Stand: Oktober 2026

Auftraggeber: der Kunde, der Knotenhirn für sein Team nutzt (Verantwortlicher)

Auftragnehmer: Michael Schwarz, Kirchplatz 3, 01728 Bannewitz, Deutschland, E-Mail knotenhirn@michael-schwarz.dev (Auftragsverarbeiter)

§ 1 Gegenstand und Geltung

1. Der Auftragnehmer betreibt Knotenhirn, einen gehosteten Dienst für gemeinsame Notizen eines Teams, die im Browser und über das Model Context Protocol (MCP) von KI-Agenten gelesen und bearbeitet werden. Legt das Team des Auftraggebers personenbezogene Daten in Knotenhirn ab, verarbeitet der Auftragnehmer sie in seinem Auftrag.
2. Dieser Vertrag gilt für jedes Team, das Knotenhirn nutzt, auch während der kostenlosen Testphase. Er ergänzt die Allgemeinen Geschäftsbedingungen (AGB) unter knotenhirn.dev/agb und geht ihnen in Fragen des Datenschutzes vor.
3. Er gilt, solange der Auftragnehmer Daten des Teams verarbeitet, also auch nach Ende eines Abos, bis die Daten nach § 9 gelöscht sind.

§ 2 Art, Zweck, Daten und betroffene Personen

Art und Zweck der Verarbeitung, die Arten der Daten und die Kategorien betroffener Personen beschreibt Anlage 1.

§ 3 Weisungen

1. Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn, das Recht der Union oder Deutschlands verpflichtet ihn zu einer anderen Verarbeitung. In diesem Fall teilt er dem Auftraggeber diese Pflicht vor der Verarbeitung mit, sofern das Gesetz das nicht verbietet.
2. Weisungen sind dieser Vertrag, die AGB und die Einstellungen und Aktionen, die Admins und Mitglieder des Teams in Knotenhirn vornehmen. Weitere Weisungen erteilt der Auftraggeber per E-Mail.
3. Hält der Auftragnehmer eine Weisung für rechtswidrig, teilt er das dem Auftraggeber unverzüglich mit.

§ 4 Vertraulichkeit

Der Auftragnehmer betreibt Knotenhirn selbst. Setzt er weitere Personen ein, die Zugriff auf die Daten erhalten, verpflichtet er sie vorher zur Vertraulichkeit, soweit sie keiner gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer greift auf Inhalte des Teams nur zu, wenn es für den Betrieb, die Fehlerbehebung oder auf Wunsch des Auftraggebers nötig ist.

§ 5 Sicherheit der Verarbeitung

1. Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die Anlage 2 beschreibt.
2. Er darf die Maßnahmen an den Stand der Technik anpassen, solange das Schutzniveau nicht sinkt.

§ 6 Unterauftragsverarbeiter

1. Der Auftraggeber stimmt dem Einsatz der in Anlage 3 genannten Unterauftragsverarbeiter zu.
2. Will der Auftragnehmer einen weiteren Unterauftragsverarbeiter einsetzen oder einen ersetzen, teilt er das dem Auftraggeber mindestens vier Wochen vorher per E-Mail mit. Der Auftraggeber kann bis zum Wechsel aus wichtigem datenschutzrechtlichem Grund widersprechen. Können sich die Parteien nicht einigen, kann der Auftraggeber den Vertrag über Knotenhirn zum Zeitpunkt des Wechsels kündigen.
3. Der Auftragnehmer legt Unterauftragsverarbeitern Pflichten auf, die diesem Vertrag entsprechen.

§ 7 Unterstützung des Auftraggebers

1. Der Auftragnehmer unterstützt den Auftraggeber dabei, Anträge betroffener Personen nach Kapitel III DSGVO zu beantworten. Notizen lassen sich in Knotenhirn selbst lesen, ändern, exportieren und löschen. Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet er die Anfrage an den Auftraggeber weiter.
2. Er unterstützt den Auftraggeber außerdem bei den Pflichten aus Art. 32 bis 36 DSGVO, soweit ihm die nötigen Informationen vorliegen.

