Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

Fassung AVV-2026-09-v1

VERANTWORTLICHER
— der jeweilige Kunde —

AUFTRAGSVERARBEITER
IT Solutions Sascha Wolf
An der Hebemärchte 1
04316 Leipzig, Deutschland
USt-IdNr.: DE365311442

Noch nicht abgeschlossen

Hinweis	Dieses Exemplar ist eine Vorschau und kein Nachweis.
Prüfsumme Fassung	2d125969229be33b7a280af7d1f0a05b10911fe6b184d84a759610a11de4ccbd

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

nach Art. 28 der Verordnung (EU) 2016/679 (DSGVO)

Fassung: **AVV-2026-09-v1** - Stand: September 2026

Die Vertragsparteien

Verantwortlicher (nachfolgend „Auftraggeber")

— der jeweilige Kunde —

Auftragsverarbeiter (nachfolgend „Auftragnehmer")

IT Solutions Sascha Wolf An der Hebemärchte 1, 04316 Leipzig, Deutschland Vertreten durch: Sascha Wolf E-Mail: info@wolfinity.io - Telefon: +49 341 9898 2398 USt-IdNr.: DE365311442

Präambel

Der Auftragnehmer stellt dem Auftraggeber die webbasierte Fuhrparkverwaltungs-Software **Fuhriva** als Software-as-a-Service zur Verfügung. Grundlage ist der zwischen den Parteien geschlossene Hauptvertrag (Allgemeine Geschäftsbedingungen des Auftragnehmers).

Bei der Nutzung verarbeitet der Auftraggeber personenbezogene Daten — im Wesentlichen Daten seiner Beschäftigten und Fahrer. Für diese Verarbeitung ist der Auftraggeber Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Der Auftragnehmer verarbeitet diese Daten ausschließlich in seinem Auftrag und ist Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO.

Dieser Vertrag konkretisiert die Pflichten beider Parteien nach Art. 28 DSGVO. Er wird in elektronischer Form geschlossen; das genügt der Form des Art. 28 Abs. 9 DSGVO, der ausdrücklich ein elektronisches Format zulässt. Der Zeitpunkt des Abschlusses, die handelnde Person, die Fassung und eine Prüfsumme des Dokuments werden protokolliert und sind im Kundenbereich unter „Einstellungen -> Auftragsverarbeitung" jederzeit abrufbar.

§ 1 Gegenstand, Dauer und Beendigung

(1) Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Rahmen der Bereitstellung und des Betriebs der Software Fuhriva.

(2) Die Dauer dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Er beginnt mit dem Abschluss dieses Vertrags und endet mit der Beendigung des Hauptvertrags.

(3) Der Auftraggeber kann diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen datenschutzrechtliche Vorschriften oder gegen die Bestimmungen dieses Vertrags vorliegt, oder wenn der Auftragnehmer eine Weisung nicht ausführen kann oder will. Eine Kündigung dieses Vertrags berührt den Hauptvertrag nicht; sie führt jedoch dazu, dass die Software nicht weiter genutzt werden kann, da ihre Nutzung ohne diesen Vertrag nicht zulässig wäre.

§ 2 Art, Umfang und Zweck der Verarbeitung

(1) **Art und Zweck.** Der Auftragnehmer verarbeitet die Daten ausschließlich zum Zweck der Bereitstellung der vertraglich vereinbarten Leistungen: Speicherung, Organisation, Auswertung und Anzeige von Fuhrpark-, Fahrzeug-, Fahrer- und Belegdaten, Versand von Erinnerungen und Benachrichtigungen, Support sowie technischer Betrieb (Sicherung, Fehlersuche, Wartung).

(2) **Ort der Verarbeitung.** Die Verarbeitung erfolgt grundsätzlich in Mitgliedstaaten der Europäischen Union oder in Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum. Soweit in **Anlage 3.1** ein Dienstleister mit einem Verarbeitungsort außerhalb dieses Gebiets ausgewiesen ist, erfolgt die Übermittlung ausschließlich unter den Voraussetzungen der Art. 44 bis 49 DSGVO auf Grundlage der in **Anlage 3.3** genannten Instrumente. Eine

Übermittlung an einen dort nicht ausgewiesenen Empfänger in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers. Die eingesetzten Unterauftragsverarbeiter und alle Drittlandbezüge sind in **Anlage 3.1** benannt.

(3) **Art der Daten und Kategorien betroffener Personen** sind in **Anlage 1** abschließend beschrieben.

