

# AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

gemäß Art. 28 DSGVO · Stand: Juni 2026

entneo UG (haftungsbeschränkt)  
Donaustraße 44  
12043 Berlin  
Deutschland  
E-Mail: hi@service-win.de

## Vertragspartner

Zwischen dem Nutzer von SoloOS, im Folgenden „Verantwortlicher“, und der

entneo UG (haftungsbeschränkt)  
Donaustraße 44  
12043 Berlin  
Deutschland

Vertreten durch:  
Christoph Hahn, Geschäftsführer

Registergericht:  
Amtsgericht Charlottenburg  
Handelsregisternummer:  
HRB 268903 B

Umsatzsteuer-Identifikationsnummer:  
DE451877052

E-Mail:  
hi@service-win.de

im Folgenden „Auftragsverarbeiter“, wird folgender Vertrag zur Auftragsverarbeitung geschlossen.

## 1. Gegenstand und Dauer

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Rahmen der Nutzung der Software-as-a-Service-Plattform „SoloOS“.

Der Vertrag gilt für die Dauer der Nutzung der Plattform durch den Verantwortlichen. Er wird mit Annahme der Nutzungsbedingungen, Registrierung eines Nutzerkontos oder Aktivierung eines Workspaces wirksam, soweit im Rahmen der Nutzung personenbezogene Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet werden.

## 2. Art und Zweck der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten zur Bereitstellung, Sicherung, Wartung und Weiterentwicklung der SoloOS-Plattform.

Dies umfasst insbesondere:

- Kundenverwaltung (CRM)
- Lead- und Anfrageverwaltung
- Angebots- und Rechnungserstellung
- Auftragsverwaltung
- Aufgaben- und Projektverwaltung
- Kalender- und Terminverwaltung
- Zeiterfassung

- Mitarbeiter- und Teamverwaltung
- Teamkommunikation und Benachrichtigungen
- Dokumentenverwaltung
- Inventarverwaltung
- Exportfunktionen, insbesondere CSV, PDF, DATEV-Vorbereitung, XRechnung und ZUGFeRD, soweit verfügbar
- Zahlungs- und Abonnementverwaltung
- technische Protokollierung, Fehleranalyse und Systemsicherheit

### **3. Art der personenbezogenen Daten**

Im Rahmen der Nutzung von SoloOS können insbesondere folgende Kategorien personenbezogener Daten verarbeitet werden:

- Stammdaten, insbesondere Name, Anschrift, Telefonnummer, E-Mail-Adresse
- Unternehmens- und Geschäftsdaten
- Kunden-, Lead- und Interessentendaten
- Vertrags-, Angebots-, Rechnungs- und Zahlungsdaten
- Auftrags- und Leistungsdaten
- Kommunikationsdaten
- Termin-, Kalender- und Aufgabendaten
- Standort- und Einsatzortdaten, insbesondere Adressen von Einsatzorten
- Mitarbeiterdaten, insbesondere Name, Kontaktdaten, Rolle, Einsatzzeiten und Arbeitszeiten
- Dokumente, Anhänge, Fotos und Nachweise, soweit vom Verantwortlichen hochgeladen
- Inventardaten mit Personenbezug, soweit Gegenstände Personen, Standorten oder Teams zugewiesen werden
- technische Nutzungs- und Protokolldaten, insbesondere Login-Zeitpunkte, IP-Adressen, Geräteinformationen und Fehlermeldungen, soweit für Sicherheit, Betrieb und Nachweis erforderlich

### **4. Kategorien betroffener Personen**

Betroffene Personen können insbesondere sein:

- Endkunden des Verantwortlichen
- Leads und Interessenten des Verantwortlichen
- Mitarbeiter des Verantwortlichen
- Subunternehmer und freie Mitarbeitende des Verantwortlichen
- Geschäftspartner, Lieferanten und Dienstleister des Verantwortlichen
- Ansprechpartner bei Unternehmen, Behörden oder Organisationen
- Nutzer und eingeladene Mitglieder des jeweiligen SoloOS-Workspaces

### **5. Pflichten des Auftragsverarbeiters**

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der dokumentierten Weisungen des Verantwortlichen, sofern keine gesetzliche Verpflichtung zu einer anderweitigen Verarbeitung besteht.

