

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO - für die App „Zettelfuchs“

Stand: 12.10.2026

Version: AVV_1.2_2026-10-12

Dieser Auftragsverarbeitungsvertrag (AVV) regelt die Verarbeitung personenbezogener Daten im Auftrag eines registrierten Betriebs bei Nutzung von Zettelfuchs, soweit der Betrieb Verantwortlicher und Zettelfuchs Auftragsverarbeiter ist.

Präambel und Parteien

Auftraggeber (Verantwortlicher):

der registrierte Betrieb bzw. Auftraggeber gemäß Unternehmenskonto, soweit er personenbezogene Daten eigener Endkunden oder Ansprechpartner über Zettelfuchs durch den Auftragnehmer verarbeiten lässt (nachfolgend „Auftraggeber“).

Auftragnehmer (Auftragsverarbeiter):

Oscar Gumbmann

Garagenweg 7

91088 Bubenreuth

Deutschland

E-Mail: info@zettelfuchs.app

(nachfolgend „Auftragnehmer“).

Elektronischer Abschluss: Der AVV wird beim ersten Start bzw. bei einer neuen AVV-Version über eine Checkbox abgeschlossen. AGB und AVV werden getrennt versioniert. Der Server speichert Dokumenttyp, Version und Server-Zeitpunkt. Die akzeptierte AVV-Fassung ist in der App unter „Betrieb > Rechtliches“ abrufbar.

§ 1 Gegenstand und Anwendungsbereich

(1) Der Auftragnehmer verarbeitet im Rahmen von Zettelfuchs personenbezogene Daten des Auftraggebers ausschließlich soweit dies für die in Anlage 1 beschriebenen App-Funktionen erforderlich ist.

(2) Auftragsdaten sind Kundendaten, die der Auftraggeber in Angeboten verarbeitet: Name, Straße, PLZ und Ort des Endkunden sowie gegebenenfalls Freitext in Angebotspositionen, den der Nutzer selbst diktiert. E-Mail-Adresse und Telefonnummer des Endkunden werden nicht als Kundendaten des Angebots verarbeitet.

(3) Betroffene Personen sind Endkunden und Ansprechpartner des Auftraggebers.

(4) Nicht Gegenstand dieses AVV sind Verarbeitungen, für die der Auftragnehmer selbst Verantwortlicher ist, insbesondere Nutzerkonto, Betriebsprofil, Zettelfuchs-Pro-Abonnement, Zustimmungsnachweise, Widerrufsnachweise und optionale PostHog-Analyse.

§ 2 Pflichten des Auftraggebers

- (1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung seiner Kundendaten, die Wahrung der Rechte betroffener Personen und die Erfüllung seiner Informationspflichten verantwortlich.
- (2) Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO und Daten nach Art. 10 DSGVO sind für Zettelfuchs nicht vorgesehen und sollen vom Auftraggeber nicht eingegeben oder diktiert werden.

§ 3 Weisungsgebundene Verarbeitung

- (1) Der Auftragnehmer verarbeitet Auftragsdaten ausschließlich auf dokumentierte Weisung des Auftraggebers, soweit keine gesetzliche Verpflichtung zu einer abweichenden Verarbeitung besteht.
- (2) Die Nutzung der App, die Eingaben des Auftraggebers und dieser AVV gelten als dokumentierte Weisungen. Ergänzende Weisungen können in Textform an info@zettelfuchs.app erteilt werden.
- (3) Hält der Auftragnehmer eine Weisung für datenschutzrechtswidrig, informiert er den Auftraggeber unverzüglich und kann die Ausführung bis zur Klärung aussetzen.