(4) Die Verarbeitung **besonderer Kategorien personenbezogener Daten** (Art. 9 DSGVO) ist nicht bestimmungsgemäßer Bestandteil der Leistung. Die Software sieht dafür keine Felder vor, und der Auftragnehmer wertet solche Daten nicht aus. Der Auftraggeber hat ihre Eingabe zu unterlassen, soweit nichts anderes ausdrücklich vereinbart ist; das betrifft insbesondere Freitextfelder (Notizen der Fahrer- und Führerscheinakte, Schadens- und Reparaturbeschreibungen). Gelangen solche Daten gleichwohl in die Software, gelten für sie dieselben Schutzmaßnahmen wie für die übrigen Daten dieses Vertrags.

§ 3 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Rahmen dieses Vertrags allein Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er ist für die Rechtmäßigkeit der Verarbeitung, insbesondere für das Vorliegen einer Rechtsgrundlage, sowie für die Wahrung der Rechte betroffener Personen verantwortlich.

(2) Der Auftraggeber ist allein weisungsbefugt hinsichtlich der verarbeiteten Daten.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er bei der Prüfung der Ergebnisse der Verarbeitung Fehler oder Unregelmäßigkeiten feststellt.

(4) Der Auftraggeber ist verpflichtet, die im Rahmen dieses Vertrags erlangten Informationen über technische und organisatorische Maßnahmen des Auftragnehmers vertraulich zu behandeln.

(5) Der Auftraggeber benennt dem Auftragnehmer eine ansprechbare Person für Fragen des Datenschutzes. Ohne gesonderte Benennung gilt die Person, die diesen Vertrag abgeschlossen hat.

§ 4 Weisungsgebundenheit (Art. 28 Abs. 3 lit. a DSGVO)

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, einschließlich in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland.

(2) Als dokumentierte Weisung gelten dieser Vertrag, der Hauptvertrag sowie die Nutzung der Funktionen der Software durch den Auftraggeber und seine Nutzer im vertragsgemäßen Rahmen. Darüber hinausgehende Einzelweisungen erteilt der Auftraggeber in Textform an info@wolfinity.io oder über das Support-System der Software. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Der Auftragnehmer ist berechtigt, die Ausführung einer solchen Weisung auszusetzen, bis sie vom Auftraggeber bestätigt oder geändert wird.

(4) Eine Verarbeitung außerhalb der Weisungen ist nur zulässig, soweit der Auftragnehmer hierzu nach dem Recht der Union oder der Mitgliedstaaten verpflichtet ist. In diesem Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

§ 5 Vertraulichkeit (Art. 28 Abs. 3 lit. b DSGVO)

(1) Der Auftragnehmer setzt zur Verarbeitung ausschließlich Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung wirkt über das Ende der Tätigkeit hinaus.

(2) Der Auftragnehmer macht die eingesetzten Personen vor Aufnahme der Tätigkeit mit den für sie geltenden Datenschutzbestimmungen vertraut.

(3) Der Zugriff auf Daten des Auftraggebers ist auf diejenigen Personen beschränkt, die ihn zur Erfüllung der vertraglichen Leistungen benötigen. Zugriffe im Rahmen des Supports, bei denen der Auftragnehmer die

Benutzersicht des Auftraggebers einnimmt, sind technisch zeitlich begrenzt und werden protokolliert; das Protokoll ist dem Auftraggeber auf Anforderung zugänglich.

§ 6 Technische und organisatorische Maßnahmen (Art. 28 Abs. 3 lit. c, Art. 32 DSGVO)

(1) Der Auftragnehmer trifft die zur Sicherheit der Verarbeitung erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Der Stand dieser Maßnahmen bei Vertragsschluss ist in **Anlage 2** beschrieben.

(2) Die Maßnahmen unterliegen der technischen Weiterentwicklung. Dem Auftragnehmer steht es frei, sie anzupassen, solange das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber mit.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der in Art. 32 DSGVO genannten Pflichten.

§ 7 Unterauftragsverarbeiter (Art. 28 Abs. 2 und 4 DSGVO)

(1) Der Auftraggeber erteilt dem Auftragnehmer die **allgemeine Genehmigung** zur Hinzuziehung weiterer Auftragsverarbeiter. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in **Anlage 3.1** benannt und damit genehmigt. Die in Anlage 3.2 aufgeführte Zahlungsabwicklung ist davon nicht erfasst; sie betrifft die Vertrags- und Rechnungsdaten des Auftraggebers und nicht die dem Auftrag anvertrauten Daten.