§ 8 Verletzungen des Schutzes personenbezogener Daten

Erfährt der Auftragnehmer von einer Verletzung des Schutzes personenbezogener Daten des Auftraggebers, meldet er sie ihm unverzüglich, möglichst innerhalb von 48 Stunden, per E-Mail an die Admins des Teams. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO. Der Auftragnehmer ergreift sofort die Maßnahmen, die nötig sind, um die Daten zu sichern und mögliche Folgen zu mindern.

§ 9 Rückgabe und Löschung

1. Der Auftraggeber kann den Datenbestand seines Teams während und nach dem Vertrag als Markdown erhalten (AGB § 9).
2. Nach Ende des Vertrags löscht der Auftragnehmer die Daten des Teams auf Weisung des Auftraggebers vollständig, soweit keine gesetzliche Pflicht zur Aufbewahrung besteht, und bestätigt die Löschung per E-Mail. Löst ein Admin das Team in der Verwaltung auf, werden die Daten sofort gelöscht. Aus den Sicherungen verschwinden die Daten spätestens nach 14 Tagen.

§ 10 Nachweise und Kontrollen

1. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die Informationen zur Verfügung, die nötig sind, um die Einhaltung dieses Vertrags nachzuweisen.
2. Der Auftraggeber kann die Einhaltung nach rechtzeitiger Ankündigung selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer kontrollieren. Kontrollen finden zu den üblichen Geschäftszeiten statt, stören den Betrieb nicht unnötig und betreffen die Rechenzentren der Unterauftragsverarbeiter nur über deren Nachweise und Zertifikate.

§ 11 Ort der Verarbeitung

Der Auftragnehmer verarbeitet die Daten in der Europäischen Union. Die Anwendung, die Datenbank und die Sicherungen liegen in Deutschland; die KI-Funktionen nutzen ausschließlich den EU-Endpunkt von Google Vertex AI. Eine Verlagerung in ein Drittland erfolgt nur nach § 6 und unter den Voraussetzungen der Art. 44 ff. DSGVO. Google Cloud EMEA Limited gehört zu einem Konzern mit Sitz in den USA; Google ist nach dem EU-US Data Privacy Framework zertifiziert.

§ 12 Schlussbestimmungen

1. Die Haftung richtet sich nach Art. 82 DSGVO; im Übrigen gelten die Regelungen der AGB.
2. Änderungen dieses Vertrags teilt der Auftragnehmer mindestens sechs Wochen vorher per E-Mail mit; AGB § 11 gilt entsprechend.
3. Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam.
4. Es gilt deutsches Recht. Der Vertrag liegt elektronisch vor (Art. 28 Abs. 9 DSGVO). Wer eine unterschriebene Fassung braucht, schreibt an knotenhirn@michael-schwarz.dev.

Anlage 1: Gegenstand der Verarbeitung

Art und Zweck

Speichern, Ordnen, Durchsuchen und Bereitstellen der Notizen eines Teams im Browser und über MCP, einschließlich der Historie jeder Änderung, der Suche nach Bedeutung, der automatischen Themen, der Hinweise auf ähnliche Notizen und der Übersicht über Wissenslücken.

Arten der Daten

- Inhalte der Notizen, Titel, Gruppen und Verweise, mit allen personenbezogenen Daten, die das Team darin ablegt
- Historie der Notizen: wer was wann auf welchem Weg (Browser oder MCP) geändert hat
- Namen und E-Mail-Adressen der Teammitglieder, ihre Rollen und Gruppensichtbarkeiten
- Suchanfragen von KI-Agenten über MCP, für die Übersicht über Wissenslücken (höchstens 60 Tage)
- Embeddings, also Zahlenvektoren, die aus Notiztexten und Suchanfragen berechnet werden

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht vorgesehen. Legt das Team sie dennoch ab, ist der Auftraggeber dafür verantwortlich, dass das zulässig ist.

Betroffene Personen

- Mitglieder des Teams
- Personen, über die Notizen etwas enthalten, etwa Kunden, Ansprechpartner, Lieferanten oder Beschäftigte des Auftraggebers

Nicht Gegenstand dieses Vertrags sind Daten, die der Auftragnehmer als eigener Verantwortlicher verarbeitet, etwa für die Anmeldung, die Abrechnung über Stripe oder Kündigungen. Dafür gilt die Datenschutzerklärung unter knotenhirn.dev/datenschutz.