§ 4 Vertraulichkeit und Zugriff

- (1) Der Auftragnehmer gewährleistet die Vertraulichkeit der im Auftrag verarbeiteten Daten und beschränkt Zugriffe auf den für die Aufgabenerfüllung erforderlichen Umfang.
- (2) Technisch wird der Zugriff auf Datenbankebene durch Row Level Security getrennt. Die Identität des Nutzers wird serverseitig aus dem Anmeldetoken ermittelt; jeder Nutzer kann nur auf die seinem Konto zugeordneten Daten zugreifen. Datenbankfunktionen mit erhöhten Rechten sind nur serverseitig verfügbar.

§ 5 Sicherheit der Verarbeitung

- (1) Der Auftragnehmer trifft angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Die technisch bestätigten Maßnahmen sind in Anlage 2 beschrieben.
- (2) Zu Backups oder einer Verschlüsselung ruhender Daten werden in diesem AVV keine über die bestätigten Fakten hinausgehenden technischen Zusagen gemacht.

§ 6 Unterstützung des Auftraggebers

- (1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Betroffenenrechten, soweit dies möglich und erforderlich ist.
- (2) Auskunft und Export können über info@zettelfuchs.app angefordert werden; eine eigene Exportfunktion in der App besteht nicht. Angebote können durch den Nutzer gelöscht werden; bei Kontolöschung werden die im Konto gespeicherten Angebote und damit die darin enthaltenen Kundendaten gelöscht.
- (3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei den Pflichten nach Art. 32 bis 36 DSGVO.

§ 7 Datenschutzverletzungen

- (1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, die Daten aus diesem Auftragsverhältnis betrifft.
- (2) Soweit verfügbar, enthält die Mitteilung die Informationen, die der Auftraggeber für seine Bewertung und gegebenenfalls für Meldungen nach Art. 33 und 34 DSGVO benötigt.

§ 8 Unterauftragsverarbeiter

- (1) Der Auftraggeber erteilt eine allgemeine Genehmigung für die in Anlage 3 genannten Unterauftragsverarbeiter.
- (2) Änderungen an Unterauftragsverarbeitern werden dem Auftraggeber per E-Mail an die Konto-Adresse mitgeteilt. Der Auftraggeber kann innerhalb von 14 Tagen aus einem nachvollziehbaren datenschutzrechtlichen Grund widersprechen.
- (3) Unterauftragsverarbeiter werden durch die jeweiligen AVV/DPA zu den datenschutzrechtlich erforderlichen Pflichten verpflichtet. Der Auftragnehmer bleibt im gesetzlichen Umfang für die Erfüllung der Pflichten verantwortlich.

§ 9 Drittlandübermittlungen

- (1) Die Kern-Projektdaten bei Supabase Pte. Ltd. werden in der vom Auftragnehmer gewählten Region Frankfurt (EU) gehostet. Soweit Supabase oder dessen Unterauftragsverarbeiter im Rahmen von Support, Sicherheit oder Betrieb Daten außerhalb des EWR verarbeiten, gelten die Transferregelungen des abgeschlossenen Supabase-DPA.
- (2) Soweit Auftragsdaten über OpenAI verarbeitet werden, ist für Kunden im EWR nach dem aktuellen OpenAI-DPA OpenAI Ireland Ltd. Vertragspartner. Weiterübermittlungen an verbundene Unternehmen oder Unterauftragsverarbeiter außerhalb des EWR werden nach den im DPA vorgesehenen Transfermechanismen, insbesondere Standardvertragsklauseln oder einem anwendbaren Angemessenheitsbeschluss, abgesichert.
- (3) Soweit Auftragsdaten an Anthropic, PBC in die USA übermittelt werden, erfolgt die Verarbeitung nach den kommerziellen Nutzungsbedingungen und dem darin einbezogenen Anthropic-DPA einschließlich Standardvertragsklauseln.
- (4) Zu providerseitigen Aufbewahrungsdauern oder Trainingsverwendungen bei OpenAI und Anthropic werden keine über die jeweiligen Vertrags- und DPA-Regelungen hinausgehenden Aussagen getroffen.