(2) Beabsichtigt der Auftragnehmer, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden auszutauschen, teilt er dies dem Auftraggeber mindestens **vier Wochen** vorher in Textform mit. Der Auftraggeber kann der Änderung innerhalb von **zwei Wochen** nach Zugang der Mitteilung aus wichtigem, datenschutzbezogenem Grund in Textform widersprechen. Widerspricht er, und lässt sich die Leistung ohne den betreffenden Unterauftragsverarbeiter nicht in gleicher Weise erbringen, so ist jede Partei berechtigt, den Hauptvertrag zum Zeitpunkt des beabsichtigten Wechsels zu kündigen.

(3) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten, die ihn selbst nach diesem Vertrag treffen, und wählt ihn sorgfältig aus. Er bleibt dem Auftraggeber gegenüber für die Einhaltung dieser Pflichten verantwortlich.

(4) Nicht als Unterauftragsverarbeitung im Sinne dieser Bestimmung gelten Nebenleistungen, die der Auftragnehmer bei Dritten in Anspruch nimmt und die nicht auf die Verarbeitung personenbezogener Daten des Auftraggebers gerichtet sind (z. B. Telekommunikations- oder Reinigungsleistungen). Der Auftragnehmer trifft auch insoweit angemessene Vorkehrungen zum Schutz der Daten.

§ 8 Unterstützung bei Betroffenenrechten (Art. 28 Abs. 3 lit. e DSGVO)

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen nach Kapitel III der DSGVO nachzukommen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch).

(2) Die Software stellt dem Auftraggeber hierfür eigene Funktionen bereit, insbesondere zur Einsicht, Berichtigung, Löschung und zum Export von Daten. Soweit der Auftraggeber sein Anliegen damit selbst erfüllen kann, gilt die Unterstützungspflicht als erfüllt.

(3) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Anliegen unverzüglich an den Auftraggeber weiter und beantwortet es nicht selbst.

(4) Der Auftragnehmer berichtigt oder löscht Daten nur auf Weisung des Auftraggebers, es sei denn, er ist gesetzlich zu etwas anderem verpflichtet.

§ 9 Unterstützung bei Sicherheit, Meldepflichten und Folgenabschätzung (Art. 28 Abs. 3 lit. f DSGVO)

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

(2) Der Auftragnehmer meldet dem Auftraggeber jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten **unverzüglich, spätestens innerhalb von 48 Stunden** nach Kenntnisnahme, in Textform. Die Meldung enthält, soweit bekannt: die Art der Verletzung, die betroffenen Datenkategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Gegenmaßnahmen.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO sowie, soweit erforderlich, bei einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer vorherigen Konsultation nach Art. 36 DSGVO.

(4) Meldungen an die Aufsichtsbehörde oder an betroffene Personen gibt ausschließlich der Auftraggeber ab.

§ 10 Löschung und Rückgabe nach Beendigung (Art. 28 Abs. 3 lit. g DSGVO)

(1) Nach Beendigung der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer alle personenbezogenen Daten des Auftraggebers oder gibt sie nach dessen Wahl zurück, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht.

(2) Der Auftraggeber teilt dem Auftragnehmer **innerhalb von 30 Tagen nach Beendigung** mit, ob er die Rückgabe der Daten oder ihre Löschung wünscht. Erteilt er innerhalb dieser Frist keine Weisung, löscht der Auftragnehmer die Daten nach Absatz 3. Unabhängig davon kann der Auftraggeber seine Daten bis zur Beendigung jederzeit selbst über die Exportfunktionen der Software herausziehen; nach Beendigung stellt der Auftragnehmer sie auf Anforderung in einem gängigen, maschinenlesbaren Format bereit.

(3) Die Löschung aus den produktiven Systemen erfolgt spätestens **90 Tage** nach Beendigung des Vertrags. Aus den Datensicherungen werden die Daten im Rahmen des regulären Sicherungszyklus gelöscht oder überschrieben, spätestens jedoch **90 Tage** nach der Löschung aus den produktiven Systemen; bis dahin bleiben sie verschlüsselt, für die weitere Verarbeitung gesperrt und werden ausschließlich zum Zweck der Wiederherstellung vorgehalten.

