Vereinbarung zur Auftragsverarbeitung (AVV) gemäß Art. 28 DSGVO

Geltungsbereich & Abschluss

Diese Vereinbarung zur Auftragsverarbeitung („AVV“) ist integraler Bestandteil der Allgemeinen Geschäftsbedingungen (AGB) bzw. des Servicevertrags zwischen dem **Kunden** (nachfolgend **„Verantwortlicher**“) und der **GOBERU SOLUTIONS UG (haftungsbeschränkt)** (nachfolgend **„Auftragsverarbeiter**“). Der „Kunde“ im Sinne der AGB ist zugleich der „Verantwortliche“ im Sinne dieser AVV; der „Anbieter“ im Sinne der AGB ist zugleich der „Auftragsverarbeiter“.

Die AVV kommt mit Abschluss des Hauptvertrags (z. B. durch digitale Registrierung, Buchung eines Abonnements oder Nutzung der Software) in elektronischer Form zustande. Einer gesonderten Unterzeichnung bedarf es nicht.

Maßgeblich ist die dem Verantwortlichen bei Vertragsschluss bereitgestellte Fassung dieser AVV (Version/Datum). Der Verantwortliche kann diese Fassung in dauerhaft speicherbarer Form herunterladen. Ein Abruf einer „aktuellen Fassung“ über die Website dient ausschließlich der Information; Änderungen dieser AVV erfolgen ausschließlich nach Maßgabe der Änderungsregelungen dieser AVV und der AGB.

§ 1 Gegenstand und Dauer

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen. Gegenstand ist die Bereitstellung, der Betrieb und der Support der SaaS-Plattform „Autaxo“ (Dealer-Management-System) zur Digitalisierung des Fahrzeughandels.

(2) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags (Abonnement). Sie endet automatisch mit dessen Beendigung, vorbehaltlich etwaiger vertraglicher oder gesetzlicher Nachwirkungspflichten (z. B. Datenexport, Löschung).

§ 2 Art und Zweck der Verarbeitung

(1) Die Verarbeitung dient ausschließlich der Erfüllung der Leistungen aus dem Hauptvertrag. Hierzu gehören insbesondere:

- Digitale Verwaltung von Fahrzeugbeständen, Kunden, Lieferanten und Verträgen.
- Abwicklung von An- und Verkaufsprozessen (inkl. automatisierter Steuerlogiken).
- Erstellung, Versand und Archivierung von Belegen (Rechnungen, Gutschriften).
- Technische Validierung von Daten via Schnittstellen (z. B. Adressen, Fahrzeugdaten via VIN).

- Hosting, Backup-Management, Wartung und technischer Support.

(2) Folgende Datenarten sind Gegenstand der Verarbeitung:

- **Stammdaten:** Namen, Anschriften, Kontaktdaten (E-Mail, Telefon), Firmennamen, USt-ID.
- **Fahrzeugdaten:** Fahrzeug-Identifizierungsnummern (FIN/VIN), Kennzeichen, Fahrzeugmerkmale (soweit personenbeziehbar).
- **Transaktionsdaten:** Kaufpreise, Bankverbindungen, Vertragsinhalte, Steuerdaten, Rechnungsdaten.
- **Dokumentendaten:** Uploads (z. B. Zulassungsbescheinigungen, Ausweiskopien, Verträge).
- **Nutzungsdaten:** Systemprotokolle (Logs), Login-Historie, User-IDs, Metadaten der API-Nutzung.

(3) Der Kreis der betroffenen Personen umfasst:

- Kunden und Interessenten des Verantwortlichen (Käufer/Verkäufer/Fahrzeughalter).
- Mitarbeiter und Benutzer des Verantwortlichen.
- Lieferanten und Geschäftspartner des Verantwortlichen.

(4) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO ist mit der Plattform grundsätzlich nicht vorgesehen. Der Verantwortliche stellt durch geeignete organisatorische Maßnahmen sicher, dass solche Daten nicht in die Plattform eingegeben oder hochgeladen werden. Soweit der Verantwortliche ausnahmsweise besondere Kategorien personenbezogener Daten verarbeiten möchte (z.B. durch Upload entsprechender Dokumente), bedarf dies einer vorherigen Abstimmung in Textform und ggf. einer Ergänzung dieser AVV (einschließlich angepasster technischer und organisatorischer Maßnahmen). Erfolgt keine Abstimmung, ist der Auftragsverarbeiter berechtigt, solche Inhalte zu sperren oder zu löschen, soweit dies zur Einhaltung datenschutzrechtlicher Pflichten erforderlich ist.

§ 3 Weisungsbefugnis

(1) Der Auftragsverarbeiter verarbeitet die Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach den dokumentierten Weisungen des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO).

(2) Weisungen werden primär durch die **Konfiguration und Nutzung der Softwarefunktionen** durch den Verantwortlichen erteilt (z. B. Anlegen, Ändern, Löschen oder Exportieren von Datensätzen). Einzelweisungen, die über die Standardfunktionen hinausgehen, bedürfen der Textform (z. B. via Ticket-System oder E-Mail).

(3) Weisungen, die über die im Rahmen der Plattform bereitgestellten Standardfunktionen hinausgehen oder zusätzliche Mitwirkungsleistungen des Auftragsverarbeiters erfordern (z. B. Sonderauswertungen, individuelle Datenmigrationen, besondere Exportformate),

werden vom Auftragsverarbeiter im Rahmen des rechtlich Zulässigen und Zumutbaren umgesetzt; soweit hierdurch ein zusätzlicher, nicht vom Standard-Leistungsumfang erfasster Aufwand entsteht, kann der Auftragsverarbeiter hierfür eine angemessene Vergütung bzw. Aufwandsentschädigung verlangen. Gesetzliche Unterstützungs- und Mitwirkungspflichten bleiben unberührt.

(4) Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich. Er darf die Ausführung aussetzen, bis die Weisung bestätigt oder geändert wurde.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verpflichtet alle mit der Verarbeitung betrauten Personen (Mitarbeiter und Subunternehmer) schriftlich auf die Vertraulichkeit.

(2) Der Auftragsverarbeiter gewährleistet durch geeignete technische und organisatorische Maßnahmen ein angemessenes Schutzniveau. Die Maßnahmen sind in **Anlage 1** detailliert beschrieben. Der Auftragsverarbeiter darf die Maßnahmen der technischen Entwicklung anpassen, solange das Sicherheitsniveau nicht unterschritten wird.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Möglichkeiten und – sofern nicht im Standard-Service enthalten – gegen angemessene Vergütung bei:

- der Erfüllung von Betroffenenrechten (Export, Löschung via Software-Funktion),
- der Meldung von Datenschutzverletzungen (Art. 33, 34 DSGVO),
- Datenschutz-Folgenabschätzungen (Art. 35 DSGVO).

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er eine Verletzung des Schutzes personenbezogener Daten feststellt.

(5) Der Auftragsverarbeiter erteilt betroffenen Personen keine eigenen Auskünfte und nimmt keine eigenen Erklärungen vor, sondern verweist diese grundsätzlich an den Verantwortlichen. Etwas anderes gilt nur, wenn der Verantwortliche den Auftragsverarbeiter hierzu im Einzelfall in Textform angewiesen hat oder eine gesetzliche Verpflichtung des Auftragsverarbeiters besteht.

§ 5 Unterauftragsverarbeiter

(1) Der Verantwortliche genehmigt den Einsatz der in **Anlage 2** aufgeführten Unterauftragsverarbeiter.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über geplante Änderungen (Hinzuziehung oder Ersetzung) rechtzeitig (z. B. per E-Mail oder System-Benachrichtigung). Der Verantwortliche kann innerhalb von 14 Tagen aus

wichtigem datenschutzrechtlichem Grund widersprechen. Erfolgt ein Widerspruch, werden die Parteien prüfen, ob die Leistungen ohne den betreffenden Unterauftragsverarbeiter fortgeführt werden können. Ist dies nicht möglich, steht beiden Parteien ein Sonderkündigungsrecht zu. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt.

(3) Der Auftragsverarbeiter stellt durch den Abschluss geeigneter Vereinbarungen (z. B. Auftragsverarbeitungsverträge, Data Processing Terms, Standardvertragsklauseln) sicher, dass Unterauftragsverarbeiter die Anforderungen der DSGVO erfüllen. Den Unterauftragsverarbeitern werden dabei mindestens die gleichen Datenschutzpflichten auferlegt, wie sie sich aus dieser AVV ergeben, insbesondere hinsichtlich Vertraulichkeit, Sicherheit der Verarbeitung, Unterstützungspflichten und Löschung/Rückgabe. Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für die Erfüllung der Pflichten der Unterauftragsverarbeiter verantwortlich.

§ 6 Datenverarbeitung in Drittländern

(1) Die Verarbeitung erfolgt primär innerhalb der EU/EWR. Soweit der Auftragsverarbeiter oder ein Unterauftragsverarbeiter personenbezogene Daten in ein Drittland übermittelt oder dort verarbeitet, erfolgt dies ausschließlich unter Einhaltung der Art. 44 ff. DSGVO.

(2) Als geeignete Garantien kommen insbesondere in Betracht: (i) Angemessenheitsbeschluss der EU-Kommission (z.B. EU-US Data Privacy Framework, soweit anwendbar), und/oder (ii) EU-Standardvertragsklauseln (SCC) einschließlich ggf. erforderlicher zusätzlicher Maßnahmen. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage die relevanten Informationen zur Absicherung zur Verfügung.

(3) Datenflüsse, Länder und Unterauftragsverarbeiter mit Drittlandbezug werden transparent in Anlage 2 benannt bzw. nach dem Verfahren in § 5 Abs. 2 aktualisiert.

§ 7 Kontrollrechte (Audits)

(1) Der Verantwortliche hat das Recht, die Einhaltung dieser Vereinbarung zu überprüfen.

(2) Der Nachweis der Konformität erfolgt primär durch Vorlage geeigneter, verfügbarer Dokumentationen und Nachweise (z. B. Sicherheits- und Datenschutzkonzepte, TOM-Dokumentation, Audit-/Prüfberichte oder Zertifizierungen von eingesetzten Infrastruktur-/Rechenzentrumsbetreibern, soweit vorhanden) sowie durch Remote-Audits.

(3) Vor-Ort-Kontrollen (einschließlich Inspektionen) sind zulässig, wenn (a) die Prüfung nach Abs. 2 keinen hinreichenden Nachweis liefert oder (b) ein begründeter Anlass besteht (z. B. erheblicher Datenschutzvorfall, konkrete Sicherheitsmängel, wesentliche Änderungen der Verarbeitung oder der Unterauftragsverarbeiter-Kette). Die Parteien führen Prüfungen vorrangig als Remote-Audit (z. B. Videokonferenz, Screensharing,

Dokumentenprüfung) durch, um Eingriffe in Betriebsabläufe zu minimieren. Vor-Ort-Kontrollen sind mindestens 4 Wochen vorher anzukündigen, dürfen den Geschäftsbetrieb nicht unzumutbar stören und erfolgen unter angemessenen Vertraulichkeits- und Sicherheitsvorkehrungen. Vor-Ort-Kontrollen finden grundsätzlich höchstens einmal jährlich statt, sofern kein begründeter Anlass für häufigere Prüfungen besteht. Die Kosten trägt der Verantwortliche, sofern kein Verstoß des Auftragsverarbeiters festgestellt wird.

§ 8 Löschung und Rückgabe

(1) Nach Beendigung der Verarbeitung im Auftrag des Verantwortlichen wird der Auftragsverarbeiter – nach Wahl des Verantwortlichen – die personenbezogenen Daten löschen oder dem Verantwortlichen zurückgeben, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

(2) Soweit der Verantwortliche die Rückgabe wünscht, kann er innerhalb von dreißig (30) Tagen nach Vertragsende einmalig die Herausgabe der personenbezogenen Daten in einem gängigen maschinenlesbaren Format anfordern.

(3) Nach Ablauf der Frist gemäß Abs. 2 löscht der Auftragsverarbeiter die personenbezogenen Daten, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Näheres zu Löschfristen für aktive Kopien und Sicherungsmedien ergibt sich aus Anlage 1 (TOM) bzw. den dort beschriebenen Lösch- und Backup-Routinen.

§ 9 Haftung

Die Haftung der Parteien richtet sich nach den Haftungsbestimmungen des Hauptvertrags (**§ 12 der AGB**). Die unmittelbare Haftung gegenüber Betroffenen nach Art. 82 DSGVO bleibt hiervon unberührt.

§ 10 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Anlage bedürfen der Textform.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Anstelle der unwirksamen Bestimmung gelten die gesetzlichen Vorschriften.

(3) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist der im Hauptvertrag vereinbarte Sitz (Essen, gemäß § 16 AGB).

(4) Änderungen dieser AVV sind nur aus sachlichen Gründen zulässig (z.B. Änderungen der Gesetzeslage/Rechtsprechung, Anpassungen an Sicherheitsanforderungen, Änderungen im Subprozessor-Setup) und dürfen das Schutzniveau für personenbezogene Daten nicht wesentlich absenken. Der Auftragsverarbeiter informiert

den Verantwortlichen mindestens vier (4) Wochen vor Inkrafttreten in Textform. Der Verantwortliche kann innerhalb von zwei (2) Wochen ab Zugang in Textform widersprechen. Im Falle des Widerspruchs gelten die bisherigen Regelungen fort; können die Parteien keine zumutbare Lösung finden, steht beiden Parteien ein Sonderkündigungsrecht zum Zeitpunkt des beabsichtigten Inkrafttretens zu. Textform im Sinne dieser AVV umfasst auch elektronische Erklärungen (z.B. E-Mail oder In-App-Bestätigung).

Anlage 1: Technische und organisatorische Maßnahmen (TOMs)

gemäß Art. 32 DSGVO

Stand: 29.12.2025

Der Auftragsverarbeiter setzt die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen ein, um ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten sicherzustellen (Art. 32 DSGVO). Die Maßnahmen orientieren sich an den Risiken der Verarbeitung (insb. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit). Der Auftragsverarbeiter kann diese Maßnahmen weiterentwickeln oder anpassen, sofern das insgesamt erreichte Schutzniveau nicht wesentlich unterschritten wird.

Die Plattform wird in einer Cloud-Infrastruktur betrieben (z. B. Google Cloud Platform). Physische Rechenzentrums-Sicherheitsmaßnahmen werden überwiegend durch den jeweiligen Cloud-Anbieter erbracht; der Auftragsverarbeiter ergänzt dies durch eigene organisatorische und technische Kontrollen auf System-, Netzwerk- und Anwendungsebene.

1. Maßnahmen zur Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Zutrittskontrolle (Physisch):**
  - *Maßnahme:* Schutz der Infrastruktur vor unbefugtem Zutritt.
  - *Umsetzung:* Betrieb der Plattform in Rechenzentren von Cloud-Dienstleistern mit branchenüblichen Zutrittsbeschränkungen und Sicherheitsmaßnahmen (z. B. Zugangskontrollen, Besucher-/Berechtigungsmanagement, Überwachung nach Standard des jeweiligen Rechenzentrumsbetreibers).
- **Zugangskontrolle (Systemebene):**
  - *Maßnahme:* Verhinderung unbefugter Systemnutzung.
  - *Umsetzung: Zugriff auf Systeme und Administrationsoberflächen erfolgt nur nach Authentifizierung und Berechtigung. Es werden individualisierte Konten genutzt; Berechtigungen werden nach dem Erforderlichkeitsprinzip vergeben. Es gelten angemessene Anforderungen an Authentifizierungsverfahren (z. B. Passwort-Richtlinien) sowie zusätzliche Schutzmaßnahmen für administrative Zugänge, soweit technisch verfügbar und angemessen.*

- **Zugriffskontrolle (Datenzugriff):**
  - *Maßnahme:* Sicherstellen, dass Nutzer nur auf Daten des jeweiligen Kunden zugreifen können.
  - *Umsetzung: Mandanten-/Kundentrennung in der Anwendung (logische Trennung). Innerhalb eines Kundenaccounts können alle autorisierten Nutzer derzeit die gleichen Berechtigungen besitzen. Der Auftragsverarbeiter behält sich vor, rollenbasierte Berechtigungen künftig einzuführen. Nutzerkonten können durch den Verantwortlichen verwaltet und bei Bedarf deaktiviert werden.*
- **Weitergabekontrolle (Übertragung/Transport):**
  - *Maßnahme:* Schutz personenbezogener Daten bei Übertragung.
  - *Umsetzung:* Verschlüsselte Übertragung (z. B. TLS) für Web-Zugriffe und Schnittstellen; Einschränkung und Absicherung von Integrationen nach dokumentierten Schnittstellen; soweit eingesetzt: angemessene Schlüssel-/Zugriffsverwaltung

2. Maßnahmen zur Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- **Eingabekontrolle:**
  - *Maßnahme:* Nachvollziehbarkeit wesentlicher Verarbeitungsvorgänge.
  - *Umsetzung:* Protokollierung wesentlicher sicherheits- bzw. nachvollziehbarkeitsrelevanter Ereignisse (z. B. Anmeldungen, Berechtigungsänderungen, zentrale Datenänderungen), soweit technisch angemessen und zur Sicherheits-/Nachvollziehbarkeitsanforderung erforderlich.
- **Auftragskontrolle:**
  - *Maßnahme:* Verarbeitung personenbezogener Daten ausschließlich entsprechend den Weisungen des Verantwortlichen.
  - *Umsetzung:* Weisungs- und Berechtigungskonzepte; Zugriff durch Mitarbeitende des Auftragsverarbeiters erfolgt nur, soweit dies zur Support-/Fehleranalyse oder zur Sicherstellung des Betriebs erforderlich ist, und unter Beachtung von Vertraulichkeit und Berechtigungsprinzipien.
- **Verfügbarkeitskontrolle (Ausfallsicherheit/Backup):**
  - *Maßnahme:* Schutz gegen zufällige Zerstörung oder Verlust.
  - *Umsetzung:* Einsatz technischer Maßnahmen zur Stabilität und Verfügbarkeit der Systeme (z. B. Monitoring/Alerting, Redundanzen nach technischem Betriebsbedarf). Datenbestände werden durch automatisierte Sicherungsmechanismen abgesichert; Sicherungen werden im Rahmen einer regelmäßigen Rotation vorgehalten und überschrieben. Wiederherstellungsprozesse werden nach Bedarf geprüft.

3. Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- **Verfügbarkeitskontrolle & Backups:**
  - *Maßnahme:* Schutz vor Verlust, Zerstörung und längerfristiger Nichtverfügbarkeit personenbezogener Daten.

    - *Umsetzung: Der Auftragsverarbeiter nutzt technische und organisatorische Maßnahmen zur Sicherstellung der Betriebsfähigkeit (z. B. Monitoring/Alerting, Kapazitäts- und Störungsmanagement, Redundanzen nach technischem Betriebsbedarf). Datenbestände werden durch automatisierte Sicherungsmechanismen abgesichert. Sicherungen werden im Rahmen einer Rotation vorgehalten und überschrieben; Umfang und Aufbewahrung richten sich nach technischem Betriebsbedarf und Sicherheitsanforderungen. Soweit technisch vorgesehen, werden Sicherungen getrennt vom Primärsystem gespeichert.*
- **Wiederherstellbarkeit (Recovery):**
    - *Maßnahme:* Wiederherstellung von Daten und Systemfunktionen nach Störungen/Vorfällen..
    - *Umsetzung: Der Auftragsverarbeiter hält Prozesse zur Wiederherstellung vor und verfolgt hierfür interne Zielwerte, die sich nach Art, Ursache und Umfang des Vorfalls sowie den technischen Rahmenbedingungen richten. Wiederherstellungsmaßnahmen (z. B. Wiederanlauf-/Restore-Prozesse) werden anlassbezogen sowie in angemessenen Abständen überprüft. Interne Zielwerte stellen keine garantierten Wiederherstellungszusagen im Einzelfall dar*

