Auftragsbearbeitungsvertrag (AVV)

avendo AG · Version 1.0 · Stand 02.11.2026

Zwischen der **Kundin** gemäss Kundenvereinbarung («Verantwortliche») und der **avendo AG**, Hardturmstrasse 161, 8005 Zürich («avendo»). Dieser AVV ist Bestandteil der Kundenvereinbarung und der AGB von avendo. Bei Widerspruch geht dieser AVV für den Datenschutz vor. Er gilt für Kundinnen in der Schweiz und in der EU, insbesondere in Deutschland.

1. Gegenstand und Dauer

1. avendo bearbeitet Personendaten im Auftrag der Verantwortlichen, um die Software avendo (CRM, Webseiten, Publikationen, Kommunikation) bereitzustellen.
2. Der AVV gilt, solange avendo Personendaten der Verantwortlichen bearbeitet.
3. Für Kundinnen in der Schweiz gilt das Schweizer Datenschutzgesetz (DSG). Für Kundinnen in der EU gilt die EU-Datenschutz-Grundverordnung (DSGVO), insbesondere Art. 28. «Auftragsbearbeitung» meint dann «Auftragsverarbeitung», «EDÖB» die zuständige Aufsichtsbehörde.

2. Art der Daten und betroffene Personen

1. **Betroffene Personen:** Eigentümerinnen und Eigentümer, Kaufinteressierte, Mietinteressierte, weitere Kontakte der Verantwortlichen sowie deren Mitarbeitende, die avendo nutzen.
2. **Daten:** Namen, Adressen, E-Mail-Adressen, Telefonnummern, Kommunikation (E-Mail, SMS, WhatsApp), Notizen, Termine, Suchprofile, Angaben zu Liegenschaften, Dokumente und Bilder sowie Nutzungs- und Protokolldaten.
3. Besonders schützenswerte Personendaten bearbeitet avendo nur, wenn die Verantwortliche sie selbst erfasst.

3. Weisungen

1. avendo bearbeitet die Daten nur nach dokumentierter Weisung der Verantwortlichen. Die Kundenvereinbarung, die AGB, dieser AVV und die Nutzung der Software gelten als Weisung. Weitere Weisungen erteilt die Verantwortliche in Textform. Das gilt auch für die Bekanntgabe von Daten in Drittländer (Ziffer 7).
2. avendo nutzt die Daten nicht für eigene Zwecke und verkauft sie nicht.
3. Hält avendo eine Weisung für rechtswidrig, informiert avendo die Verantwortliche sofort.

4. Vertraulichkeit

Alle Personen bei avendo mit Zugriff auf die Daten sind zur Vertraulichkeit verpflichtet. Diese Pflicht gilt auch nach Ende der Anstellung.

5. Sicherheit

avendo trifft die technischen und organisatorischen Massnahmen (TOM) in Anhang 2. avendo darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt.

6. Unterauftragsbearbeiter

1. Die Verantwortliche genehmigt allgemein, dass avendo Unterauftragsbearbeiter beizieht. Die bei Vertragsschluss eingesetzten stehen in Anhang 1.
2. avendo darf Unterauftragsbearbeiter jederzeit hinzufügen oder ersetzen. avendo veröffentlicht die aktuelle Liste mit Datum unter pro.avendo.ch/avv. Eine weitere Mitteilung erfolgt nicht. Die

Verantwortliche kann einem neuen Unterauftragsbearbeiter innert 30 Tagen nach der Veröffentlichung aus wichtigem Grund widersprechen. Findet sich keine Lösung, kann sie den betroffenen Dienst kündigen.

3. avendo verpflichtet jeden Unterauftragsbearbeiter vertraglich auf mindestens gleichwertige Datenschutzpflichten. avendo haftet gegenüber der Verantwortlichen dafür, dass die Unterauftragsbearbeiter diese Pflichten einhalten.

