



Vereinbarung zur Auftragsverarbeitung

nach Art. 28 Datenschutz-Grundverordnung (DSGVO)
einschließlich Anlage zu den technischen und organisatorischen Maßnahmen nach Art. 32
DSGVO

Vertragsmuster: Dieses Dokument wird erst durch Unterzeichnung oder eine nachweisbare Einbeziehung in den Hauptvertrag wirksam. Vor dem ersten Einsatz mit Kunden wird eine anwaltliche Prüfung empfohlen.

zwischen

- nachfolgend Auftraggeber oder Verantwortlicher -

und

Smart Car Logistik UG (haftungsbeschränkt)
Geschäftsführer: Sebastian Steinke
Karlstraße 29, 44532 Lünen
Ansprechpartner: Noel Roggenkämper und Sebastian Steinke
Telefon: +49 173 8557303 | E-Mail: info@flottenwacht.de
Amtsgericht Dortmund, HRB 32483 | USt-IdNr. DE338748343
- nachfolgend Auftragnehmer oder Auftragsverarbeiter -
Flottenwacht ist ein Angebot der Smart Car Logistik UG (haftungsbeschränkt).



1. Gegenstand und Dauer

1.1 Der Auftragnehmer stellt dem Auftraggeber die im Hauptvertrag vereinbarten Flottenwacht-Leistungen zur Verfügung. Dazu können insbesondere Portalbetrieb, Benutzerverwaltung, Fahrzeug- und Fahrerakten, Fristen- und Aufgabenverwaltung, Dokumentenspeicherung, Kosten- und Vertragsdaten, Übergaben, Erinnerungen, Berichte sowie vereinbarte Support- und Verwaltungsleistungen gehören.

1.2 Diese Vereinbarung gilt für alle Verarbeitungsvorgänge, bei denen der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Sie beginnt mit Wirksamwerden des Hauptvertrags oder der erstmaligen Verarbeitung und endet, wenn alle Auftragsdaten vertragsgemäß zurückgegeben oder gelöscht wurden.

1.3 Art, Umfang und Dauer der Verarbeitung richten sich nach dem Hauptvertrag, dem gebuchten Leistungsumfang, dokumentierten Weisungen und dieser Vereinbarung.

2. Rollen und Weisungen

2.1 Der Auftraggeber ist für die Rechtmäßigkeit der Erhebung und Verarbeitung der Auftragsdaten, die Wahrung der Rechte betroffener Personen und die Erteilung zulässiger Weisungen verantwortlich.

2.2 Der Auftragnehmer verarbeitet Auftragsdaten ausschließlich auf dokumentierte Weisung des Auftraggebers, soweit keine gesetzliche Verpflichtung zur Verarbeitung besteht. Der Hauptvertrag, diese Vereinbarung, freigegebene Portalaktionen und in Textform erteilte Einzelweisungen gelten als dokumentierte Weisungen.

2.3 Hält der Auftragnehmer eine Weisung für datenschutzrechtswidrig, weist er den Auftraggeber unverzüglich darauf hin. Er darf die Ausführung bis zur Bestätigung oder Änderung der Weisung aussetzen.

2.4 Verarbeitungen, bei denen der Auftragnehmer eigene Zwecke und Mittel festlegt - insbesondere eigene Vertrags-, Abrechnungs-, Sicherheits- und Missbrauchspräventionsdaten - fallen nicht unter diese Auftragsverarbeitung. Für Full-Service-Leistungen ist die Rollenverteilung je Tätigkeit im Hauptvertrag festzulegen.

3. Pflichten des Auftragnehmers

- Verarbeitung ausschließlich innerhalb des vereinbarten Leistungsumfangs und nach dokumentierten Weisungen.
- Verpflichtung aller zugriffsberechtigten Personen auf Vertraulichkeit.
- Umsetzung und fortlaufende Überprüfung angemessener technischer und organisatorischer Maßnahmen.
- Unterstützung des Auftraggebers bei Betroffenenrechten, Datenschutz-Folgenabschätzungen, Konsultationen und Nachweisen, soweit die Art der Verarbeitung dies ermöglicht.
- Unverzügliche Information über bekannt gewordene Verletzungen des Schutzes personenbezogener Daten; die Meldung enthält die verfügbaren Angaben zu Art, Umfang, Folgen und Abhilfemaßnahmen.
- Führung der erforderlichen Verzeichnisse und Bereitstellung angemessener Informationen zum Nachweis der Einhaltung dieser Vereinbarung.