§ 10 Nachweise und Kontrollen

- (1) Der Auftragnehmer stellt dem Auftraggeber die Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Pflichten aus Art. 28 DSGVO nachzuweisen.
- (2) Der Auftraggeber kann die Einhaltung dieses AVV in angemessenem Umfang selbst oder durch einen zur Vertraulichkeit verpflichteten Prüfer kontrollieren. Vorrangig können geeignete Dokumentationen und technische Beschreibungen genutzt werden.

§ 11 Rückgabe und Löschung

- (1) Preislisten, Vorlagen und Angebote werden bis zur Löschung durch den Nutzer oder bis zur Kontolöschung gespeichert. Bei Kontolöschung werden die im Konto gespeicherten Angebote und die darin enthaltenen Kundendaten gelöscht.
- (2) Eine Rückgabe bzw. ein Export kann vor der Löschung auf Anfrage an info@zettelfuchs.app angefordert werden; eine eigene Exportfunktion in der App besteht nicht.
- (3) Audio wird auf den Servern von Zettelfuchs nicht gespeichert. Transkripte und erzeugte PDFs werden nicht dauerhaft gespeichert. Die Hauptaufnahme bleibt auf dem Gerät des Nutzers nur bis eine neue Aufnahme startet, sie verworfen wird, der Bildschirm verlassen oder die App neu gestartet wird; Adress-Aufnahmen werden direkt nach Verarbeitung gelöscht.
- (4) Soweit Unterauftragsverarbeiter Auftragsdaten verarbeiten, gelten für deren Verarbeitung und Löschung die jeweils abgeschlossenen AVV/DPA.

§ 12 Rangfolge, Haftung und Schlussbestimmungen

- (1) Bei Widersprüchen zwischen diesem AVV und anderen Vereinbarungen der Parteien gehen die Regelungen dieses AVV hinsichtlich der Auftragsverarbeitung vor.
- (2) Die gesetzliche Verantwortungs- und Haftungsverteilung, insbesondere nach Art. 82 DSGVO, bleibt unberührt.
- (3) Änderungen und Ergänzungen dieses AVV können elektronisch vereinbart werden. Bei einer neuen AVV-Version wird die Bestätigung über eine Checkbox erfasst; der Server speichert Dokumenttyp, Version und Server-Zeitpunkt.
- (4) Es gilt deutsches Recht, soweit dem keine zwingenden datenschutzrechtlichen Vorschriften entgegenstehen.

Anlage 1 - Beschreibung der Verarbeitung

Gegenstand	Verarbeitung von Kundendaten des Auftraggebers im Rahmen der Angebotserstellung und -speicherung in Zettelfuchs.
Art und Zweck	Aufnahme und Upload einer Spracheingabe; Transkription durch OpenAI (<code>whisper-1</code>); Strukturierung, Preiszuordnung und bei Adress-Diktaten Erkennung von Name, Straße, PLZ und Ort durch Anthropic Claude Sonnet; Speicherung des Angebots; serverseitige PDF-Erzeugung im eigenen Code und Bereitstellung über das iOS-Teilen-Menü.
Datenarten	Name, Straße, PLZ und Ort des Endkunden; gegebenenfalls personenbezogener Freitext in Angebotspositionen. Keine E-Mail-Adresse und keine Telefonnummer des Endkunden. Für die Preiszuordnung werden Positionen und bis zu 500 Preislisteneinträge (Bezeichnung, Einheit, Preis) an Anthropic übermittelt.
Betroffene Personen	Endkunden und Ansprechpartner des Auftraggebers.
Besondere Daten	Besondere Kategorien nach Art. 9 DSGVO und Daten nach Art. 10 DSGVO sind nicht vorgesehen und sollen nicht eingegeben oder diktiert werden.
Dauer	Das Angebot bleibt bis zur Löschung durch den Nutzer oder bis zur Kontolöschung gespeichert. Audio wird auf Zettelfuchs-Servern nicht gespeichert; Transkripte und PDFs werden nicht dauerhaft gespeichert.