7. Bekanntgabe ins Ausland

1. Die Daten liegen in der EU (Anwendung und Dateien in Paris, Datenbank in Frankfurt).
2. Werden Daten in ein Land ohne angemessenen Datenschutz bekanntgegeben, sorgt avendo für geeignete Garantien. Das sind insbesondere die Standardvertragsklauseln der EU-Kommission mit Schweizer Anpassungen oder eine Zertifizierung nach dem Swiss-US bzw. EU-US Data Privacy Framework.

8. Unterstützung der Verantwortlichen

avendo unterstützt die Verantwortliche angemessen bei:

1. Auskünften, Berichtigungen, Löschungen und Datenübertragungen an betroffene Personen.
2. der Sicherheit der Bearbeitung, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen (DSGVO Art. 32 bis 36).
3. Meldungen an den EDÖB oder die zuständige Aufsichtsbehörde in der EU.

9. Verletzung der Datensicherheit

1. avendo informiert die Verantwortliche ohne unnötige Verzögerung, spätestens innert **48 Stunden** nach Kenntnis, über eine Verletzung der Datensicherheit, die ihre Daten betrifft.
2. Die Meldung enthält, soweit bekannt: was passiert ist, welche Daten und Personen betroffen sind, die möglichen Folgen und die getroffenen Massnahmen.
3. avendo ergreift sofort Massnahmen, um den Schaden zu begrenzen.

10. Kontrollen

1. avendo gibt der Verantwortlichen auf Anfrage die Informationen, die nötig sind, um die Einhaltung dieses AVV zu belegen.
2. Prüfungen vor Ort sind nach Voranmeldung von mindestens 30 Tagen möglich, durch die Verantwortliche oder eine von ihr beauftragte, zur Verschwiegenheit verpflichtete Prüfperson. Sie finden höchstens einmal pro Jahr und während der Bürozeiten statt, ausser bei einem Vorfall nach Ziffer 9. Die Kosten trägt die Verantwortliche, ausser die Prüfung zeigt einen wesentlichen Verstoss.

11. Export, Rückgabe und Löschung

1. Die Verantwortliche kann ihre Daten während der Vertragsdauer jederzeit exportieren.
2. Nach Vertragsende stellt avendo auf Wunsch einen vollständigen Export bereit. Danach löscht avendo die Daten innert 90 Tagen, soweit kein Gesetz der Schweiz, der EU oder eines EU-Mitgliedstaats eine längere Aufbewahrung verlangt.
3. Kopien in Backups werden mit dem regulären Ablauf der Backups gelöscht, spätestens nach 12 Monaten.

12. Haftung und Schluss

1. Für die Haftung gelten die Regeln der Kundenvereinbarung und der AGB.

2. Die jeweils geltende Fassung dieses AVV steht unter pro.avendo.ch/avv.
3. Es gilt Schweizer Recht. Zwingende Bestimmungen der DSGVO bleiben vorbehalten. Gerichtsstand ist Zürich. Datenschutz-Kontakt bei avendo: datenschutz@avendo.ch.

Ort, Datum · Verantwortliche (Kundin)	Ort, Datum · avendo AG

Anhang 1: Unterauftragsbearbeiter

Stand 02.11.2026. Die jeweils aktuelle Liste steht unter pro.avendo.ch/avv. Alle Kerndaten liegen in der EU: Anwendung und Dateien in Paris, Datenbank in Frankfurt. Einige Zusatzfunktionen nutzen Anbieter mit Sitz in den USA. Dafür gelten EU-Standardvertragsklauseln oder das Data Privacy Framework.

