

Auftragsverarbeitungsvertrag

KAAI · nach Art. 28 DSGVO · Version 2026-07-21

Version	Datum	Aenderung
2026-07	20.07.2026	Initiale Version (Kurzfassung, als HTML-Seite auf kaai.at)
2026-07-21	21.07.2026	Vollstaendig ueberarbeitet: Historie, echte Unterauftragsverarbeiter-Liste (Hetzner, OpenAI, Google, Enable Banking, Stripe), Technische/Organisatorische Massnahmen ausformuliert, Bereitstellung als PDF statt eigener Webseite.

1. Preamble und Geltungsbereich

Dieser Auftragsverarbeitungsvertrag ("AVV") regelt die Verarbeitung personenbezogener Daten, die der Nutzer von KAAI (nachfolgend "Verantwortlicher") im Rahmen der Nutzung des Dienstes KAAI durch Michael Kasteneder (nachfolgend "Auftragsverarbeiter") verarbeiten laesst. Er wird durch die ausdrueckliche Zustimmung des Verantwortlichen (Checkbox bei Registrierung bzw. bei Abo-Abschluss) wirksam Bestandteil des Nutzungsverhaeltnisses und ergaenzt die AGB. Es findet ausschliesslich die Verordnung (EU) 2016/679 ("DSGVO") Anwendung; KAAI wird als Cloud-Dienst innerhalb der EU (Hetzner, Deutschland) betrieben.

2. Gegenstand und Dauer

KAAI ist ein AI-first Business Workspace fuer kleine Unternehmen: zentraler Business-Assistent/Chat, Kundenverwaltung, Angebote, Rechnungen, Auftraege, Zeiterfassung, E-Mail-Postfach-Anbindung, Kalendersynchronisation und optionaler read-only Bankabgleich. Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten, die der Verantwortliche im Rahmen dieser Nutzung eintraegt, importiert oder ueber Integrationen anbindet. Die Dauer entspricht der Laufzeit des Nutzungsverhaeltnisses gemaess AGB und endet automatisch mit dessen Beendigung, unbeschadet fortbestehender Loeschungs- und Nachweispflichten.

3. Konkretisierung des Auftragsinhalts

3.1 Art und Zweck der Verarbeitung

Die Verarbeitung erfolgt ausschliesslich zum Zweck der Bereitstellung der KAAI-Anwendung:

- Speicherung, Anzeige und Bearbeitung der vom Verantwortlichen eingegebenen Geschaeftsdaten (Kunden, Angebote, Rechnungen, Auftraege, Kalender, Wissensdatenbank).
- KI-gestuetzte Analyse und Vorschlagsfunktionen im Chat (Textverarbeitung eingegebener/importierter Inhalte durch ein Sprachmodell, siehe 5.2 und Unterauftragsverarbeiter).
- E-Mail-Synchronisation (IMAP/SMTP-Anbindung des vom Verantwortlichen selbst betriebenen oder gewaehlten Postfachs; optional zusaetzlich eine KAAI-seitige Import-Mailadresse als Catch-All-Weiterleitung, siehe 5.2) und automatisierte Inhaltsauswertung eingehender Nachrichten (Intent-Erkennung, Angebots-/Rechnungserkennung).
- Kalenderabgleich mit Google Calendar, sofern vom Verantwortlichen aktiv verbunden.
- Optionaler, ausschliesslich lesender Bankkontoabgleich (Open Banking) zur automatischen Rechnungs-/Zahlungszuordnung, sofern vom Verantwortlichen aktiv eingerichtet.
- Erstellung und Versand von Dokumenten (Angebote, Rechnungen) als PDF.
- Abwicklung der eigenen KAAI-Abo-Zahlung des Verantwortlichen (Zahlungsmethode, Einzug), sobald ein kostenpflichtiges Abo abgeschlossen wird.

3.2 Kategorien betroffener Personen

- Kunden und Interessenten des Verantwortlichen

- Ansprechpartner bei Kunden/Lieferanten
- Lieferanten des Verantwortlichen
- Mitarbeiter des Verantwortlichen (soweit im Rahmen von Zeiterfassung/Workspace-Mitgliedschaft verarbeitet)
- Der Verantwortliche selbst und seine Workspace-Mitglieder (Login-/Kontaktdaten)

3.3 Kategorien der Daten

- Personen-Stammdaten (Namen, Kontaktdaten, Firmendaten)
- Kommunikationsdaten (E-Mail-Inhalte und -Metadaten, Telefonnummern)
- Vertrags- und Rechnungsdaten (Angebote, Rechnungen, Zahlungsstatus)
- Termindaten (Kalender)
- Zeiterfassungsdaten
- Bankverbindungs- und Transaktionsdaten, ausschliesslich lesend und ausschliesslich bei aktiv eingerichtetem Bankabgleich (Enable Banking)
- Zahlungsmethoden-Metadaten des Verantwortlichen selbst (Kartentyp/letzte 4 Ziffern, SEPA-Mandatsreferenz), ausschliesslich fuer die eigene KAAI-Abo-Abrechnung (Stripe)

