Vereinbarung zur Auftragsverarbeitung (AVV)

Stand: 3. Juli 2026

Präambel und Parteien

Diese Vereinbarung zur Auftragsverarbeitung („**AVV**") konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien im Rahmen der Nutzung von Klausi.app gemäß den zugrunde liegenden Allgemeinen Geschäftsbedingungen („**Hauptvertrag**").

Verantwortlicher (nachfolgend „Kunde"): Der:die Nutzer:in von Klausi.app gemäß den im Konto hinterlegten Stammdaten.

Auftragsverarbeiter (nachfolgend „Anbieter"): CLOCKKNOCK GmbH, Buchheimer Str. 1a, 51063 Köln, Deutschland Geschäftsführer: Cem Tekin · Amtsgericht Köln, HRB 98717 · USt-IdNr. DE325875212 Kontakt Datenschutz: hello@klausi.app

Soweit der Kunde über Klausi.app personenbezogene Daten Dritter (z. B. seiner eigenen Kund:innen und Kontakte) verarbeitet, ist der Kunde **Verantwortlicher** und der Anbieter **Auftragsverarbeiter** im Sinne von Art. 4 Nr. 8, Art. 28 DSGVO.

---

1. Gegenstand, Art und Zweck der Verarbeitung; Dauer

1.1 Gegenstand ist die Verarbeitung personenbezogener Daten durch den Anbieter im Auftrag des Kunden, soweit dies zur Erbringung der im Hauptvertrag vereinbarten Leistungen (Zeiterfassung, Projekt- und Aufgabenverwaltung, Rechnungsstellung, Notizen, Terminplanung, CRM sowie optionale Zusatzfunktionen) erforderlich ist.

1.2 Art, Zweck und Umfang der Verarbeitung, die Art der Daten und die Kategorien betroffener Personen ergeben sich abschließend aus **Anlage 1**.

1.3 Die Verarbeitung findet ausschließlich innerhalb der EU/des EWR statt, soweit nicht in **Anlage 3** (Subprozessoren) oder durch vom Kunden aktivierte optionale Funktionen ausdrücklich anders geregelt (siehe Ziffer 11).

1.4 Die Dauer dieser AVV entspricht der Laufzeit des Hauptvertrags. Kündigungsrechte aus dem Hauptvertrag bleiben unberührt.

---

2. Weisungsrecht des Kunden

2.1 Der Anbieter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden, einschließlich in Bezug auf Drittlandübermittlungen, sofern nicht eine Rechtsvorschrift der EU/eines Mitgliedstaats den Anbieter hierzu verpflichtet.

2.2 Die im Hauptvertrag und in dieser AVV festgelegten Leistungen sowie die Nutzung der Funktionen durch den Kunden gelten als Weisung. Einzelweisungen sind an hello@klausi.app zu richten und werden dokumentiert.

2.3 Hält der Anbieter eine Weisung für datenschutzrechtswidrig, informiert er den Kunden unverzüglich; er darf die Ausführung bis zur Bestätigung aussetzen.

3. Pflichten des Anbieters (Art. 28 Abs. 3 DSGVO)

Der Anbieter verpflichtet sich insbesondere:

- (a) Daten nur weisungsgebunden zu verarbeiten (Ziffer 2);
- (b) die zur Verarbeitung befugten Personen zur Vertraulichkeit zu verpflichten;
- (c) die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO umzusetzen

und einzuhalten (**Anlage 2**);

- (d) die Bedingungen für die Inanspruchnahme von Unterauftragsverarbeitern

einzuhalten (Ziffer 6);

- (e) den Kunden bei der Beantwortung von Anträgen betroffener Personen zu

unterstützen (Ziffer 7);

- (f) den Kunden bei der Einhaltung der Art. 32–36 DSGVO zu unterstützen (Ziffer 8);
- (g) nach Wahl des Kunden alle Daten nach Ende der Verarbeitung zu löschen oder

zurückzugeben (Ziffer 9);

- (h) dem Kunden alle erforderlichen Informationen zum Nachweis der Einhaltung

bereitzustellen und Überprüfungen zu ermöglichen (Ziffer 10);

- (i) einen Datenschutzbeauftragten zu benennen, soweit gesetzlich erforderlich, und

einen Ansprechpartner zu benennen (hello@klausi.app).

---

4. Technische und organisatorische Maßnahmen (TOM)

Der Anbieter unterhält die in **Anlage 2** beschriebenen TOM. Er darf sie weiterentwickeln, solange das Schutzniveau nicht unterschritten wird.

---

5. Betroffenenrechte

5.1 Der Anbieter unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträgen betroffener Personen (Art. 15–22 DSGVO) nachzukommen (u. a. Selbstbedienungs-Export, Löschung des Kontos samt zugehöriger Daten, Einsicht in das MCP-Audit-Log).