(4) Dokumentationen, die dem Nachweis der auftragsgemäßen Verarbeitung dienen, darf der Auftragnehmer über das Vertragsende hinaus entsprechend den jeweiligen Aufbewahrungsfristen verwahren. Er kann sie dem Auftraggeber zu dessen Entlastung bei Vertragsende übergeben.

§ 11 Nachweise und Überprüfungen (Art. 28 Abs. 3 lit. h DSGVO)

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

(2) Der Auftragnehmer ermöglicht Überprüfungen — einschließlich Inspektionen — durch den Auftraggeber oder einen von diesem beauftragten Prüfer und trägt dazu bei. Der beauftragte Prüfer darf kein Wettbewerber des Auftragnehmers sein und ist zur Verschwiegenheit zu verpflichten.

(3) Überprüfungen erfolgen nach Ankündigung mit angemessener Frist, grundsätzlich mindestens **zwei Wochen** vorher, während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs, in der Regel höchstens einmal je Kalenderjahr. **Die Beschränkungen dieses Absatzes gelten nicht, soweit eine Datenschutz-Aufsichtsbehörde eine Prüfung verlangt oder konkrete Anhaltspunkte für einen Verstoß bestehen** — insbesondere nach einer Verletzung des Schutzes personenbezogener Daten. In diesen Fällen entfällt die Beschränkung auf einmal jährlich und die Ankündigungsfrist verkürzt sich angemessen.

(4) Der Auftragnehmer kann den Nachweis auch durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Stellen, geeignete Zertifizierungen oder eine Selbstauskunft mit aussagekräftiger Dokumentation der technischen und organisatorischen Maßnahmen führen.

(5) Für Überprüfungen, die über die Bereitstellung von Informationen hinausgehen und einen erheblichen Aufwand verursachen, kann der Auftragnehmer eine angemessene Vergütung verlangen; dies gilt **nicht**, wenn die Überprüfung durch einen vom Auftragnehmer zu vertretenden Umstand veranlasst ist oder von einer Aufsichtsbehörde verlangt wird.

§ 12 Haftung

(1) Für die Haftung der Parteien untereinander gelten die Regelungen des Hauptvertrags.

(2) Art. 82 DSGVO bleibt unberührt.

§ 13 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Das gilt auch für die Aufhebung dieses Formerfordernisses.

(2) Der Auftragnehmer kann diesen Vertrag anpassen, wenn dies aufgrund einer Änderung der Rechtslage, aufgrund von Vorgaben einer Aufsichtsbehörde oder aufgrund der technischen Weiterentwicklung der Leistung erforderlich ist. **Wesentliche Änderungen** legt er dem Auftraggeber in der Software zur erneuten Bestätigung vor. Für die Bestätigung stehen **sieben Tage** ab Veröffentlichung der neuen Fassung zur Verfügung; bei Konten, die erst danach angelegt werden, läuft die Frist ab der Anlage des Kontos. **Bis zur Bestätigung bleibt die zuletzt bestätigte Fassung maßgeblich**, soweit sie die laufende Verarbeitung weiterhin abdeckt.

Erfolgt die Bestätigung nicht innerhalb der Frist, nimmt das Konto **keine Änderungen mehr an**: Anlegen, Ändern und Löschen von Daten sind gesperrt. Einsicht in den vorhandenen Bestand, dessen Ausleitung über die Exportfunktionen, die Verwaltung des Kontos und der Zugang zum Support bleiben möglich, damit der Auftraggeber jederzeit über seine Daten verfügen kann.

Redaktionelle Änderungen, die den Inhalt der Rechte und Pflichten nicht berühren, teilt der Auftragnehmer mit, ohne eine erneute Bestätigung zu verlangen. Jede Fassung bleibt in der Software abrufbar; für den Zeitraum, in dem sie galt, ist sie der maßgebliche Vertrag.

(3) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die dem wirtschaftlichen Zweck am nächsten kommt.

(4) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags vor, soweit es um die Verarbeitung personenbezogener Daten geht.