Der Verantwortliche stellt sicher, dass ueber KAAI keine besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO (u.a. Gesundheitsdaten, ethnische Herkunft, religioese/politische Ueberzeugungen, Gewerkschaftszugehoerigkeit, biometrische/genetische Daten) verarbeitet werden. Sollte dies dennoch geschehen, ist der Auftragsverarbeiter unverzueglich zu informieren.

4. Technische und organisatorische Massnahmen (Art. 32 DSGVO)

Die folgenden Massnahmen beziehen sich auf den tatsaechlichen technischen Aufbau von KAAI (Stand 2026-07-21):

- **Vertraulichkeit:** Verschluesselte Uebertragung (HTTPS/TLS) fuer saemtlichen Datenverkehr. Passwoerter werden ausschliesslich als Hash gespeichert (scrypt, kein Klartext). Sensible Integrations-Zugangsdaten (IMAP/SMTP-Passwoerter, Banking-Zugangsdaten) werden AES-256-GCM-verschluesselt in der Datenbank abgelegt. Zugriff auf Produktivsysteme erfolgt ausschliesslich ueber personengebundene, SSH-Key-basierte Zugaenge; administrativer Zugriff auf das Control Center ist per Zwei-Faktor-Authentifizierung (TOTP) abgesichert.
- **Integritaet:** Mandantentrennung erfolgt ueber durchgaengige `tenant_id`-Filterung auf Datenbankebene (Shared-Database-Architektur, keine physisch getrennten Datenbanken pro Mandant). Sicherheitsrelevante administrative Aktionen (Tenant einfrieren, Datenexport, Loeschung) werden in einem unveraenderlichen Audit-Log protokolliert.
- **Verfuegbarkeit und Belastbarkeit:** Regelmassige Backups der Produktionsdatenbank, insbesondere vor jedem Produktions-Deployment. Hosting bei Hetzner Online GmbH (Deutschland/EU) mit dessen eigener Infrastruktur-Redundanz.
- **Verfahren zur Ueberpruefung:** Aenderungen an Produktivsystemen laufen ueber ein versioniertes Deployment (Git, CI-Tests) mit manueller Freigabe fuer Produktions-Deployments; Migrationen und Code-Aenderungen sind nachvollziehbar historisiert.
- **Loeschkonzept:** Ein Workspace-Owner kann jederzeit selbst einen vollstaendigen Datenexport herunterladen. Nach Kuendigung/Beendigung durchlaeuft ein Tenant eine Loeschvormerkung mit Frist (mindestens 30 Tage) samt Bestaetigung, dass aufbewahrungspflichtige Unterlagen (z.B. Rechnungen, §132 BAO) vom Verantwortlichen selbst gesichert wurden; danach werden saemtliche Daten des Tenants transaktional geloescht (Datenbank und Dateien), automatisiert per taeglichem Hintergrundjob nach Fristablauf oder jederzeit vorzeitig manuell durch einen Admin.

Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt; der Auftragsverarbeiter darf gleichwertige alternative Massnahmen umsetzen, ohne das bestehende Schutzniveau zu unterschreiten.

5. Unterauftragsverarbeiter

5.1 Grundsatz

Der Verantwortliche stimmt dem Einsatz der folgenden Unterauftragsverarbeiter zu. Ueber den Austausch oder die Hinzunahme weiterer Unterauftragsverarbeiter wird der Verantwortliche informiert (z.B. per E-Mail an die hinterlegte Kontaktadresse oder Hinweis in der Anwendung); er kann der Aenderung aus wichtigem Grund widersprechen.

