

Auftragsverarbeitungsvertrag

KAAI · nach Art. 28 DSGVO · Version 2026-10-19

Version	Datum	Änderung
2026-07	20.07.2026	Initiale Version (Kurzfassung, als HTML-Seite auf kaai.at)
2026-07-21	21.07.2026	Vollständig überarbeitet: Historie, echte Unterauftragsverarbeiter-Liste (Hetzner, OpenAI, Google, Enable Banking, Stripe), Technische/Organisatorische Maßnahmen ausformuliert, Bereitstellung als PDF statt eigener Webseite.
2026-10-19	19.10.2026	Löschkonzept neu: Löschung 30 Tage nach Ende von Abo oder Testzeitraum mit Erinnerungen, sofortige Löschung durch den Verantwortlichen, vollständiger Export inklusive Dateien, Aufbewahrungsdauer der Backups.

1. Präambel 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 lässt. Er wird durch die ausdrückliche Zustimmung des Verantwortlichen (Checkbox bei Registrierung bzw. bei Abo-Abschluss) wirksam Bestandteil des Nutzungsverhältnisses und ergänzt 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 für kleine Unternehmen: zentraler Business-Assistent/Chat, Kundenverwaltung, Angebote, Rechnungen, Aufträge, 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 einträgt, importiert oder über Integrationen anbindet. Die Dauer entspricht der Laufzeit des Nutzungsverhältnisses gemäß AGB und endet automatisch mit dessen Beendigung, unbeschadet fortbestehender Löschungs- 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 Geschäftsdaten (Kunden, Angebote, Rechnungen, Aufträge, Kalender, Wissensdatenbank).
- KI-gestützte 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 gewählten Postfachs; optional zusätzlich 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 für die eigene KAAI-Abo-Abrechnung (Stripe)

Der Verantwortliche stellt sicher, dass über KAAI keine besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO (u.a. Gesundheitsdaten, ethnische Herkunft, religiöse/politische Überzeugungen, Gewerkschaftszugehörigkeit, biometrische/genetische Daten) verarbeitet werden. Sollte dies dennoch geschehen, ist der Auftragsverarbeiter unverzüglich zu informieren.

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

Die folgenden Maßnahmen beziehen sich auf den tatsächlichen technischen Aufbau von KAAI (Stand 2026-10-19):

- **Vertraulichkeit:** Verschlüsselte Übertragung (HTTPS/TLS) für sämtlichen Datenverkehr. Passwörter werden ausschließlich als Hash gespeichert (bcrypt, kein Klartext). Sensible Integrations-Zugangsdaten (IMAP/SMTP-Passwörter, Banking-Zugangsdaten) werden AES-256-GCM-verschlüsselt in der Datenbank abgelegt. Zugriff auf Produktivsysteme erfolgt ausschließlich über personengebundene, SSH-Key-basierte Zugänge; administrativer Zugriff auf das Control Center ist per Zwei-Faktor-Authentifizierung (TOTP) abgesichert.
- **Integrität:** Mandantentrennung erfolgt über durchgängige `tenant_id`-Filterung auf Datenbankebene (Shared-Database-Architektur, keine physisch getrennten Datenbanken pro Mandant). Sicherheitsrelevante administrative Aktionen (Tenant einfrieren, Datenexport, Löschung) werden in einem unveränderlichen Audit-Log protokolliert.
- **Verfügbarkeit und Belastbarkeit:** Regelmäßige Backups der Produktionsdatenbank, insbesondere vor jedem Produktions-Deployment; Backups werden 30 Tage aufbewahrt. Hosting bei Hetzner Online GmbH (Deutschland/EU) mit dessen eigener Infrastruktur-Redundanz.
- **Verfahren zur Überprüfung:** Änderungen an Produktivsystemen laufen über ein versioniertes Deployment (Git, CI-Tests) mit manueller Freigabe für Produktions-Deployments; Migrationen und Code-Änderungen sind nachvollziehbar historisiert.
- **Löschkonzept:**
 - **Export:** Der Inhaber des Workspace (Owner) kann jederzeit selbst einen vollständigen Export herunterladen: alle Daten des Workspace sowie alle hochgeladenen und erzeugten Dateien (z.B. Belege, Anhänge, PDFs), ohne Passwörter und Zugangsdaten.
 - **Löschung nach Vertragsende:** Endet das Abo durch Kündigung oder der Testzeitraum ohne Abschluss eines Abos, wird der Workspace gesperrt und bleibt 30 Tage erreichbar, damit der Verantwortliche seine Daten exportieren kann. Der

