# Vertrag zur Auftragsverarbeitung

nach Art. 28 DSGVO

Version 1.1
Stand: 3. Mai 2026

Dieser Vertrag konkretisiert die Pflichten aus Art. 28 DSGVO zwischen dem Nutzer der SaaS-Plattform „Wo ist der Auftrag?" (Verantwortlicher) und dem Betreiber der Plattform (Auftragsverarbeiter).

# Vertragsparteien

### Auftragsverarbeiter

Jürgen Lichtenauer
Am Hasel 11b
85139 Wettstetten
Deutschland
E-Mail: info@woistderauftrag.de
Telefon: +49 176 343 991 73

*vertreten durch den Inhaber — nachfolgend „Auftragsverarbeiter" genannt*

### Verantwortlicher

Der Nutzer der Plattform „Wo ist der Auftrag?"
— nachfolgend „Verantwortlicher" genannt —

*Die Identität des Verantwortlichen ergibt sich aus dem Hauptvertrag (Account-Registrierung).*

# Präambel

Der Verantwortliche nutzt die SaaS-Anwendung „Wo ist der Auftrag?" zur stationsbasierten Auftragsverfolgung in seinem Handwerksbetrieb. Im Rahmen dieser Nutzung verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen.

Dieser Vertrag konkretisiert die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten gemäß Art. 28 DSGVO. Er ergänzt den zwischen den Parteien bestehenden Hauptvertrag (Allgemeine Geschäftsbedingungen).

## § 1 Gegenstand und Dauer der Verarbeitung

Gegenstand der Auftragsverarbeitung ist die in der SaaS-Anwendung „Wo ist der Auftrag?" erbrachte Leistung gemäß Hauptvertrag, insbesondere die Erfassung, Speicherung und Auswertung von Auftrags-, Stations- und Zeiterfassungsdaten.

Die Auftragsverarbeitung läuft auf unbestimmte Zeit und endet mit dem Ende des Hauptvertrags oder der Löschung des Accounts durch den Verantwortlichen.

## § 2 Art und Zweck der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zur Erbringung der vertraglich vereinbarten SaaS-Leistungen. Dies umfasst insbesondere:

- Bereitstellung einer Mandanten-getrennten Datenbank für Aufträge, Stationen und Zeiterfassungen
- Authentifizierung und Autorisierung der Nutzer
- Erstellung von Dashboards, Ampel-Berechnungen und Auslastungs-Statistiken
- Export von Daten als CSV auf Anforderung des Verantwortlichen
- Backup und Wiederherstellung der Daten
- Supportleistungen auf Anfrage des Verantwortlichen

Eine Verarbeitung zu anderen Zwecken — insbesondere für Werbung, Profiling, KI-Training oder Weitergabe an Dritte — findet nicht statt.

## § 3 Art der personenbezogenen Daten

Vom Auftrag umfasst sind folgende Datenkategorien:

- Stammdaten von Mitarbeitern des Verantwortlichen (Name, Benutzerkennung, Rolle)
- Zeiterfassungsdaten (Stempelzeiten pro Mitarbeiter und Station)
- Auftragsdaten (Auftragsnummer, Titel, Beschreibung, Liefertermin)
- Kundendaten des Verantwortlichen (Name, Anschrift, Kontaktdaten — soweit vom Verantwortlichen eingegeben)
- Technische Protokolldaten (IP-Adresse, Login-Zeitstempel, Aktionslog)

Besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO werden vom Auftragsverarbeiter nicht verarbeitet und dürfen vom Verantwortlichen nicht in der Plattform eingegeben werden.