Der Auftragsverarbeiter verpflichtet sich insbesondere:

- die Vertraulichkeit der Verarbeitung gemäß Art. 28 Abs. 3 lit. b DSGVO sicherzustellen
- geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO umzusetzen
- Personen, die Zugriff auf personenbezogene Daten haben, zur Vertraulichkeit zu verpflichten
- den Verantwortlichen bei der Erfüllung seiner Pflichten nach Art. 32 bis 36 DSGVO angemessen zu unterstützen
- den Verantwortlichen bei der Bearbeitung von Betroffenenanfragen angemessen zu unterstützen
- Verletzungen des Schutzes personenbezogener Daten unverzüglich zu melden

- personenbezogene Daten nach Beendigung des Vertrags nach Maßgabe dieses Vertrags zu löschen oder zurückzugeben
- die Einhaltung der in Art. 28 DSGVO genannten Pflichten nachweisen zu können

## 6. Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Vertraulichkeit:

- Zugangskontrolle durch verschlüsselte Authentifizierung
- Passwort-Policy und sichere Login-Verfahren
- rollenbasiertes Berechtigungssystem
- Row Level Security bzw. mandantenbezogene Zugriffsbeschränkung
- Mandantentrennung durch workspacebasierte Datenarchitektur
- Zugriff auf produktive Systeme nur für berechtigte Personen
- TLS-Verschlüsselung bei Datenübertragung
- Integrität: Eingabekontrolle und Protokollierung kritischer Operationen, soweit technisch vorgesehen
- Integrität: Schutz vor unberechtigter Änderung von Daten
- Integrität: Validierung wesentlicher Eingaben
- Integrität: Berechtigungsprüfung vor schreibenden Operationen
- Verfügbarkeit und Belastbarkeit: Einsatz skalierbarer Cloud-Infrastruktur
- Verfügbarkeit und Belastbarkeit: regelmäßige automatische Backups, soweit durch eingesetzte Infrastruktur unterstützt
- Verfügbarkeit und Belastbarkeit: Wiederherstellungsmechanismen, insbesondere über Datenbank-Backups und Point-in-Time-Recovery, soweit verfügbar
- Verfügbarkeit und Belastbarkeit: Monitoring technischer Systeme
- Verfügbarkeit und Belastbarkeit: Schutz vor typischen Webangriffen durch angemessene Sicherheitskonfigurationen
- Trennungskontrolle: getrennte Workspaces und mandantenbezogene Datenzugriffe
- Trennungskontrolle: rollen- und rechtebasierte Zugriffsbeschränkungen
- Trennungskontrolle: Trennung von Entwicklungs-, Test- und Produktivumgebungen, soweit technisch umgesetzt
- Verfahren zur regelmäßigen Überprüfung: regelmäßige Sicherheitsupdates
- Verfahren zur regelmäßigen Überprüfung: Prüfung sicherheitsrelevanter Konfigurationen
- Verfahren zur regelmäßigen Überprüfung: Auswertung von Fehlerprotokollen
- Verfahren zur regelmäßigen Überprüfung: Überprüfung eingesetzter Unterauftragsverarbeiter
- Verfahren zur regelmäßigen Überprüfung: Sicherheitsprüfungen durch Infrastruktur- und Cloud-Anbieter, soweit verfügbar

## 7. Unterauftragsverarbeiter

Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung zur Beauftragung von Unterauftragsverarbeitern.

Zum Stand Juni 2026 können insbesondere folgende Unterauftragsverarbeiter eingesetzt werden:

Anbieter | Zweck | Sitz / Drittlandbezug

Supabase Inc. | Datenbank, Authentifizierung, Storage und Backend-Infrastruktur | EU-Region, insbesondere Frankfurt, soweit konfiguriert; Anbieter mit Sitz in den USA

Vercel Inc. | Application Hosting, Deployment und Edge-Infrastruktur | USA / weltweite Infrastruktur

Cloudflare Inc. | DNS, CDN, Sicherheit und Performance | USA / weltweite Infrastruktur

Bravo / Sendinblue SAS | Transaktions-E-Mails und Systembenachrichtigungen | Frankreich

Stripe Payments Europe Ltd. | Zahlungsabwicklung, Rechnungs- und Abonnementprozesse, soweit eingesetzt | Irland

RevenueCat Inc. | Abonnementverwaltung, Entitlements und Zahlungsstatus, soweit eingesetzt | USA

Mollie B.V. | Zahlungsabwicklung, soweit eingesetzt | Niederlande

Slack Technologies LLC | Interne Systembenachrichtigungen, Support- oder Betriebsprozesse, soweit eingesetzt | USA

Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern mit angemessener Frist, in der Regel 30 Tage vor Wirksamwerden der Änderung.

Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen. Kann dem Widerspruch nicht abgeholfen werden, steht dem Verantwortlichen ein außerordentliches Kündigungsrecht bezüglich der betroffenen Leistung zu.

## 8. Drittlandtransfer

Soweit personenbezogene Daten in Drittländer außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums übermittelt werden, erfolgt dies nur, soweit die datenschutzrechtlichen Voraussetzungen erfüllt sind.