5.2 Aktuelle Unterauftragsverarbeiter

Unterauftragsverarbeiter	Zweck	Standort	Aktiv fuer
Hetzner Online GmbH	Hosting der Anwendung, der Datenbank und aller gespeicherten Dateien (Uploads, generierte PDFs); Versand von System-E-Mails (Passwort-Reset, Willkommens-E-Mail) ueber einen bei Hetzner betriebenen Mailserver; optionaler Catch-All-Mailserver fuer die KAAI-Import-Mailadresse (falls vom Verantwortlichen aktiviert)	Deutschland (EU)	Alle Nutzer (immer aktiv)
OpenAI OpCo, LLC	KI-gestuetzte Kernfunktionen: Chat-Assistent, automatische Analyse eingehender E-Mails (Intent-Erkennung, Angebots-/Rechnungserkennung), Dokumentenklassifikation	USA, auf Grundlage von Standardvertragsklauseln (SCC)	Alle Nutzer (immer aktiv, Kernfunktion)
Google Ireland Limited	Google-Kalender-Synchronisation	EU / USA	Nur bei aktiver Google-Kalender-Verbindung durch den Nutzer (Opt-in)
Enable Banking Oy	Ausschliesslich lesender Abruf von Bankkonto-Umsaetzen (Open Banking / PSD2) zur automatischen Rechnungs-/Zahlungszuordnung. Kein Zugriff auf Zahlungsausloesung.	Finnland (EU)	Nur bei aktiv eingerichteter Bankverbindung durch den Nutzer (Opt-in)
Stripe Payments Europe, Ltd.	Abwicklung der Zahlungsmethode und des Zahlungseinzugs fuer das eigene KAAI-Abo des Verantwortlichen (nicht fuer dessen eigene Kundenzahlungen - KAAI bietet dem Verantwortlichen selbst keine Zahlungsabwicklung fuer dessen Kunden an)	Irland (EU), mit Sub-Processing in den USA	Nur ab Abschluss eines kostenpflichtigen KAAI-Abos

Der Verantwortliche wird darauf hingewiesen, dass IMAP/SMTP-Postfaecher, die er selbst zur E-Mail-Synchronisation mit KAAI verbindet (eigenes Firmenpostfach), nicht Unterauftragsverarbeiter von KAAI sind - der jeweilige E-Mail-Provider des Verantwortlichen ist insoweit dessen eigene Wahl und eigene Verantwortung; KAAI greift lesend/schreibend darauf zu, ohne die Daten dort selbst zu hosten.

6. Wahrnehmung der Betroffenenrechte

Fuer die Beantwortung von Betroffenenrechten (Art. 12 ff. DSGVO: Auskunft, Berichtigung, Loeschung, Einschraenkung, Datenuebertragbarkeit, Widerspruch) ist der Verantwortliche zustaeendig. Der Auftragsverarbeiter unterstuetzt ihn dabei, soweit dies nicht bereits ueber die Anwendung selbst moeglich ist (z.B. Kunden-/Kontaktdaten koennen direkt in KAAI eingesehen, berichtigt und geloescht werden). Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet dieser die Anfrage unverzueglich an den Verantwortlichen weiter.

7. Pflichten des Auftragsverarbeiters

- Verarbeitung ausschliesslich auf dokumentierte Weisung des Verantwortlichen, es sei denn, eine gesetzliche Verpflichtung besteht. Haelt der Auftragsverarbeiter eine Weisung fuer datenschutzwidrig, informiert er den Verantwortlichen unverzueglich und darf die Ausfuehrung bis zur Bestaetigung oder Aenderung der Weisung aussetzen.

- Gewährleistung, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind.
- Umsetzung der in Abschnitt 4 genannten technischen und organisatorischen Massnahmen.
- Unverzügliche Meldung von Verletzungen des Schutzes personenbezogener Daten an den Verantwortlichen (Art. 33 DSGVO), inkl. Unterstützung bei dessen Informationspflichten gegenüber Betroffenen und Aufsichtsbehörde.
- Unterstützung des Verantwortlichen bei Datenschutz-Folgenabschätzungen (Art. 35 DSGVO), soweit die zu beurteilenden Verarbeitungen im Verantwortungsbereich des Auftragsverarbeiters liegen.
- Löschung oder Rückgabe aller personenbezogenen Daten nach Beendigung des Vertragsverhältnisses gemäss Abschnitt 4 (Löschkonzept), sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

8. Information und Kontrollrechte des Verantwortlichen

Der Verantwortliche kann sich in angemessenem Umfang von der Einhaltung der in diesem AVV genannten Pflichten überzeugen, etwa durch Anforderung entsprechender Auskünfte per E-Mail an info@kaai.at. Für Kosten, die dem Auftragsverarbeiter durch die Ausübung weitergehender Kontrollrechte entstehen, kann eine aufwandsbasierte Vergütung vereinbart werden.

9. Haftung

Es gelten die Haftungsregelungen der AGB. Der Auftragsverarbeiter haftet für Schaden aus einer Verarbeitung nur, wenn er seinen Pflichten aus diesem Vertrag nicht nachgekommen ist oder entgegen rechtmässigen Weisungen des Verantwortlichen gehandelt hat.

10. Schlussbestimmungen

Nebenabreden oder Änderungen dieses AVV bedürfen der Schriftform (Textform genügt). Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Es gilt österreichisches Recht. Gerichtsstand für Unternehmer ist, soweit gesetzlich zulaessig, der Sitz des Anbieters in Österreich.