(5) Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1 — Gegenstand der Verarbeitung

1.1 Kategorien betroffener Personen

- Beschäftigte des Auftraggebers, die die Software nutzen (Benutzerkonten)
- Fahrerinnen und Fahrer des Auftraggebers, auch ohne eigenen Zugang
- Ansprechpartner des Auftraggebers für Vertrag, Rechnung und Support
- Ansprechpartner von Werkstätten, Partnern und Geschäftspartnern, soweit

der Auftraggeber sie erfasst

1.2 Art der personenbezogenen Daten

Datenkategorie	Inhalt
Benutzer-Stammdaten	Name, E-Mail-Adresse, Passwort-Hash, Sprache, Zeitpunkt der letzten Anmeldung
Zweiter Faktor	TOTP-Geheimnis (verschlüsselt gespeichert), Backup-Codes, registrierte Push-Geräte
Sitzungsdaten	IP-Adresse, Browserkennung, Sitzungs-Token

Datenkategorie	Inhalt
Mitgliedschaft und Rechte	Zuordnung Benutzer <-> Konto, Rolle, Berechtigungsgruppe, Tochterfirma
Personaldaten der Fahrer	Name, Kontakt-E-Mail, Telefonnummer, Personalnummer, Geburtsdatum
Führerscheindaten	Führerscheinnummer, Ausstellungs- und Ablaufdatum, Klassen, Kontrolltermine, Notizen
Fahreignung / Punkte	Vom Auftraggeber selbst gepflegte Angaben zu Verkehrsverstößen und Punkten: Tattag, Punktzahl, vorbelegtes Tilgungsdatum — keine Auskunft aus dem Fahreignungsregister
Fahrtenbuch	Fahrerzuordnung, Start- und Zielort, Kilometerstände, Zweck, Geschäftspartner, Änderungsprotokoll, Integritäts-Prüfsumme
Fahrzeug- und Flottendaten	Kennzeichen, Fahrgestellnummer, Halter- und Standortangaben, Zuordnung zu Personen
Schäden und Reparaturen	meldende Person, Beschreibung, Fotos, Kosten
Tankvorgänge	erfassende Person, Zeitpunkt, Menge, Betrag, Ort
Poolbuchungen	buchende Person, Fahrer, Zweck, Ziel, Rückgabe
Telemetrie (Erweiterung „Fuhriva Connect")	Fahrzeugzustandsdaten aus dem Bordnetz, Fehlerspeicher, Kilometerstand, Aufprallereignisse, jeweils mit Zeitstempel und Fahrzeugbezug
Support	Tickets und Nachrichten, Absender, Inhalt
Protokolle	Sicherheitsprotokoll (Ereignis, IP-Adresse, Browserkennung, Benutzer, Pfad), E-Mail-Versandprotokoll (Empfänger, Betreff, Status), Push-Versandprotokoll
Vertrags- und Rechnungsdaten	Firmenname, Anschrift, USt-IdNr., Steuernummer, Rechnungs-E-Mail

1.3 Zweck der Verarbeitung

Bereitstellung und Betrieb der Fuhrparkverwaltung: Verwaltung von Fahrzeugen, Personen und Terminen, Unterstützung bei Dokumentations- und Nachweispflichten des Auftraggebers (Fahrtenbuch, Führerscheinkontrolle, Halterpflichten), Erinnerungen und Benachrichtigungen, Auswertungen für den Auftraggeber, Support sowie technischer Betrieb einschließlich Datensicherung und Fehlersuche.

1.4 Aufbewahrung und Löschung

Daten	Regel
Stamm- und Bewegungsdaten	Löschung mit dem Konto bzw. auf Weisung des Auftraggebers

Daten	Regel
Sitzungen	Löschung 30 Tage nach Ablauf; IP-Adresse und Browserkennung werden nach 30 Tagen anonymisiert
Sicherheitsprotokoll	Löschung nach 90 Tagen
E-Mail-Versandprotokoll	Löschung nach 12 Monaten
Push-Versandprotokoll	Löschung nach 90 Tagen
Telemetrie-Messwerte	Löschung nach 180 Tagen, gerechnet ab dem Zeitpunkt der Aufzeichnung
Aufprallereignisse (Telemetrie)	Löschung 730 Tage nach Quittierung; unquittierte Ereignisse bleiben erhalten
Fahrtenbuch	keine automatische Löschung — steuerliche Aufbewahrungspflichten des Auftraggebers
Unbestätigte Registrierungen	Löschung nach 24 Tagen

Anlage 2 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

2.1 Vertraulichkeit

Zutrittskontrolle. Die Systeme werden im Rechenzentrum der Hetzner Online GmbH in Falkenstein (Sachsen, Deutschland) betrieben — die Anwendung, die Datenbank, der Objektspeicher für hochgeladene Dateien und die Datensicherungen. Zutrittsschutz, Videoüberwachung und Besucherverwaltung obliegen dem Rechenzentrumsbetreiber; der Auftragnehmer selbst betreibt keine eigene Serverinfrastruktur mit Kundendaten.