## § 4 Kategorien betroffener Personen

Von der Datenverarbeitung betroffen sind:

- Mitarbeiterinnen und Mitarbeiter des Verantwortlichen
- Endkunden des Verantwortlichen, soweit deren Daten in Aufträgen erfasst werden
- Weitere Personen, deren Daten der Verantwortliche im Rahmen der Nutzung eingibt

## § 5 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich:

- Die Datenverarbeitung ausschließlich im Rahmen dieses Vertrages und nach dokumentierten Weisungen des Verantwortlichen durchzuführen — es sei denn, eine Verarbeitung ist nach Unionsrecht oder nationalem Recht vorgeschrieben; in diesem Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern dies nicht gesetzlich untersagt ist.
- Alle zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit zu verpflichten, sofern diese nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen.
- Die gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zu treffen (siehe Anlage 2).
- Den Verantwortlichen bei der Wahrnehmung seiner Pflichten aus Art. 32 bis 36 DSGVO zu unterstützen (Datensicherheit, Meldung von Datenpannen, Datenschutz-Folgenabschätzung, vorherige Konsultation).
- Alle Daten nach Beendigung des Hauptvertrags nach Wahl des Verantwortlichen zu löschen oder zurückzugeben, sofern keine Pflicht zur Speicherung nach Unionsrecht oder nationalem Recht besteht.
- Dem Verantwortlichen alle Informationen bereitzustellen, die zum Nachweis der Einhaltung der in Art. 28 DSGVO festgelegten Pflichten erforderlich sind.

## § 6 Pflichten des Verantwortlichen

Der Verantwortliche ist im Sinne der DSGVO für die Rechtmäßigkeit der Datenverarbeitung und die Wahrung der Rechte der betroffenen Personen allein verantwortlich. Er verpflichtet sich insbesondere,

- nur solche Daten in die Plattform einzugeben, für deren Verarbeitung er eine geeignete Rechtsgrundlage nach Art. 6 DSGVO hat,
- die gesetzlichen Informations- und Betriebsrats-Pflichten gegenüber seinen Mitarbeitern einzuhalten (insbesondere § 87 Abs. 1 Nr. 6 BetrVG, § 26 BDSG),
- keine besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO in die Plattform einzugeben,
- seine Zugangsdaten vertraulich zu behandeln und den Auftragsverarbeiter unverzüglich zu informieren, wenn der Verdacht einer Kompromittierung besteht,
- den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen festgestellt werden.

## § 7 Weisungsrecht des Verantwortlichen

Der Verantwortliche erteilt alle Weisungen in Textform (E-Mail genügt) an die Adresse info@woistderauftrag.de. Der Auftragsverarbeiter setzt die Weisungen unverzüglich, spätestens innerhalb von 30 Tagen, um.

Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies dem Verantwortlichen unverzüglich mit und ist bis zur Klärung berechtigt, die Ausführung auszusetzen.

## § 8 Unterauftragsverarbeiter

Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine schriftliche Genehmigung zur Inanspruchnahme weiterer Auftragsverarbeiter im Sinne von Art. 28 Abs. 2 DSGVO. Die derzeit eingesetzten Unterauftragsverarbeiter sind in Anlage 1 aufgeführt.

Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter mindestens 30 Tage im Voraus in Textform. Der Verantwortliche kann der Änderung innerhalb von 14 Tagen nach Zugang der Mitteilung widersprechen. Im Falle eines berechtigten Widerspruchs ist der Auftragsverarbeiter berechtigt, den Hauptvertrag außerordentlich zu kündigen.

Mit sämtlichen eingesetzten Unterauftragsverarbeitern bestehen Verträge, die denselben Datenschutzpflichten entsprechen wie dieser Vertrag — insbesondere Garantien für die Umsetzung geeigneter technisch-organisatorischer Maßnahmen.

## § 9 Technisch-organisatorische Maßnahmen (TOMs)

Der Auftragsverarbeiter trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DSGVO. Die Maßnahmen werden laufend an den Stand der Technik angepasst; Änderungen zulasten der Sicherheit sind nicht zulässig.

## § 10 Meldung von Datenschutzverletzungen

Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Kenntniserlangung, spätestens innerhalb von 48 Stunden, in Textform an die beim Verantwortlichen hinterlegte E-Mail-Adresse. Die Meldung enthält mindestens:

- eine Beschreibung der Art der Verletzung,
- die Kategorien und, soweit möglich, die ungefähre Zahl der betroffenen Personen und Datensätze,
- die wahrscheinlichen Folgen der Verletzung,
- die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und Schadensbegrenzung.

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Meldungen an die Aufsichtsbehörde nach Art. 33 DSGVO und bei Benachrichtigungen betroffener Personen nach Art. 34 DSGVO.