Anlage 2 - Technische und organisatorische Maßnahmen (TOM)

- **Zugriffsschutz und Mandantentrennung:** Row Level Security auf Datenbankebene; jeder Nutzer sieht nur eigene Daten.
- **Authentisierung:** Supabase Auth; serverseitige Ermittlung der Identität aus dem Anmeldetoken.
- **Übertragung:** verschlüsselte Übertragung über HTTPS/TLS.
- **Dateien:** privater Dateispeicher; das Logo ist nur serverseitig abrufbar.
- **Eingabe- und Funktionsschutz:** serverseitige Eingabeprüfung, Rate- und Tageslimits.
- **Privilegierte Datenbankfunktionen:** nur mit Server-Rechten.
- **Hosting:** Supabase-Region Frankfurt (EU).
- **Datenminimierung:** keine dauerhafte Speicherung von Audio auf Zettelfuchs-Servern, keine Speicherung von Transkripten, keine dauerhafte Speicherung erzeugter PDFs.

Zu Backups oder einer Verschlüsselung ruhender Daten werden keine darüber hinausgehenden Aussagen gemacht.

Anlage 3 - Genehmigte Unterauftragsverarbeiter

Dienst	Zweck / Daten	Ort / Vertrag
Supabase Pte. Ltd.	Datenbank, Authentifizierung, Edge Functions und privater Dateispeicher.	Kern-Projektdaten in der gewählten Region Frankfurt (EU); DPA abgeschlossen; begrenzte weitere Verarbeitung nach DPA/Subprocessor-Regelungen möglich.
OpenAI Ireland Ltd. (<code>api.openai.com</code> , <code>whisper-1</code>)	Transkription der Sprachaufnahme; Audio kann Kundendaten enthalten.	EWR-Vertragspartner nach aktuellem OpenAI-DPA; Weiterübermittlungen außerhalb des EWR nach den im DPA vorgesehenen Transfermechanismen.
Anthropic, PBC (<code>api.anthropic.com</code>)	Claude Sonnet für Strukturierung, Preiszuordnung und Adresserkennung.	USA; kommerzielle API-Nutzung nach Anthropic-DPA einschließlich Standardvertragsklauseln.

PostHog, Apple und Resend werden nicht als Unterauftragsverarbeiter für die Kundendaten des Auftraggebers geführt: PostHog verarbeitet nur optionale Analyseereignisse ohne Verknüpfung mit Konto, Name oder E-Mail; Apple verarbeitet das App-Store-Abonnement; Resend versendet App-E-Mails an den Kontoinhaber und die Widerrufsbestätigung.

Anlage 4 - Drittlandübermittlungen und Garantien

- **Supabase:** Supabase Pte. Ltd. hostet die Kern-Projektdaten in der gewählten Region Frankfurt (EU). Begrenzte weitere Support-, Sicherheits- oder Betriebsverarbeitungen erfolgen nach den Regelungen des DPA und der jeweils aktuellen Unterauftragsverarbeiterliste.
- **OpenAI:** Für Kunden im EWR ist nach dem aktuellen OpenAI-DPA OpenAI Ireland Ltd. Vertragspartner. Weiterübermittlungen außerhalb des EWR erfolgen nach den im DPA vorgesehenen Transfermechanismen, insbesondere Standardvertragsklauseln oder einem anwendbaren Angemessenheitsbeschluss.
- **Anthropic:** Anthropic, PBC ist der eingesetzte Anbieter für die kommerzielle API. Der Anthropic-DPA einschließlich Standardvertragsklauseln ist in die kommerziellen Nutzungsbedingungen einbezogen.

Zu providerseitigen Aufbewahrungsdauern oder Trainingsverwendungen bei OpenAI und Anthropic werden keine darüber hinausgehenden Aussagen gemacht.