5.2 Wendet sich eine betroffene Person direkt an den Anbieter, leitet er das Anliegen unverzüglich an den Kunden weiter.

---

6. Unterauftragsverarbeiter (Subprozessoren)

6.1 Der Kunde erteilt dem Anbieter die **allgemeine Genehmigung** zur Beauftragung von Unterauftragsverarbeitern. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Subprozessoren sind in **Anlage 3** aufgeführt; die stets aktuelle Liste ist unter `https://klausi.app/subprozessoren` abrufbar.

6.2 Der Anbieter informiert den Kunden über beabsichtigte Änderungen (Aufnahme oder Austausch) mit einer Frist von **14 Tagen** im Voraus per E-Mail und/oder über die Subprozessoren-Seite. Der Kunde kann aus wichtigem datenschutzrechtlichem Grund innerhalb von **14 Tagen** widersprechen.

6.3 Der Anbieter erlegt jedem Subprozessor per Vertrag dieselben Datenschutzpflichten auf, wie sie in dieser AVV vereinbart sind (Art. 28 Abs. 4 DSGVO).

6.4 **Klarstellung KI-Clients / MCP:** Verbindet der Kunde Klausi.app über das Model Context Protocol (MCP) oder eine sonstige Schnittstelle mit einem **externen KI-Client oder Drittdienst** (z. B. Claude, Cursor), so ist der Anbieter dieses Dienstes ein **Auftragsverarbeiter des Kunden** und **kein Subprozessor des Anbieters**. Auswahl, Rechtsgrundlage und ein etwaiger eigener AVV mit diesem Anbieter obliegen allein dem Kunden (vgl. Datenschutzerklärung §3.7). Der Anbieter stellt für diese vom Kunden veranlasste Übermittlung keine eigenen Garantien bereit.

---

7. Datenschutzverletzungen

Der Anbieter meldet dem Kunden Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden (Ziel: ohne unangemessene Verzögerung, i. d. R. innerhalb von 48 Stunden) und unterstützt ihn bei dessen Pflichten nach Art. 33, 34 DSGVO.

---

8. Unterstützung bei Art. 32–36 DSGVO

Der Anbieter unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Sicherheit der Verarbeitung, bei Meldungen und Benachrichtigungen sowie bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen.

---

9. Löschung und Rückgabe nach Vertragsende

9.1 Nach Abschluss der Verarbeitung löscht der Anbieter nach Wahl des Kunden alle personenbezogenen Daten oder gibt sie zurück, sofern nicht eine gesetzliche Aufbewahrungspflicht besteht.

9.2 Die technische Löschung erfolgt spätestens innerhalb von 7 Tagen nach Kontolöschung, vorbehaltlich rollierender Backup-Zyklen; Backups werden im Rahmen der Zyklen überschrieben.

---

10. Nachweise und Überprüfungen (Audits)

10.1 Der Anbieter stellt dem Kunden auf Anfrage die zum Nachweis der Einhaltung erforderlichen Informationen zur Verfügung (u. a. diese AVV, die Subprozessorenliste, die Verfahrensdokumentation und Angaben zu den TOM).

10.2 Überprüfungen können vorrangig durch Selbstauskünfte, Zertifikate oder Berichte erfolgen. Vor-Ort-Prüfungen sind mit angemessener Vorankündigung und ohne Betriebsstörung zulässig.

---

11. Drittlandübermittlung

11.1 Übermittlungen in Drittländer finden nur statt, soweit in **Anlage 3** ausgewiesen oder durch vom Kunden **aktiv eingeschaltete optionale Funktionen** (z. B. KI-/ Sprachdienste, Kartenfunktionen) veranlasst, und werden auf einen Angemessenheitsbeschluss und/oder EU-Standardvertragsklauseln nebst ergänzenden Maßnahmen gestützt.

11.2 Für Übermittlungen, die der Kunde selbst durch Anbindung externer Dienste (Ziffer 6.4) veranlasst, ist der Kunde für ein angemessenes Schutzniveau verantwortlich.

---

12. Haftung

Es gelten Art. 82 DSGVO sowie die Haftungsregelungen des Hauptvertrags.

---

13. Schlussbestimmungen

13.1 Bei Widersprüchen zwischen dieser AVV und dem Hauptvertrag gehen hinsichtlich des Datenschutzes die Regelungen dieser AVV vor.

13.2 Es gilt deutsches Recht. Gerichtsstand ist — soweit zulässig — Köln.

13.3 Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt.