Dies kann insbesondere erfolgen auf Grundlage:

- eines Angemessenheitsbeschlusses der Europäischen Kommission
- des EU-U.S. Data Privacy Framework, soweit der jeweilige Anbieter zertifiziert ist
- von Standardvertragsklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO
- zusätzlicher technischer und organisatorischer Schutzmaßnahmen, soweit erforderlich

## 9. Rechte und Kontrollmöglichkeiten des Verantwortlichen

Der Verantwortliche ist berechtigt:

- Auskunft über die Verarbeitung personenbezogener Daten zu verlangen
- die Einhaltung der vertraglichen und gesetzlichen Pflichten zu kontrollieren
- Weisungen zur Verarbeitung personenbezogener Daten zu erteilen
- Nachweise über geeignete technische und organisatorische Maßnahmen anzufragen
- Audits mit angemessener Vorankündigung durchzuführen oder durch einen geeigneten Prüfer durchführen zu lassen
- Audits sind so durchzuführen, dass Betriebsabläufe, Sicherheitsinteressen und Rechte anderer Kunden nicht unangemessen beeinträchtigt werden. Der Auftragsverarbeiter kann angemessene Nachweise, Zertifizierungen oder Dokumentationen bereitstellen.

## 10. Pflichten des Verantwortlichen

Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten verantwortlich.

Insbesondere stellt der Verantwortliche sicher, dass:

- eine gültige Rechtsgrundlage für die Verarbeitung besteht
- betroffene Personen ordnungsgemäß informiert wurden
- erforderliche Einwilligungen eingeholt wurden
- personenbezogene Daten richtig und erforderlich sind
- Zugriffsrechte innerhalb des eigenen Workspaces angemessen vergeben werden
- Betroffenenanfragen, insbesondere Auskunft, Berichtigung, Löschung und Einschränkung, ordnungsgemäß bearbeitet werden
- keine unzulässigen oder rechtswidrigen Inhalte in SoloOS gespeichert werden

## 11. Unterstützung bei Betroffenenrechten

Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Zumutbaren bei der Erfüllung von Anfragen betroffener Personen nach Kapitel III DSGVO.

Dies betrifft insbesondere:

- Auskunft
- Berichtigung
- Löschung
- Einschränkung der Verarbeitung
- Datenübertragbarkeit
- Widerspruch
- Soweit eine betroffene Person sich unmittelbar an den Auftragsverarbeiter wendet und die Anfrage erkennbar Daten des Verantwortlichen betrifft, leitet der Auftragsverarbeiter die Anfrage nach Möglichkeit an den Verantwortlichen weiter.

## **12. Mitteilungspflichten bei Datenpannen**

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens innerhalb von 24 Stunden nach Bekanntwerden, über Verletzungen des Schutzes personenbezogener Daten, soweit Daten des Verantwortlichen betroffen sind.

Die Meldung enthält, soweit verfügbar, mindestens:

- Beschreibung der Art der Verletzung
- Kategorien und ungefähre Zahl der betroffenen Personen
- Kategorien und ungefähre Zahl der betroffenen Datensätze
- wahrscheinliche Folgen der Verletzung
- ergriffene oder vorgeschlagene Maßnahmen zur Behebung oder Minderung
- Ansprechpartner für Rückfragen

## **13. Löschung und Rückgabe der Daten**

Nach Beendigung des Vertrags werden personenbezogene Daten nach Wahl des Verantwortlichen gelöscht oder in einem maschinenlesbaren Format zur Verfügung gestellt, soweit dies technisch möglich und zumutbar ist.

Sofern keine gesetzlichen Aufbewahrungspflichten oder berechtigten Gründe entgegenstehen, werden personenbezogene Daten innerhalb von 90 Tagen nach Vertragsende gelöscht.

Gesetzliche Aufbewahrungspflichten, insbesondere aus § 147 AO oder § 257 HGB, können einer sofortigen Löschung entgegenstehen. Dies betrifft insbesondere rechnungs-, steuer- und buchhaltungsrelevante Daten.

## **14. Haftung**

Die Haftung richtet sich nach den gesetzlichen Bestimmungen, insbesondere Art. 82 DSGVO, sowie nach den jeweils geltenden Nutzungsbedingungen und Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters.

## **15. Sonstige Bestimmungen**

Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anstelle der unwirksamen Bestimmung gilt die gesetzliche Regelung.

Es gilt deutsches Recht.

Gerichtsstand ist, soweit gesetzlich zulässig, Berlin.

## **16. Inkrafttreten**

Dieser Vertrag wird mit Annahme der Nutzungsbedingungen, Registrierung eines Nutzerkontos, Aktivierung eines Workspaces oder fortgesetzter Nutzung von SoloOS wirksam, soweit personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet werden.

Bei Fragen zum Auftragsverarbeitungsvertrag wenden Sie sich bitte an:

