Auftragsverarbeitungsvertrag (AVV)

Stand: 27. Oktober 2026

nach Art. 28 Abs. 3 DSGVO zwischen dem Kunden als **Verantwortlichem** und Henri Steckhan, Oemberg 67, 45481 Mülheim an der Ruhr, Deutschland, als **Auftragsverarbeiter**.

Der AVV wird nach § 9 unserer AGB mit der Registrierung abgeschlossen und gilt für die gesamte Laufzeit des Hauptvertrags. Eine Unterschrift ist dafür nicht nötig (Textform, Art. 28 Abs. 9 DSGVO). Wer für die eigenen Unterlagen eine unterschriebene Fassung braucht, lädt das PDF mit Unterschriftsfeldern herunter oder schreibt an simon.kurdziel@altoris.one.

1. Gegenstand und Dauer

1. Der Auftragsverarbeiter stellt dem Verantwortlichen die Software HireFlow bereit und verarbeitet dabei personenbezogene Daten in dessen Auftrag. Einzelheiten der Leistung ergeben sich aus dem Hauptvertrag (AGB und gegebenenfalls Angebot).
2. Der AVV gilt, solange der Auftragsverarbeiter personenbezogene Daten für den Verantwortlichen verarbeitet. Bei Widersprüchen geht dieser AVV dem Hauptvertrag in Fragen des Datenschutzes vor.

2. Art, Zweck, Daten, Betroffene

Art und Zweck: Speichern, Strukturieren, Auswerten, Abgleichen, Übermitteln und Löschen von Daten, um Recruiting-Verfahren des Verantwortlichen zu unterstützen: Stellen anlegen, Bewerbungen und Lebensläufe verwalten, Online-Interviews durchführen, Antworten mit KI auswerten, Kandidaten im Talent-Pool abgleichen, Bewerbende per E-Mail einladen und erinnern, Zustimmungen verwalten und Fristen überwachen.

Betroffene: Bewerbende und Kandidaten des Verantwortlichen beziehungsweise seiner Mandanten, Ansprechpersonen bei Mandanten, Mitarbeitende und Teammitglieder des Verantwortlichen.

Datenarten:

- Stamm- und Kontaktdaten (Name, E-Mail-Adresse, Telefonnummer, Wohnort)
- Bewerbungsunterlagen und Lebenslaufdaten (Ausbildung, beruflicher Werdegang, Qualifikationen, Gehaltsvorstellung, Verfügbarkeit)
- Interviewdaten (Antworttexte, aus Sprache erzeugte Texte, Videoaufzeichnungen, Antwortzeiten, Tab-Wechsel)
- Ergebnisse des Persönlichkeitsprofils (Arbeitsweise, Teamfit)
- Auswertungen, Bewertungen, Empfehlungen, Notizen, Pipeline-Status, Zustimmungen mit Zeitpunkt
- Nutzungsdaten der Teammitglieder (Name, E-Mail-Adresse, Rolle, Aktivitäten)

Besondere Kategorien nach Art. 9 DSGVO verarbeitet HireFlow nicht gezielt. Sie können aber in Unterlagen oder Antworten enthalten sein, die Bewerbende oder der Verantwortliche bereitstellen.

3. Weisungen

1. Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf Übermittlungen in Drittländer, es sei denn, er ist durch Unionsrecht oder deutsches Recht dazu verpflichtet. In diesem Fall teilt er dem Verantwortlichen die rechtlichen Anforderungen vorher mit, sofern das Recht dies nicht verbietet.
2. Weisungen sind der Hauptvertrag, dieser AVV und die Einstellungen und Aktionen des Verantwortlichen in HireFlow. Weitere Weisungen erteilt der Verantwortliche in Textform.
3. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich und darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.

4. Pflichten des Auftragsverarbeiters

1. Er verpflichtet alle Personen, die Zugang zu den Daten haben, zur Vertraulichkeit, soweit sie nicht ohnehin einer gesetzlichen Verschwiegenheitspflicht unterliegen.
2. Er trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO aus Anlage 1 und passt sie dem Stand der Technik an. Das Schutzniveau darf dabei nicht sinken.

3. Er nutzt die Daten nicht für eigene Zwecke und nicht zum Training von KI-Modellen und hält die Daten verschiedener Kunden logisch getrennt.
4. Er meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 48 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit verfügbar.
5. Er benennt dem Verantwortlichen eine Ansprechperson für den Datenschutz. Das ist derzeit die im Impressum genannte Kontaktadresse.

5. Unterauftragsverarbeiter

1. Der Verantwortliche genehmigt die in Anlage 2 genannten Unterauftragsverarbeiter.
2. Der Auftragsverarbeiter darf weitere Unterauftragsverarbeiter einsetzen oder bestehende ersetzen (allgemeine Genehmigung nach Art. 28 Abs. 2 DSGVO). Er informiert den Verantwortlichen mindestens vier Wochen vorher in Textform. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund innerhalb dieser Frist widersprechen. Können sich die Parteien nicht einigen, darf der Verantwortliche den Hauptvertrag zum Zeitpunkt des Wechsels kündigen.
3. Der Auftragsverarbeiter legt Unterauftragsverarbeitern vertraglich dieselben Datenschutzpflichten auf wie in diesem AVV. Er haftet gegenüber dem Verantwortlichen für deren Pflichtverletzungen.
4. Keine Unterauftragsverarbeitung sind Nebenleistungen wie Telekommunikation oder die Spracherkennung im Browser der Bewerbenden, die der Browser-Hersteller selbst erbringt.

6. Übermittlung in Drittländer

Eine Verarbeitung außerhalb des Europäischen Wirtschaftsraums findet nur statt, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (EU-US Data Privacy Framework) oder von Standardvertragsklauseln der EU-Kommission. Die jeweilige Grundlage steht in Anlage 2.

7. Unterstützung des Verantwortlichen

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Beantwortung von Anträgen Betroffener (Art. 12 bis 22

DSGVO). HireFlow bietet dafür unter anderem Export, Löschung, automatische Fristen, Zustimmungsverwaltung und eine Selbstauskunft für Bewerbende unter hireflow.one/datenauskunft.

2. Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter.
3. Er unterstützt den Verantwortlichen bei Meldungen nach Art. 33 und 34 DSGVO, bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen (Art. 35, 36 DSGVO) und stellt die dafür nötigen Informationen zur Verfügung, insbesondere zur Funktionsweise der KI-Auswertung.
4. Aufwand, der über die Funktionen der Software und einfache Auskünfte hinausgeht, kann der Auftragsverarbeiter nach vorheriger Ankündigung angemessen in Rechnung stellen, außer er beruht auf einem eigenen Verstoß.

8. Nachweise und Kontrollen

1. Der Auftragsverarbeiter stellt alle Informationen zur Verfügung, die zum Nachweis der Einhaltung seiner Pflichten erforderlich sind, zum Beispiel diese Dokumentation, Zertifikate und Berichte seiner Unterauftragsverarbeiter.
2. Der Verantwortliche oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer kann nach Ankündigung mit angemessener Frist, in der Regel mindestens zwei Wochen, Kontrollen durchführen, auch vor Ort, ohne den Betrieb unverhältnismäßig zu stören.

9. Löschung und Rückgabe

1. Während der Laufzeit löscht HireFlow Bewerberdaten automatisch nach den eingestellten Fristen: ohne Zustimmung 90 Tage nach der letzten Aktivität im Verfahren, mit Zustimmung 12 Monate ab Zustimmung, verlängerbar um jeweils 12 Monate. Der Verantwortliche kann einzelne Daten jederzeit früher löschen.
2. Nach Ende des Hauptvertrags kann der Verantwortliche seine Daten 30 Tage lang exportieren. Danach löscht der Auftragsverarbeiter alle Daten, soweit keine Pflicht zur Speicherung nach Unionsrecht oder deutschem Recht besteht. Kopien in Datensicherungen werden im regulären Rotationszyklus überschrieben, spätestens nach 30 weiteren Tagen.
3. Die Löschung bestätigt der Auftragsverarbeiter auf Anfrage in Textform.

10. Haftung und Schluss

1. Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregeln des Hauptvertrags.
2. Änderungen und Ergänzungen dieses AVV bedürfen der Textform. Für Änderungen gilt § 14 der AGB entsprechend.
3. Sollte eine Bestimmung unwirksam sein, bleibt der AVV im Übrigen wirksam.

