Auftragsverarbeitungsvertrag (AVV)

Stand: 27. Oktober 2026

Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch CARL im Auftrag des Unternehmens nach Art. 28 DSGVO. Er ist Anlage zu den AGB und kommt mit dem Nutzungsvertrag zustande.

1. Gegenstand und Dauer

1.1

CARL („Auftragsverarbeiter“) verarbeitet personenbezogene Daten im Auftrag des Unternehmens („Verantwortlicher“), um die Software nach den AGB bereitzustellen.

1.2

Der AVV gilt für die Dauer des Nutzungsvertrags und darüber hinaus, solange CARL personenbezogene Daten des Unternehmens verarbeitet.

2. Zweck, Art, Daten und Betroffene

Merkmal	Beschreibung
Zweck	Bereitstellung der Software: Verwaltung von Kunden, Projekten, Terminen, Belegen, Arbeitsberichten und Dateien; Freigabelinks; E-Mails an Endkunden; Anbindung der E-Mail-Konten der Nutzer: Empfang, Anzeige, Versand und Zuordnung von E-Mails; technische Anbindung der Online-Zahlungen: Anzeige des Zahlungsstatus, Übermittlung von Erstattungsaufträgen und Nachweisen des Unternehmens an Stripe, Versand von Zahlungs- und Erstattungsbestätigungen und von Mitteilungen über gescheiterte Lastschriften an Endkunden; KI-Funktionen, soweit genutzt; Support
Art der Verarbeitung	Erheben, Speichern, Ordnen, Anzeigen, Übermitteln, Löschen
Datenarten	Stamm- und Kontaktdaten; Vertrags-, Beleg- und Zahlungsstatusdaten; Termin- und Einsatzdaten; Arbeitszeiten und Tätigkeitsbeschreibungen; Fotos und Dateien; digitale Unterschriften; Bewertungen; Kommunikations- und Protokolldaten; Zahlungsdaten der Endkunden, soweit Stripe sie CARL übermittelt: Betrag, Zeitpunkt, Status, Zahlungsart (Typ, z. B. Karte oder SEPA-Lastschrift), E-Mail-Adresse des Zahlers, Zahlungs-, Erstattungs- und Rückbuchungsreferenzen; vom Unternehmen eingereichte Nachweise zu Anfechtungen; Inhalte von E-Mails einschließlich Anhängen, Absender- und Empfängerangaben und Zeitpunkte; Zugangsdaten zu E-Mail-Konten (verschlüsselt)
Betroffene	Endkunden und deren Ansprechpartner; Endkunden als Zahler; Nutzer des Unternehmens; Absender und Empfänger von E-Mails; sonstige Personen in Inhalten, etwa Lieferanten

Die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) ist nicht vorgesehen. Kartendaten verarbeitet ausschließlich Stripe.

Nicht Gegenstand dieses AVV sind (a) die Zahlungsdaten, die Stripe als eigener Verantwortlicher verarbeitet, denn vollständige Karten- und Kontodaten erreichen CARL nicht, (b) die Angaben zur Verifizierung des Unternehmens und seiner Personen für Online-Zahlungen, für die CARL eigener Verantwortlicher ist (Datenschutzerklärung, Ziffern 5.4 und 5.4a), (c) die Auswertung von Höhe, Art und Verlauf der Zahlungen eines Unternehmens zur Festlegung von Grenzen nach Ziffer 9 der Besonderen Bedingungen Online-Zahlungen (Datenschutzerklärung, Ziffer 5.5) und (d) die Analyse der Nutzung der Software anhand der Nutzer- und Unternehmenskennung (Ziffer 8.4 der AGB; Datenschutzerklärung, Ziffern 2.3 und 3.4) und die anonyme Statistik zu Freigabelink-Seiten (Datenschutzerklärung, Ziffer 4.4). Für beides ist CARL eigener Verantwortlicher; die Zusicherungen in Ziffer 4.5 gelten.

3. Weisungen

3.1

CARL verarbeitet Daten nur auf dokumentierte Weisung des Unternehmens. Die Weisungen ergeben sich aus den AGB und aus der Nutzung der Funktionen der Software. Weitere Weisungen erteilt das Unternehmen in Textform. Die Nutzung der Funktion Online-Zahlungen, insbesondere das Auslösen einer Erstattung und das Einreichen von Nachweisen, ist eine Weisung zur Übermittlung der zugehörigen Daten an Stripe. Bestätigungs-E-Mails an Endkunden versendet CARL nach den in der Software bereitgestellten Vorlagen auf Weisung des Unternehmens; das Unternehmen verantwortet ihre Rechtmäßigkeit (Ziffer 7.8 der AGB).