Owner wird 7 Tage und 1 Tag vor der Löschung per E-Mail erinnert. Danach löscht ein stündlich laufender Hintergrundjob sämtliche Daten des Workspace: alle Datenbankeinträge, Dateien, Benutzerzugänge und gespeicherten Zugangsdaten zu angebundenen Diensten. Die Löschung erfolgt in einer Transaktion vollständig oder gar nicht. Gelöscht wird nur, wenn mindestens eine Erinnerung tatsächlich versendet wurde. Schließt der Verantwortliche vorher wieder ein Abo ab, unterbleibt die Löschung.

- o **Sofortige Löschung:** Der Owner kann den Workspace jederzeit selbst sofort löschen. Dazu bestätigt er, alle Daten heruntergeladen zu haben und aufbewahrungspflichtige Unterlagen (z.B. Rechnungen, § 132 BAO) selbst zu sichern, und gibt den Namen des Workspace ein. Daneben kann der Auftragsverarbeiter einen Workspace auf Anfrage des Verantwortlichen über eine Löschvormerkung mit Frist löschen.
- o **Nachweis:** Jede Löschung wird mit Workspace, handelnder Person bzw. automatischem Job, Zeitpunkt sowie bei der sofortigen Löschung mit IP-Adresse und der erteilten Bestätigung protokolliert. Das Protokoll bleibt nach der Löschung erhalten.
- o **Sicherungskopien:** Gelöschte Daten können noch bis zu 30 Tage in Sicherungskopien der Datenbank enthalten sein, die ausschließlich der Wiederherstellung des Dienstes dienen.

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. Über 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 Änderung aus wichtigem Grund widersprechen.

5.2 Aktuelle Unterauftragsverarbeiter

Unterauftragsverarbeiter	Zweck	Standort	Aktiv für
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) über einen bei Hetzner betriebenen Mailserver; optionaler Catch-All-Mailserver für die KAAI-Import-Mailadresse (falls vom Verantwortlichen aktiviert)	Deutschland (EU)	Alle Nutzer (immer aktiv)
OpenAI OpCo, LLC	KI-gestützte 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-Umsätzen (Open Banking / PSD2) zur automatischen Rechnungs-/Zahlungszuordnung. Kein Zugriff auf Zahlungsauslösung.	Finnland (EU)	Nur bei aktiv eingerichteter Bankverbindung durch den Nutzer (Opt-in)
Stripe Payments Europe, Ltd.	Abwicklung der Zahlungsmethode und des Zahlungseinzugs für das eigene KAAI-Abo des Verantwortlichen (nicht für dessen eigene	Irland (EU), mit Sub-Processing in den USA	Nur ab Abschluss eines

	Kundenzahlungen - KAAI bietet dem Verantwortlichen selbst keine Zahlungsabwicklung für dessen Kunden an)		kostenpflichtigen KAAI-Abos
--	--	--	-----------------------------

Der Verantwortliche wird darauf hingewiesen, dass IMAP/SMTP-Postfächer, 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

Für die Beantwortung von Betroffenenrechten (Art. 12 ff. DSGVO: Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) ist der Verantwortliche zuständig. Der Auftragsverarbeiter unterstützt ihn dabei, soweit dies nicht bereits über die Anwendung selbst möglich ist (z.B. Kunden-/Kontaktdaten können direkt in KAAI eingesehen, berichtigt und gelöscht werden). Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet dieser die Anfrage unverzüglich an den Verantwortlichen weiter.

7. Pflichten des Auftragsverarbeiters

- Verarbeitung ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, eine gesetzliche Verpflichtung besteht. Hält der Auftragsverarbeiter eine Weisung für datenschutzwidrig, informiert er den Verantwortlichen unverzüglich und darf die Ausführung bis zur Bestätigung oder Änderung 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 Schäden 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 zulässig, der Sitz des Anbieters in Österreich.