Zugangskontrolle. Der Zugang zu Daten des Auftraggebers erfolgt über persönliche Benutzerkonten, wahlweise mit Passwort oder über ein verknüpftes Google-Konto. Davon ausgenommen sind zwei Wege: das öffentlich zugängliche Demonstrationskonto des Auftragnehmers, das ohne Zugangsdaten betreten werden kann, mit erfundenen Beispieldaten befüllt ist und keine Änderungen an Fahrzeug-, Personen- oder Fahrtdaten zulässt, sowie kurzlebige signierte Verweise auf einzelne Dateien (Standard 10, höchstens 60 Minuten), die ausschließlich ein bereits berechtigter Benutzer ausstellen kann. Passwörter werden ausschließlich als Hash gespeichert, nicht protokolliert und über die unter *Weitergabekontrolle* beschriebene verschlüsselte Verbindung übertragen. Zwei-Faktor-Authentisierung (TOTP oder Freigabe per App mit Zahlenabgleich) ist verfügbar und kann vom Auftraggeber verpflichtend geschaltet werden; sie wird serverseitig auf allen Endpunkten durchgesetzt, die Kundendaten führen. Anmeldeversuche unterliegen einer IP-genauen Ratenbegrenzung; fehlgeschlagene Anmeldungen werden protokolliert und ausgewertet. Eine IP-Sperrliste steht zur Verfügung.

Zugriffskontrolle. Rollen- und gruppenbasierte Berechtigungen je Konto; Sichtbarkeit von Fahrzeugen und Personen ist zusätzlich einschränkbar. Zugriffe des Auftragnehmers in der Benutzersicht eines Kunden (Impersonation) sind auf 30 Minuten begrenzt, jederzeit widerrufbar und werden mit Zeitpunkt, handelndem Administrator und betroffenem Benutzer protokolliert. Die Protokolleinträge werden 90 Tage aufbewahrt.

Trennungskontrolle. Die Daten mehrerer Auftraggeber liegen in einer gemeinsamen Datenbank und werden logisch getrennt: Abfragen auf Kundendaten werden auf das Konto des angemeldeten Benutzers eingegrenzt.

Gehört ein Benutzer mehreren Konten an und wählt eines davon über eine Kopfzeile oder einen Parameter aus, wird diese Angabe serverseitig gegen seine Mitgliedschaften geprüft; ein Konto, dem er nicht angehört, ist darüber nicht erreichbar. Die Einhaltung wird durch einen automatisierten Angriffstest nachgewiesen, der bei jeder Änderung am System läuft: er ruft mit den Zugangsdaten eines Mandanten die Endpunkte mit den Kennungen eines zweiten auf und prüft, dass keine Antwort fremde Daten enthält und dass sich der Bestand des zweiten Mandanten dabei nicht verändert. Die geprüfte Endpunktliste wird dabei aus dem Quelltext abgeleitet, damit sie nicht veraltet.

Dateien werden je Konto getrennt abgelegt und nur an Benutzer des jeweiligen Kontos ausgeliefert; für Clients ohne Sitzung (mobile Anwendung) über signierte Verweise mit höchstens 60 Minuten Gültigkeit.

Pseudonymisierung und Anonymisierung. Die Adresse des anfragenden Rechners wird im Zugriffslog des Webservers vor dem Schreiben um das letzte Oktett bzw. die unteren IPv6-Blöcke gekürzt. IP-Adresse und Browserkennung in Sitzungen werden nach 30 Tagen anonymisiert. Im Reichweiten-Tracking werden IP-Adressen ausschließlich gekürzt gespeichert.

2.2 Integrität

Weitergabekontrolle. Die Anwendung wird ausschließlich über TLS 1.2 oder 1.3 ausgeliefert. Ein unverschlüsselter Aufruf auf Port 80 wird ohne Verarbeitung auf HTTPS umgeleitet; HSTS verhindert weitere Klartext-Aufrufe. Datenbank und Cache sind ausschließlich im internen Container-Netz erreichbar und aus dem öffentlichen Netz nicht ansprechbar.