3.2

Ist CARL nach dem Recht der Union oder eines Mitgliedstaats zu einer Verarbeitung verpflichtet, teilt CARL dies vorher mit, soweit das Recht dies nicht verbietet.

3.3

Hält CARL eine Weisung für rechtswidrig, informiert CARL das Unternehmen unverzüglich. CARL darf die Ausführung bis zur Bestätigung oder Änderung der Weisung aussetzen.

3.4

Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, behandeln die Parteien als Antrag auf Leistungsänderung.

4. Pflichten von CARL

4.1

CARL setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind.

4.2

CARL trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO aus Anlage 1. CARL darf sie weiterentwickeln, solange das Schutzniveau nicht unterschritten wird.

4.3

Den Ansprechpartner für Datenschutz erreicht das Unternehmen unter datenschutz@carl.app.

4.4

CARL verarbeitet Daten in der EU oder im EWR. Eine Übermittlung in Drittländer erfolgt nur durch Unterauftragsverarbeiter nach Anlage 2 und nur unter den Voraussetzungen der Art. 44 ff. DSGVO.

4.5

Bei der Analyse der Nutzung und der Statistik zu Freigabelink-Seiten nach Ziffer 2 (d) verarbeitet CARL keine Inhalte des Unternehmens. CARL sichert zu:

Serverseitig erfasst CARL nur, welcher Schritt wann stattgefunden hat, die Nutzer- und die Unternehmenskennung sowie Merkmale ohne Personenbezug: ob die Registrierung über eine Einladung erfolgte, Name und Nummer des Einrichtungsschritts, Rechtsform und Teamgröße des Unternehmens, Anzahl der Gewerke, ob ein Kunde manuell oder mit KI angelegt wurde, ob ein Kunde, Projekt oder Angebot das erste im Unternehmen ist, Belegart, ob ein Angebot als Kopie entstand, Tarif, Abrechnungsintervall, Anzahl der Plätze und ob die Testphase verlängert wurde. Namen, Adressen, Beträge, Dateien, Inhalte von Belegen und E-Mails sowie IP-Adressen werden dafür nicht übermittelt.

Heatmaps und Sitzungsaufzeichnungen im Browser erfasst CARL nur mit Einwilligung des jeweiligen Nutzers (§ 25 Abs. 1 TDDDG, Art. 6 Abs. 1 lit. a DSGVO). Texte, Eingaben, Bilder, Datei- und Dokumentvorschauen, Unterschriften und Karten werden vor der Übertragung unkenntlich gemacht oder ausgeblendet; Seitenadressen werden ohne Parameter und ohne Kennungen einzelner Datensätze übermittelt; Netzwerkanfragen und Konsolenausgaben werden nicht aufgezeichnet. Aufzeichnungen stellt CARL dem Unternehmen nicht zur Verfügung und nutzt sie nicht zur Verhaltens- oder Leistungskontrolle einzelner Nutzer. Die Entscheidung über die Einwilligung trifft jeder Nutzer selbst; das Unternehmen weist seine Nutzer nicht zur Einwilligung an.

Auf Freigabelink-Seiten führt CARL kein Analyse-Skript aus, setzt keine Cookies und speichert nichts auf dem Gerät des Endkunden. CARL zählt ausschließlich aus den Anfragen, die der Browser für Anzeige und Bedienung der Seite ohnehin sendet, je Kalendertag, Belegart, Schritt, Gerätetyp und Zahlungsart eine Anzahl in der eigenen Datenbank (Anlage 2, Supabase, EU). Die Zähler enthalten keinen Bezug zum Unternehmen, zum Beleg, zum Link, zur Uhrzeit oder zu einer Person und werden an keinen Dritten übermittelt. Sie sind anonym und unterliegen nicht diesem AVV.

Ereignisse der Nutzungsanalyse löscht CARL nach 12 Monaten, Sitzungsaufzeichnungen nach 30 Tagen. Dienstleister für die Nutzungsanalyse ist die PostHog, Inc., USA, als Auftragsverarbeiter von CARL; die Daten liegen in der EU-Cloud von PostHog in Frankfurt am Main, ein Zugriff aus den USA ist auf Grundlage des EU-U.S. Data Privacy Framework und ergänzend der Standardvertragsklauseln möglich. Für die Statistik zu Freigabelink-Seiten ist kein Dienstleister beteiligt.