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- *Maßnahme:* Evaluierung und Verbesserung der Wirksamkeit der TOMs.
- *Umsetzung: Die TOMs werden regelmäßig sowie anlassbezogen (z. B. bei wesentlichen Änderungen der Verarbeitung, Sicherheitsereignissen oder relevanten technischen Änderungen) überprüft und bei Bedarf angepasst. Der Auftragsverarbeiter führt geeignete Sicherheitsprüfungen im angemessenen Umfang durch (z. B. Überprüfungen bekannter Schwachstellen, Konfigurations-/Abhängigkeitsprüfungen) und unterhält einen Prozess zum Umgang mit Sicherheitsvorfällen (Incident-Management), einschließlich Bewertung, Eindämmung und Dokumentation.*

Anlage 2: Liste der Unterauftragsverarbeiter (Stand: 29.12.25)

Der Verantwortliche genehmigt den Einsatz folgender Unterauftragsverarbeiter. Diese Liste ist zum Standdatum abschließend. Weitere Unterauftragsverarbeiter werden nur nach dem Verfahren gemäß § 5 Abs. 2 AVV hinzugefügt.

Firma	Sitz / Land	Leistung / Funktion	Verarbeitungsort(e)
Google Cloud EMEA Ltd.	Dublin, Irland (EU)	**Hosting der Plattform** (Compute, Storage, Datenbanken), Logging/Monitoring sowie optionale KI-Funktionen (z. B.	**Deutschland**/EU (Data Center Region europe-west3, Frankfurt am Main)

		Vertex AI / Gemini) in der Region europe-west3 (Frankfurt/Main).	
Google Ireland Ltd.	Dublin, Irland (EU)	**E-Mail-/Kollaborationstools für Support- und Organisationskommunikation** (z. B. kontakt@autaxo.de; Kommunikation mit dem Verantwortlichen, Support-Anfragen)	EU, Verarbeitung nach Google Workspace Data Processing Amendment; Drittlandzugriffe/-übermittlungen können je nach Support-/Betriebsmodell nicht ausgeschlossen sein und erfolgen dann auf Grundlage geeigneter Garantien (z. B. SCC).
VINCARIO s.r.o.	Ostrava, Tschechien (EU)	API zur **Fahrzeugdaten-Anreicherung** (VIN Decoding).	EU
Sinch Email (Mailjet / Mailgun) Mailgun Technologies, Inc. 112 E Pecan St. #1135 San Antonio, TX 78205, USA (Mutterkonzern: Sinch AB, Stockholm)	**Primär**: EU (Frankfurt / Belgien) **Sekundär**: USA (Zugriff Support / Tech-Ops)	**E-Mail-Versanddienst** (Transactional E-Mails) für Autaxo **Transfergrundlage:** EU-U.S. Data Privacy Framework (DPF) (Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 DSGVO)	**Primär**: EU (Frankfurt / Belgien) **Sekundär**: USA (Zugriff Support / Tech-Ops)
The Constant Company, LLC *(**Unterauftragsverarbeiter in der Unterauftragskette von VINCARIO; Vertragspartner ist VINCARIO.**)*	USA	Infrastruktur/Hosting-Dienstleistungen im Rahmen der VINCARIO-Leistungserbringung	USA; Transfergrundlage: **EU-SCC** (ggf. zusätzliche Maßnahmen) – **Vertragspartner ist VINCARIO**, nicht Autaxo

Hinweis zu Dritt-Schnittstellen (eigenständige Verantwortliche / nicht Unterauftragsverarbeitung):

Dienste, die als eigenständige Verantwortliche agieren, gelten nicht als

Unterauftragsverarbeitung im Sinne dieser AVV. Dazu können insbesondere gehören: Zahlungsdienstleister (z. B. Stripe Payments Europe, Ltd.), Behörden-Schnittstellen (z. B. VIES/ELSTER) sowie Fahrzeugbörsen (z. B. mobile.de), soweit der Kunde diese Integrationen nutzt.