Eingabekontrolle. Sicherheitsrelevante Vorgänge — Anmeldungen und fehlgeschlagene Anmeldeversuche, Änderungen an Benutzern, Rollen und Berechtigungen sowie Eingriffe des Auftragnehmers — werden mit Zeitpunkt, handelnder Person, IP-Adresse und Pfad protokolliert und 90 Tage aufbewahrt. Fahrten führen ein Änderungsprotokoll und eine Integritäts-Prüfsumme und sind nach 30 Tagen unveränderlich. Korrekturen durch den Support sind nur mit Begründung möglich und werden gesondert protokolliert.

Schutz vor Schadinhalten. Hochgeladene Dateien sind auf eine feste Liste zulässiger Dateitypen begrenzt; verbreitete ausführbare und skriptfähige Dateiendungen sind zusätzlich gesperrt. Bei Formaten mit einer Dateisignatur wird der tatsächliche Inhalt gegen den vom Browser angegebenen Typ geprüft — bei Text- und E-Mail-Formaten, die keine Signatur besitzen, greift allein die Endungssperre. Ausgeliefert werden hochgeladene Dateien als Download; im Browser angezeigt werden nur Bilder und PDF. Pfadangaben werden gegen Verzeichniswechsel abgesichert. Die HTML-Auslieferung der Weboberfläche erfolgt mit einer Content-Security-Policy auf Nonce-Basis.

2.3 Verfügbarkeit und Belastbarkeit

Automatisierte, **verschlüsselte** Datenbanksicherungen; ohne hinterlegten Sicherungsschlüssel wird keine Sicherung erstellt. Überwachung von Sicherungslauf, Hintergrundaufträgen und angebundenen Diensten mit Alarmierung bei Ausfall. Getrennte Container für Weboberfläche, Schnittstelle und Hintergrundverarbeitung. Ratenbegrenzung und Begrenzung der Anfragegröße als Schutz vor Überlastung.

2.4 Verfahren zur Überprüfung, Bewertung und Evaluierung

Auftragskontrolle: die in Anlage 3.1 genannten Dienstleister werden nach § 7 Abs. 3 vertraglich auf dieselben Datenschutzpflichten verpflichtet, die den Auftragnehmer nach diesem Vertrag treffen. Datenschutzfreundliche Voreinstellungen: Module, die über die Fahrzeugverwaltung hinaus Personenbezug erzeugen — Fahrzeug-Telemetrie, Führerscheinkontrolle, Poolfahrzeuge, Versicherungen — sind im Auslieferungszustand abgeschaltet und werden erst durch eine Entscheidung des Auftraggebers aktiv. Automatisierte Sicherheits- und Mandantentrennungsprüfungen laufen bei jeder Änderung am System; Abhängigkeiten werden dabei auf bekannte Schwachstellen geprüft. Vorfälle werden dokumentiert und ausgewertet.

2.5 Verschlüsselung im Ruhezustand

Gegenstand	Maßnahme

Gegenstand	Maßnahme
Passwörter	Ausschließlich als Hash gespeichert
TOTP-Geheimnisse	Verschlüsselt in der Datenbank; der Schlüssel wird abgeleitet und nicht in der Datenbank abgelegt
Datenbanksicherungen	Symmetrisch verschlüsselt; ohne Schlüssel kein Sicherungslauf
Zugangsdaten zu Fremddiensten	Hinterlegt als Umgebungsvariablen oder in

einer Systemtabelle, die nur Administratoren des Auftragnehmers lesen; sie werden nie an die Oberfläche zurückgegeben und erscheinen in Protokollen nicht oder nur maskiert |

Anlage 3 — Eingesetzte Dienstleister

Genehmigt mit Abschluss dieses Vertrags (§ 7 Abs. 1).

3.1 Dienstleister, die dem Auftrag anvertraute Daten verarbeiten

Diese Dienstleister erhalten personenbezogene Daten, die der Auftraggeber in die Software einbringt — insbesondere Daten seiner Beschäftigten und Fahrer.

Unternehmen	Sitz / Ort der Verarbeitung	Leistung	Übermittelte Daten
Hetzner Online GmbH	Falkenstein, Deutschland (EU)	Server und Betrieb der Anwendung	alle im Rahmen der Nutzung verarbeiteten Daten
Hetzner Online GmbH — Object Storage	Falkenstein, Deutschland (EU)	Speicherung hochgeladener Dateien und Dokumente — nur bei aktivierter Objektspeicherung; andernfalls verbleiben die Dateien auf dem Server	Fahrzeugdateien, Belege, Fotos
Amazon Web Services EMEA SARL — SES	Region eu-central-1, Frankfurt am Main (EU); Konzernmutter USA	Versand transaktionaler E-Mails — nur, soweit dieser Dienst als Versandweg konfiguriert ist	Empfängeradresse, Betreff und Inhalt der Nachricht
Google Ireland Limited	Irland (EU); Konzernmutter USA	Anmeldung mit Google-Konto — nur, wenn der Auftraggeber sie nutzt	Name, E-Mail-Adresse, Profilbild der anmeldenden Person
Expo (650 Industries, Inc.)	USA	Zustellung mobiler Benachrichtigungen — nur bei Nutzung der mobilen App	Push-Token des Geräts, Inhalt der Benachrichtigung, Benutzerkennung

Unternehmen	Sitz / Ort der Verarbeitung	Leistung	Übermittelte Daten
1NCE GmbH	Deutschland (EU)	Mobilfunkanbindung der Telemetrie-Geräte — nur bei aktiver Erweiterung „Fuhriva Connect"	Gerätekennungen (IMEI, ICCID), Verbindungs- und Verbrauchsdaten; keine Fahrzeug- oder Fahrerdaten

3.2 Zahlungsabwicklung

Unternehmen	Sitz	Leistung	Übermittelte Daten
Stripe Payments Europe Ltd.	Irland (EU); Konzernmutter USA	Zahlungsabwicklung und Abonnementverwaltung	Firmenname, Rechnungsanschrift, USt-IdNr., Rechnungs-E-Mail-Adresse, Zahlungsdaten

Dieser Punkt betrifft die Vertrags- und Rechnungsdaten des Auftraggebers selbst, nicht die dem Auftrag anvertrauten Daten seiner Beschäftigten und Fahrer. Der Zahlungsdienstleister verarbeitet diese Daten teilweise zu eigenen Zwecken — etwa zur Betrugsprävention und zur Erfüllung eigener aufsichtsrechtlicher Pflichten — und ist insoweit eigenständig Verantwortlicher. Er wird hier zur Vollständigkeit aufgeführt, damit der Auftraggeber den gesamten Datenfluss übersieht.

3.3 Grundlage der Übermittlung

Die in 3.1 genannten Dienstleister werden nach § 7 Abs. 3 auf dieselben Datenschutzpflichten verpflichtet, die den Auftragnehmer nach diesem Vertrag treffen. Soweit eine Verarbeitung außerhalb der Europäischen Union stattfinden kann, erfolgt die Übermittlung auf Grundlage der mit dem jeweiligen Anbieter vereinbarten Instrumente — insbesondere Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO oder eines Angemessenheitsbeschlusses der Europäischen Kommission. Die jeweils geltenden Instrumente nennt der Auftragnehmer dem Auftraggeber auf Anfrage.

Bei den Anbietern, die ihre Leistung aus einer EU-Region erbringen, findet die Verarbeitung dort statt; die Konzernzugehörigkeit zu einem Unternehmen mit Sitz in den Vereinigten Staaten ändert daran nichts. Der einzige Dienstleister, bei dem die Verarbeitung selbst in einem Drittland stattfindet, ist der in 3.1 genannte Anbieter für mobile Benachrichtigungen.

3.4 Nicht aufgeführt

Nicht aufgeführt sind Dienste, die keine dem Auftrag anvertrauten Daten erhalten. Das sind:

- das interne Betriebsmonitoring, das ausschließlich aggregierte Zählwerte

ohne Personenbezug übermittelt;

- die Reichweitenmessung der öffentlichen Website und der

Registrierungsstrecke. Sie wird vom Auftragnehmer selbst betrieben, die Messwerte verbleiben in der Anwendung, und IP-Adressen werden ausschließlich gekürzt gespeichert;

- Analyse- und Werbedienste der Google LLC auf der öffentlichen Website.

Sie werden erst nach Einwilligung des Websitebesuchers geladen, betreffen nicht den angemeldeten Bereich und erhalten keine Daten aus dem Konto des Auftraggebers. Einzelheiten stehen in der Datenschutzerklärung des Auftragnehmers.

Dieser Vertrag wurde elektronisch geschlossen. Fassung, Zeitpunkt, handelnde Person und Prüfsumme sind im Kundenbereich unter „Einstellungen -> Auftragsverarbeitung" abrufbar.