Anbieter	Zweck	Datenstandort
Amazon Web Services EMEA SARL (Luxemburg)	Hosting der Anwendung, Dateien und Dokumente, Protokolle, Warteschlangen, SMS-Versand	EU, Paris
MongoDB Inc. (USA), Atlas	Datenbank mit allen CRM-Daten, Backups	EU, Frankfurt
Nylas Inc. (USA)	Verbindung der E-Mail-Postfächer und Kalender der Nutzenden, E-Mail-Versand	EU-Rechenzentrum
MailerSend Inc. (USA)	Versand von System-E-Mails	EU (Google Cloud, Belgien)
360dialog GmbH (Deutschland)	WhatsApp-Nachrichten, nur wenn die Kundin WhatsApp nutzt	Deutschland; Nachrichten laufen zusätzlich über Meta (WhatsApp, weltweit)
OpenAI (USA)	KI-Funktionen, z. B. Texte und Dokumentanalyse	USA
Anthropic PBC (USA)	KI-Funktionen, z. B. Exposé-Studio und Signatur	USA
PriceHubble AG (Schweiz)	Immobilienbewertung, nur Objektdaten	Schweiz, EU, USA
IAZI AG (Schweiz)	Immobilienbewertung, nur Objektdaten	Schweiz
Mapbox Inc. (USA), Google LLC (USA)	Karten und Adresssuche	USA / weltweit
Stripe Payments Europe Ltd. (Irland)	Zahlung von Guthaben, nur Rechnungsdaten der Kundin	EU / USA
Intercom R&D Unlimited (Irland)	Support-Chat mit den Nutzenden	USA

Nicht in der Liste sind Dienste, die die Kundin selbst verbindet, zum Beispiel ihr eigenes Brevo-Konto, Inserate-Portale und eigene FTP-Exporte. Dafür ist die Kundin selbst verantwortlich.

Anhang 2: Technische und organisatorische Massnahmen (TOM)

Bereich	Massnahme
Rechenzentren	Betrieb nur bei AWS und MongoDB Atlas in der EU. Beide Rechenzentren sind nach ISO 27001 und SOC 2 zertifiziert. Kein eigener Serverraum.
Trennung der Kunden	Jede Abfrage ist an die Firma der Kundin gebunden. Eine Kundin sieht nie Daten einer anderen Kundin.

Zugang	Login mit persönlichem Konto. Passwörter werden nur als bcrypt-Hash gespeichert, nie im Klartext. Optional Login mit Google oder Microsoft.
Rechte	Rollen und Rechte pro Benutzer. Objekte und Kontakte sind je nach Team und Zuständigkeit sichtbar.
Verschlüsselung bei der Übertragung	Alle Verbindungen laufen über HTTPS (TLS).
Verschlüsselung bei der Speicherung	Datenbank und Dateispeicher sind verschlüsselt (AES-256). Schlüssel für Drittdienste sind zusätzlich mit AES-256-GCM verschlüsselt.
Dateien und Dokumente	Alle Dateien sind privat. Freigabe nur über zeitlich begrenzte Links (in der Regel 15 Minuten).
Zugangsdaten der Systeme	Gespeichert im AWS Parameter Store, nicht im Code.
Schutz vor Missbrauch	Begrenzung der Anfragen pro Minute an die Schnittstellen.
Protokolle	Anfragen und Ereignisse werden in AWS CloudWatch protokolliert. Änderungen an Objekten und Kontakten stehen im Logbuch.
Löschen	Gelöschte Einträge sind zuerst nur ausgeblendet und lassen sich bei einem Fehler zurückholen.
Backups Datenbank	Automatische Sicherung in Frankfurt: alle 6 Stunden (2 Tage aufbewahrt), täglich (7 Tage), wöchentlich (4 Wochen), monatlich (12 Monate).
Backups Dateien	Versionierung aktiv: Gelöschte oder überschriebene Dateien bleiben 30 Tage wiederherstellbar. Die Dateien liegen in Paris, mehrfach verteilt auf getrennte Rechenzentren.
Mitarbeitende	Zugriff auf Produktivdaten nur für wenige Personen, nur für Support und Betrieb. Alle sind zur Vertraulichkeit verpflichtet.
Vorfälle	Meldung an betroffene Kundinnen innert 48 Stunden (AVV Ziffer 9).
Daten-Export	Kontakte, Logbuch und Einwilligungen als CSV. Dokumente als Download. Alles auch über die Partner-API.