Anlage 1: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

- **Vertraulichkeit, Zutritt:** Betrieb ausschließlich in zertifizierten Rechenzentren der Unterauftragsverarbeiter (u. a. ISO 27001, SOC 2). Keine eigenen Server.
- **Zugang:** Anmeldung per Passwort (gespeichert als Hash) oder Google-Konto. Administrative Zugänge zu Datenbank, Hosting und Code nur für die Gründer, mit Zwei-Faktor-Authentifizierung.
- **Zugriff:** Rollen und Rechte je Unternehmen (Inhaber, Admin, Recruiter, Viewer), technisch in der Datenbank durchgesetzt (Row Level Security). Mandantentrennung über Unternehmens- und Mandantenkennungen. Interviewlinks enthalten zufällige, nicht erratbare Token.
- **Weitergabe:** Verschlüsselte Übertragung (TLS) auf allen Verbindungen. Lebensläufe, Antwortvideos und Datenexporte liegen in nicht öffentlichen Speicherbereichen und werden nur über zeitlich begrenzte, signierte Links ausgeliefert. Öffentlich abrufbar sind nur Inhalte, die der Kunde für Bewerbende veröffentlicht, etwa Logo und Begrüßungsvideo.
- **Speicherung:** Verschlüsselung der Datenbank und Dateien im Ruhezustand beim Unterauftragsverarbeiter (AES-256). Datenbank in Frankfurt am Main.
- **Eingabekontrolle:** Protokolle zu Anmeldungen, Änderungen an Kandidaten (Aktivitätsverlauf) und Zustimmungen mit Zeitpunkt.
- **Verfügbarkeit:** Regelmäßige Datensicherungen durch den Datenbankanbieter, redundante Infrastruktur, Überwachung von Fehlern.
- **Datenminimierung und Löschung:** Automatische Löschung bzw. Anonymisierung von Bewerberdaten nach Fristablauf (täglicher Lauf), Erinnerung vor Ablauf einer Zustimmung, Löschung verwaister Dateien.
- **KI-Einsatz:** Übermittlung an KI-Anbieter nur, soweit für die Funktion nötig. Vertragliche Zusage der Anbieter, Daten nicht zum Training zu nutzen. Auswertungen mit Zitaten belegt, Entscheidung durch Menschen.
- **Organisation:** Verpflichtung auf Vertraulichkeit, Prüfung neuer Dienstleister vor Einsatz, regelmäßige Überprüfung dieser Maßnahmen.

Anlage 2: Unterauftragsverarbeiter

Unternehmen	Leistung und Daten	Ort und Übermittlungsgrundlage
Supabase Supabase, Inc., USA	Datenbank, Dateispeicher (Lebensläufe, Videos, Logos) und Anmeldung Alle im Konto gespeicherten Daten, inklusive Bewerberdaten	Rechenzentrum in Frankfurt am Main (AWS eu-central-1); Support und Verwaltung auch aus Drittländern Standardvertragsklauseln der EU-Kommission für Zugriffe aus Drittländern
Vercel Vercel Inc., Covina (Kalifornien), USA	Hosting der Website und Anwendung, Ausführung der Serverfunktionen, anonyme Reichweitenmessung (Vercel Web Analytics) Technische Zugriffsdaten (z. B. IP-Adresse, Zeitpunkt, aufgerufene Seite) und alle Daten, die beim Aufruf verarbeitet werden	Serverfunktionen in Frankfurt am Main (Region fra1); globales Auslieferungsnetz; Unternehmen in den USA EU-US Data Privacy Framework (zertifiziert), ergänzend Standardvertragsklauseln
Anthropic (Claude) Anthropic, PBC, San Francisco, USA	KI-Funktionen: Fragen erzeugen, Antworten und Lebensläufe auswerten, Nachfragen, Matching-Bewertung, Frage-Bot auf der Website Stellenangaben, Antworttexte, Lebenslauftexte, Chat-Fragen von Website-Besuchern	USA Standardvertragsklauseln der EU-Kommission (Bestandteil des Auftragsverarbeitungsvertrags von Anthropic)
OpenAI (Embeddings) OpenAI Ireland Ltd., Dublin, Irland (Vertragspartner im EWR); Verarbeitung durch OpenAI, L.L.C., San Francisco, USA	Umwandlung von Profil- und Stellentexten in Zahlenvektoren für die semantische Vorauswahl im Talent-Pool Lebenslauf- und Profiltexte, Stellentexte	USA Standardvertragsklauseln der EU-Kommission (Bestandteil des Auftragsverarbeitungsvertrags von OpenAI)
Resend Resend, Inc., San Francisco, USA	Versand von E-Mails (Einladungen, Erinnerungen, Benachrichtigungen, Passwort-Links) Name, E-Mail-Adresse, Inhalt der E-Mail	USA EU-US Data Privacy Framework (zertifiziert), ergänzend Standardvertragsklauseln

Unterschriften

Verantwortlicher (Kunde)

Ort, Datum

Unterschrift (Firma, Name, Funktion)

Auftragsverarbeiter: Henri Steckhan

Ort, Datum

Unterschrift (Henri Steckhan)