## § 11 Unterstützung bei Betroffenenrechten

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte nachzukommen (Art. 15 bis 22 DSGVO). Dies umfasst insbesondere:

- die Bereitstellung von Daten für Auskunftsersuchen (Art. 15 DSGVO),
- die Berichtigung oder Löschung einzelner Datensätze auf Weisung (Art. 16, 17 DSGVO),
- die Einschränkung der Verarbeitung (Art. 18 DSGVO),
- den Export personenbezogener Daten in einem strukturierten, gängigen und maschinenlesbaren Format (Art. 20 DSGVO, CSV-Export).

Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet dieser die Anfrage unverzüglich an den Verantwortlichen weiter.

## § 12 Löschung und Rückgabe nach Vertragsende

Nach Beendigung des Hauptvertrags bleibt dem Verantwortlichen ein Zeitraum von 30 Tagen eingeräumt, um seine Daten per CSV-Export abzurufen. Nach Ablauf dieser Frist werden sämtliche Daten des Verantwortlichen und seiner betroffenen Personen beim Auftragsverarbeiter und bei dessen Unterauftragsverarbeitern unwiderruflich gelöscht — sofern keine Pflicht zur weiteren Speicherung nach Unionsrecht oder nationalem Recht besteht (insb. § 147 AO, § 257 HGB bezüglich steuerrelevanter Daten).

Der Auftragsverarbeiter bestätigt die vollständige Löschung dem Verantwortlichen auf Anforderung in Textform.

## § 13 Nachweise und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anforderung alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO festgelegten Pflichten zur Verfügung.

Der Verantwortliche hat das Recht, die Einhaltung der Vorschriften über den Datenschutz sowie der vertraglichen Vereinbarungen jederzeit in angemessenem Umfang selbst oder durch beauftragte Prüfer zu kontrollieren. Vor-Ort-Kontrollen bedürfen der vorherigen Ankündigung mit einer Frist von mindestens 14 Tagen und sollen den Geschäftsbetrieb des Auftragsverarbeiters nicht unverhältnismäßig beeinträchtigen. Die Kosten der Kontrolle trägt der Verantwortliche, es sei denn, die Kontrolle deckt erhebliche Verstöße auf.

## § 14 Haftung und Vertragsstrafen

Für die Haftung gelten die Regelungen des Hauptvertrags sowie Art. 82 DSGVO. Die Parteien sind sich einig, dass jede Partei gegenüber der betroffenen Person für den gesamten Schaden haftet, der durch eine nicht datenschutzkonforme Verarbeitung entstanden ist. Im Innenverhältnis erfolgt ein Ausgleich entsprechend dem Verursachungsbeitrag.

## § 15 Schlussbestimmungen

Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform (E-Mail genügt). Dies gilt auch für die Abänderung dieser Textformklausel selbst.

Sollte eine Bestimmung dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt diejenige wirksame Regelung, die dem wirtschaftlichen Zweck der unwirksamen am nächsten kommt.

Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen anderer Vereinbarungen — insbesondere dem Hauptvertrag — gehen die Regelungen dieses Vertrags vor.

Es gilt das Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist der Sitz des Auftragsverarbeiters.

ANLAGE 1

# Unterauftragsverarbeiter

Der Auftragsverarbeiter setzt zur Erbringung der vertraglich vereinbarten Leistungen folgende Unterauftragsverarbeiter ein:

### Vercel Inc.

- Anschrift: 340 S Lemon Ave #4133, Walnut, CA 91789, USA
- Leistung: Hosting der Website und der SaaS-Anwendung
- Verarbeitungsort: EU-Region Frankfurt (fra1)
- Datenschutz-Grundlage: EU-Standardvertragsklauseln (SCC) nach Durchführungsbeschluss (EU) 2021/914; Angemessenheitsbeschluss EU-US Data Privacy Framework
- DPA-Link: vercel.com/legal/dpa

### Supabase Inc.

- Anschrift: 970 Toa Payoh North #07-04, Singapore 318992
- Leistung: Datenbank, File-Storage
- Verarbeitungsort: Schweiz (AWS Zürich, eu-central-2)
- Datenschutz-Grundlage: EU-Angemessenheitsbeschluss Schweiz (2000/518/EG); ergänzend EU-Standardvertragsklauseln (SCC) und EU-US Data Privacy Framework
- DPA-Link: supabase.com/legal/dpa

### Hostinger International Ltd.

- Anschrift: 61 Lordou Vironos Street, 6023 Larnaca, Zypern
- Leistung: SMTP-Versand (ausgehende Transaktions-E-Mails wie Pilot-Bestätigungen und Kündigungs-Eingangsbestätigungen)
- Verarbeitungsort: EU
- Datenschutz-Grundlage: Verarbeitung innerhalb der EU, DSGVO-konform

Stand der Liste: 3. Mai 2026. Änderungen werden dem Verantwortlichen nach § 8 dieses Vertrags mitgeteilt.

ANLAGE 2

# Technische und organisatorische Maßnahmen (TOMs) nach Art. 32 DSGVO

Der Auftragsverarbeiter setzt folgende Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus um:

## 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle: Die eingesetzten Rechenzentren (Vercel fra1, Supabase eu-central-2 [Schweiz], Hostinger EU) verfügen über physische Zugangskontrollen nach Industriestandard (24/7-Wachschutz, Videoüberwachung, Zutrittsprotokollierung, biometrische Authentifizierung, Besucherprotokoll).
- Zugangskontrolle: Multi-Faktor-Authentifizierung (MFA) für Administrator-Accounts; Passwort-Richtlinien nach OWASP-Standards; automatische Sperrung nach fehlgeschlagenen Anmeldeversuchen.
- Zugriffskontrolle: Rollenbasiertes Berechtigungssystem (RBAC) in der Anwendung; mandantengetrennter Datenzugriff durch Row-Level-Security (RLS) auf Datenbankebene; Prinzip der minimalen Rechtevergabe.
- Trennungskontrolle: Vollständige mandantenspezifische Datentrennung auf Datenbankebene — ein Zugriff auf Daten anderer Mandanten ist technisch ausgeschlossen.
- Pseudonymisierung und Verschlüsselung: AES-256-Verschlüsselung ruhender Daten („encryption at rest"); IP-Adressen werden im Rate-Limit nur als SHA-256-Hash gespeichert.

## 2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle: Ausschließlich TLS 1.2+ verschlüsselte Übertragung zwischen Browser, Anwendung, Datenbank und E-Mail-Dienstleister.
- Eingabekontrolle: Audit-Logs für administrative Änderungen; Kündigungen werden mit Zeitstempel und Hash der Kundenzuordnung in den Server-Logs protokolliert.
- Schutz vor Manipulation: Signatur und Integritätsprüfung der Backups.

## 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle: Tägliche automatisierte Backups mit 30 Tagen Vorhaltedauer im Verarbeitungsraum Schweiz/EU.
- Wiederherstellbarkeit: Point-in-time-Recovery (PITR) durch den Datenbank-Dienstleister; dokumentierte Wiederherstellungsverfahren.
- Belastbarkeit: Hosting auf einer horizontal skalierbaren Plattform (Vercel Fluid Compute); DDoS-Schutz auf Netzwerkebene.
- Regelmäßige Sicherheitsupdates der eingesetzten Komponenten (automatisierter Dependency-Scan).

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Auftragskontrolle: Weisungen werden ausschließlich in Textform entgegengenommen und dokumentiert.

- Datenschutz-Management: Jährliche Überprüfung der TOMs; fortlaufende Dokumentation der Verarbeitungstätigkeiten nach Art. 30 DSGVO.
- Incident-Response: Dokumentiertes Verfahren zur Behandlung und Meldung von Datenschutzverletzungen innerhalb von 48 Stunden.

Stand: 3. Mai 2026. Die Maßnahmen werden fortlaufend an den Stand der Technik angepasst.

## Unterzeichnung

Durch Unterzeichnung oder durch Nutzung der Plattform „Wo ist der Auftrag?" bestätigen die Parteien, diesen Vertrag zur Auftragsverarbeitung einschließlich der Anlagen 1 und 2 zur Kenntnis genommen und anerkannt zu haben.

**AUFTRAGSVERARBEITER**

Ort, Datum, Unterschrift

**VERANTWORTLICHER**

Ort, Datum, Unterschrift