Jeder Nutzer kann der serverseitigen Analyse nach Ziffer 8.5 der AGB widersprechen und eine Einwilligung jederzeit widerrufen. Auf Verlangen des Unternehmens (datenschutz@carl.app) deaktiviert CARL die serverseitige Analyse für alle Nutzer des Unternehmens; die Nutzbarkeit der Software bleibt unberührt. Wesentliche Änderungen, insbesondere einen Wechsel des Dienstleisters, teilt CARL dem Unternehmen vorab in Textform mit.

5. Unterauftragsverarbeiter

5.1

Das Unternehmen genehmigt allgemein den Einsatz von Unterauftragsverarbeitern. Die aktuell eingesetzten stehen in Anlage 2.

5.2

CARL informiert das Unternehmen mindestens 14 Tage vorher in Textform über die beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Das Unternehmen kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Ohne Widerspruch gilt die Änderung als genehmigt. Bei einem Widerspruch suchen die Parteien eine Lösung; gelingt das nicht, können beide den Vertrag zum Wirksamwerden der Änderung kündigen.

5.3

CARL verpflichtet Unterauftragsverarbeiter vertraglich auf ein gleichwertiges Schutzniveau.

5.4

Eine Übermittlung in Drittländer erfolgt nur auf Grundlage eines Angemessenheitsbeschlusses, einschließlich des EU-U.S. Data Privacy Framework, oder der Standardvertragsklauseln der EU-Kommission.

5.5

Keine Unterauftragsverarbeitung sind Nebenleistungen wie Telekommunikations- oder Postdienste.

6. Unterstützung des Unternehmens

6.1

CARL unterstützt das Unternehmen bei Anfragen betroffener Personen, soweit möglich über die Funktionen der Software wie Export, Berichtigung und Löschung. Anfragen, die CARL direkt erreichen, leitet CARL an das Unternehmen weiter.

6.2

CARL unterstützt das Unternehmen bei den Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei Meldungen und Datenschutz-Folgenabschätzungen.

6.3

Für Unterstützung, die über die Funktionen der Software und den üblichen Umfang hinausgeht, kann CARL eine angemessene Vergütung verlangen, soweit sie nicht auf einem Verstoß von CARL beruht.

7. Meldung von Datenschutzverletzungen

CARL meldet dem Unternehmen eine Verletzung des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 48 Stunden nach Kenntnis. Die Meldung enthält die Informationen nach Art. 33 Abs. 3 DSGVO, soweit verfügbar. CARL ergreift unverzüglich Maßnahmen, um die Folgen einzudämmen.

8. Löschung und Rückgabe

Nach Ende der Verarbeitung kann das Unternehmen seine Daten nach Ziffer 10.5 der AGB exportieren. Anschließend löscht CARL sie nach Ziffern 10.8 bis 10.11 der AGB, soweit keine gesetzliche Pflicht zur Speicherung besteht. Sicherungskopien werden im regulären Rotationszyklus überschrieben. Zahlungsdaten der Endkunden exportiert das Unternehmen als Teil der Zahlungen (Ziffer 10.5 der AGB); gesetzliche Aufbewahrungspflichten dafür erfüllt das Unternehmen selbst (Ziffer 7.5 der AGB).

9. Nachweise und Kontrollen

9.1

CARL stellt dem Unternehmen die Informationen zur Verfügung, die zum Nachweis der Pflichten aus diesem AVV erforderlich sind.

9.2

Kontrollen erfolgen vorrangig durch Auskünfte, Dokumentation und Zertifikate oder Prüfberichte der Unterauftragsverarbeiter. Prüfungen vor Ort sind nach einer Ankündigung von mindestens 30 Tagen während der Geschäftszeiten möglich, höchstens einmal pro Jahr, außer bei konkretem Anlass. Prüfer müssen zur Verschwiegenheit verpflichtet sein und dürfen keine Wettbewerber von CARL sein. Jede Partei trägt ihre eigenen Kosten.

10. Haftung und Schlussbestimmungen

10.1

Gegenüber betroffenen Personen haften die Parteien nach Art. 82 DSGVO. Im Verhältnis zueinander gelten die Haftungsregeln der AGB, soweit Art. 82 DSGVO nicht entgegensteht.

10.2

Bei Widersprüchen zwischen diesem AVV und den AGB geht der AVV in Fragen des Datenschutzes vor.