Anlage 2: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- **Zutritt:** Die Server stehen in einem Rechenzentrum der Hetzner Online GmbH in Nürnberg, das nach ISO/IEC 27001 zertifiziert ist. Zutrittskontrolle, Videoüberwachung und Zugangsprotokolle stellt Hetzner.
- **Zugang zum Server:** Anmeldung nur per SSH-Schlüssel, Passwörter sind abgeschaltet. Nach fünf Fehlversuchen sperrt fail2ban die Adresse für eine Stunde. Zwei Firewalls (Hetzner Cloud Firewall und firewalld) lassen nur SSH, HTTP und HTTPS durch. Der Schlüssel für automatische Auslieferungen darf nur den Installationsbefehl ausführen.
- **Zugang zu Knotenhirn:** Knotenhirn hat keine eigenen Passwörter. Personen melden sich über Microsoft oder Google an. KI-Agenten melden sich per OAuth mit dem Konto einer Person an; jede Anfrage trägt ein Zugangstoken, das Knotenhirn prüft.
- **Zugriff:** Admins verwalten Mitglieder und Rollen. Gruppen legen fest, wer welche Notizen sieht. Ein KI-Agent sieht nur, was die Person sehen darf, mit deren Konto er verbunden ist.
- **Trennung:** Jedes Team ist in der Datenbank per Row Level Security von allen anderen getrennt; die Regeln binden auch den Eigentümer der Tabellen. Automatisierte Tests prüfen die Trennung. Die Anwendung greift mit einem eigenen Datenbankbenutzer ohne Verwaltungsrechte zu.
- **Pseudonymisierung:** Die Übersicht über Wissenslücken nennt keine Namen oder E-Mail-Adressen. Links zur Bestätigung einer Kündigung werden nur als Hashwert gespeichert.

Integrität

- **Weitergabe:** Alle Verbindungen sind per TLS verschlüsselt (HTTPS, Zertifikate von Let's Encrypt); HSTS verpflichtet Browser darauf. Eine Content Security Policy lässt im Browser nur Skripte der Anwendung selbst laufen und verbietet das Einbetten in fremde Seiten; weitere Sicherheits-Header verhindern MIME-Sniffing und begrenzen den Referrer. Die Datenbank ist nur im internen Netz des Servers erreichbar, nicht aus dem Internet. Die KI-Funktionen rufen nur den EU-Endpunkt von Google Vertex AI auf; der Dienstschlüssel dafür ist nur für die Anwendung lesbar.
- **Eingabe:** Zu jeder Änderung einer Notiz hält Knotenhirn fest, wer sie gemacht hat, wann und auf welchem Weg. Frühere Versionen lassen sich ansehen und wiederherstellen.

Verfügbarkeit und Belastbarkeit

- Die Datenbank wird täglich gesichert; die Sicherungen werden 14 Tage aufbewahrt. Zusätzlich sichert Hetzner den gesamten Server täglich.
- Gelöschte Notizen liegen zunächst im Papierkorb des Teams.
- Das Betriebssystem installiert Sicherheitsupdates automatisch. Anwendung und Datenbank laufen in getrennten Containern mit Speichergrenzen und starten nach einem Fehler von selbst neu.

Überprüfung und Datenschutz durch Voreinstellungen

- Knotenhirn setzt keine Analyse-, Tracking- oder Werbewerkzeuge ein. Die öffentlichen Seiten laden nichts von fremden Servern. Ein Cookie setzen sie nur, wenn eine Person selbst eine Sprache wählt: „knotenhirn_sprache“ enthält nur die gewählte Sprache (de oder en) und läuft nach einem Jahr ab.
- Bei jeder Änderung am Code von Knotenhirn laufen automatisierte Tests.
- Der Auftragnehmer prüft die Maßnahmen bei jeder größeren Änderung und mindestens einmal im Jahr.

Anlage 3: Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland	Server, Rechenzentrum und Sicherungen	Deutschland (Nürnberg)
Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Irland	Google Vertex AI: Embeddings aus Notiztexten und Suchanfragen, Vorschläge für Themennamen aus Notiztiteln	Europäische Union (EU-Endpunkt)