Anlage 1 — Gegenstand und Einzelheiten der Verarbeitung

Art der Verarbeitung: Erheben, Erfassen, Speichern, Ordnen, Auslesen, Verändern, Übermitteln (an Subprozessoren gem. Anlage 3), Löschen — zur Bereitstellung der Klausi.app-Funktionen.

Zweck: Bereitstellung und Betrieb von Zeiterfassung, Projekt-/Aufgaben-/ Notizverwaltung, Rechnungsstellung, Terminplanung, CRM und optionalen Zusatzfunktionen.

Kategorien betroffener Personen:

- Nutzer:innen (Kunde selbst)
- Kund:innen, Kontakte und Ansprechpartner:innen des Kunden (CRM, Rechnungsempfänger)
- Gäste/Teilnehmer:innen von Terminbuchungen
- Weitere vom Kunden erfasste Personen (z. B. in Notizen, Projekten)

Kategorien personenbezogener Daten:

- Stamm- und Kontaktdaten (Name, E-Mail, Telefon, Anschrift, Funktion, Organisation)
- Vertrags-, Projekt- und Leistungsdaten (Zeiten, Aufgaben, Projekte, Leistungen)
- Abrechnungs- und Rechnungsdaten (Beträge, Rechnungsempfänger, USt-Angaben)
- Termin- und Verfügbarkeitsdaten
- Inhaltsdaten (Notizen, Uploads/Belege)
- Technische Metadaten (IP-Adresse, User-Agent, Logs — datenminimiert)

Besondere Kategorien (Art. 9 DSGVO): grundsätzlich nicht vorgesehen; der Kunde verpflichtet sich, solche Daten nur einzugeben, wenn er hierfür eine Rechtsgrundlage hat.

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

Stand: 3. Juli 2026.

Vertraulichkeit

- Mandantentrennung durch Supabase Row Level Security (RLS) auf `tenant_id` / `user_id`
- Authentifizierung über signierte JWT (ES256, JWKS-Prüfung)
- Zugriffskontrolle nach Least-Privilege; getrennte Rollen/Scopes
- Verschlüsselte Speicherung sensibler Secrets (OAuth-Token AES-256-GCM);

API-Tokens werden nur als SHA-256-Hash gespeichert (Klartext einmalig angezeigt)

Integrität

- Transportverschlüsselung TLS (1.2/1.3) für alle Verbindungen
- Unveränderliche ausgestellte Rechnungen; lückenlose Rechnungsnummern
- Audit-Logs für sensible Vorgänge (inkl. MCP-Tool-Aufrufe, datenminimiert:

nur Parameter-Schlüssel, keine Werte)

- Webhook-Signaturprüfung (HMAC), Upload-Validierung

Verfügbarkeit und Belastbarkeit

- EU-Hosting (Supabase AWS eu-west-1, GCS EU Multi-Region)
- Regelmäßige Backups mit rollierenden Zyklen
- Rate-Limiting und Missbrauchserkennung

Verfahren zur regelmäßigen Überprüfung

- Regelmäßige Security-Reviews (diff-basiert vor Merge + Vollaudit)
- Verbindliche Security-Guardrails
- Content-Security-Policy ohne `unsafe-inline`

Datenminimierung / Pseudonymisierung

- Analytics nur mit Einwilligung, pseudonymisiert (EU-Instanz)
- Logs datenminimiert (Pfad ohne Query-Parameter, hash-basierte IDs)

Anlage 3 — Genehmigte Subprozessoren

Es gilt die jeweils aktuelle Subprozessorenliste unter `https://klausi.app/subprozessoren`. Stand bei Vertragsschluss:

Subprozessor	Zweck	Region	Drittland-Absicherung
Supabase Inc.	DB, Auth, Edge Functions	EU (AWS eu-west-1)	—
Google Cloud (Google Ireland Ltd.)	Datei-/Medienspeicher	EU Multi-Region	SCC, soweit einschlägig
Vercel Inc.	Frontend-CDN	USA / global	SCC / Angemessenheitsbeschluss, soweit einschlägig
Gladia SAS	Live-Übersetzung/Transkription (opt.)	EU-West	—
Deepgram Inc.	Transkription/Spracheingabe (opt.)	EU	— (EU-Endpoint)
Anthropic PBC	KI-Analysen/Tagesplan (opt.)	USA	SCC (DPA), max. 30 Tage, kein Training
Postmark (Wildbit LLC)	Transaktions-E-Mail	USA	SCC (DPA)
Stripe Payments Europe Ltd.	Zahlung	EU (Irland)	SCC, soweit einschlägig
Mapbox Inc.	Karten/Routen	USA	SCC / Angemessenheitsbeschluss, soweit einschlägig
PostHog	Produkt-Analytics (opt.)	EU	—

CLOCKKNOCK GmbH · Buchheimer Str. 1a · 51063 Köln · hello@klausi.app