10.3

Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1. Technische und organisatorische Maßnahmen

Bereich	Maßnahmen
Zutritt	Betrieb ausschließlich in zertifizierten Rechenzentren der Hostinganbieter aus Anlage 2 (u. a. SOC 2 Type 2, ISO 27001); keine eigenen Server
Zugang	Anmeldung nur mit persönlichem Konto; Sitzungen über signierte Tokens (asymmetrische Signatur); Zwei-Faktor-Anmeldung für administrative Zugänge von CARL
Zugriff	Rollen- und Berechtigungskonzept in der Software; Trennung der Daten je Unternehmen auf Datenbankebene (Row Level Security); administrative Zugriffe von CARL nur für berechtigte Mitarbeiter und nur soweit erforderlich
Trennung	Logische Trennung der Daten je Unternehmen; getrennte Entwicklungs-, Test- und Produktivumgebungen
Weitergabe	Übertragung ausschließlich verschlüsselt (TLS); Zugriff auf Dateien über zeitlich begrenzte, signierte Links; Freigabelinks mit nicht erratbaren Kennungen
Eingabe	Aktivitätenprotokoll in der Software (wer hat was wann geändert); Protokollierung auf Systemebene
Verfügbarkeit	Tägliche, verschlüsselte Sicherungen durch den Datenbankanbieter; redundante Infrastruktur der Hostinganbieter; Überwachung von Fehlern
Verschlüsselung	Verschlüsselung gespeicherter Daten und Sicherungen mit AES-256 durch die Hostinganbieter; Zugangsdaten zu E-Mail-Konten zusätzlich auf Anwendungsebene mit AES-256-GCM; Schlüssel getrennt von der Datenbank
Überprüfung	Regelmäßige Überprüfung der Maßnahmen; Verpflichtung der Mitarbeiter auf den Datenschutz; sorgfältige Auswahl und Kontrolle der Unterauftragsverarbeiter

Anlage 2. Unterauftragsverarbeiter

Unterauftragsverarbeiter	Zweck	Ort der Verarbeitung	Garantie für Drittlandübermittlung
Supabase Pte. Ltd, Singapur	Datenbank, Authentifizierung, Dateispeicher	EU (Frankfurt)	Standardvertragsklauseln
Vercel Inc., USA	Hosting der Anwendung, Serverfunktionen	Serverfunktionen EU (Frankfurt); Auslieferung und Betrieb auch in den USA und weltweit	Standardvertragsklauseln
Render Services, Inc., USA	Mail-Dienst: Verbindung zu den E-Mail-Konten der Nutzer, Empfang und Versand	EU (Frankfurt)	EU-U.S. Data Privacy Framework; Standardvertragsklauseln
Plus Five Five, Inc. (Resend), USA	Versand von E-Mails	USA	EU-U.S. Data Privacy Framework; Standardvertragsklauseln
Google Ireland Limited, Irland (Google Workspace)	Geschäfts-E-Mail und Supportkorrespondenz	EU; Zugriff und Verarbeitung auch in den USA und weltweit	EU-U.S. Data Privacy Framework; Standardvertragsklauseln
API Hero Ltd (Trigger.dev), Vereinigtes Königreich	Hintergrundprozesse, etwa Export und E-Mail-Versand	USA	Angemessenheitsbeschluss für das Vereinigte Königreich; Weiterübermittlung in die USA auf Grundlage von Standardvertragsklauseln
Anthropic Ireland, Limited, Irland	KI-Funktionen	USA	Standardvertragsklauseln
OpenAI Ireland Limited, Irland	KI-Funktionen	USA	Standardvertragsklauseln

Keine Unterauftragsverarbeiter sind:

- **Stripe:** verarbeitet Daten im Rahmen der Zahlungsdienste und der Verifizierung als eigener Verantwortlicher (Besondere Bedingungen Online-Zahlungen). Für die Identitätsprüfung mit Stripe Identity ist Stripe Auftragsverarbeiter von CARL als eigenem Verantwortlichen, nicht des Unternehmens.
- **PostHog, Inc.:** verarbeitet Nutzungsdaten nach Ziffer 2 (d) als Auftragsverarbeiter von CARL als eigenem Verantwortlichen, nicht des Unternehmens (Datenschutzerklärung, Ziffern 2.3, 3.4 und 6.1).
- **Google (Google Maps Platform):** Für die Adresssuche und Kartendarstellung verarbeitet Google die übermittelten Daten nach den Controller-Controller-Datenschutzbedingungen von Google als eigener Verantwortlicher. Mit der Nutzung der Adresssuche weist das Unternehmen CARL an, die eingegebenen Suchbegriffe an Google zu übermitteln.
- **E-Mail-Anbieter des Unternehmens (etwa IONOS, Google, Microsoft):** Das Unternehmen nutzt sie auf eigene Verantwortung. CARL greift auf das verbundene Konto nur auf Weisung des Unternehmens zu.