4. Rechte betroffener Personen

4.1 Erhält der Auftragnehmer eine Anfrage einer betroffenen Person zu Auftragsdaten, leitet er sie - soweit eine Zuordnung möglich ist - an den Auftraggeber weiter und beantwortet sie nicht eigenständig, sofern keine gesetzliche Verpflichtung besteht.



4.2 Der Auftragnehmer unterstützt den Auftraggeber durch vorhandene Portal-, Export-, Berichtigungs- und Löschfunktionen sowie angemessene technische Mitwirkung. Zusätzlicher, nicht vom Leistungsumfang erfasster Aufwand kann nach vorheriger Abstimmung vergütet werden.

5. Unterauftragsverarbeiter

5.1 Der Auftraggeber erteilt eine allgemeine Genehmigung zum Einsatz der nachfolgend aufgeführten Unterauftragsverarbeiter. Der Auftragnehmer informiert über beabsichtigte wesentliche Änderungen. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Tagen widersprechen.

Dienstleister	Leistung / Daten	Ort / Transfergrundlage
Hetzner Online GmbH	Serverhosting, Infrastruktur und technische Betriebsdaten	Deutschland / EU
Supabase Pte. Ltd. und eingesetzte Unterauftragnehmer	Authentifizierung, Datenbank, Dateispeicherung und technische Protokolle	Produktivdaten in gewählter EU-Region; mögliche Drittlandverarbeitung nach Anbieter-DPA
Plus Five Five, Inc. (Resend)	E-Mail-Versand, Empfänger-, Inhalts-, Versand- und Protokolldaten	USA; EU-US Data Privacy Framework und Standardvertragsklauseln nach Anbieter-DPA
Cloudflare, Inc.	Turnstile, Bot- und Missbrauchsschutz; IP-, Browser-, Geräte- und Prüfdaten	USA / global; EU-US Data Privacy Framework und Standardvertragsklauseln nach Anbieter-DPA

5.2 Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich zu einem dieser Vereinbarung entsprechenden Datenschutzniveau. Die jeweils aktuellen Anbieterlisten und Transfermechanismen sind regelmäßig zu prüfen und zu dokumentieren.

6. Kontrollrechte und Nachweise

6.1 Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die zur Kontrolle erforderlichen Informationen zur Verfügung. Geeignete Zertifikate, Prüfberichte, Sicherheitsbeschreibungen und Anbieter-Dokumentationen können vorrangig als Nachweis verwendet werden.

6.2 Weitergehende Prüfungen sind rechtzeitig anzukündigen, auf den erforderlichen Umfang zu begrenzen und so durchzuführen, dass Geschäftsgeheimnisse, Sicherheit und Rechte anderer Kunden gewahrt bleiben. Unverhältnismäßiger Zusatzaufwand kann nach vorheriger Vereinbarung vergütet werden.

7. Rückgabe und Löschung

7.1 Nach Vertragsende erhält der Auftraggeber für 30 Tage die Möglichkeit eines vereinbarten Datenexports, soweit keine abweichende Regelung getroffen wurde.

7.2 Nach Ablauf des Exportzeitraums löscht oder anonymisiert der Auftragnehmer die Auftragsdaten nach Weisung und entsprechend dem dokumentierten Löschkonzept, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Gesetzlich aufzubewahrende Daten werden für andere Zwecke gesperrt.

7.3 Sicherungskopien werden im Rahmen der technisch festgelegten Backup-Zyklen überschrieben oder gelöscht. Konkrete Fristen ergeben sich aus dem jeweils gültigen Löschkonzept.



8. Schlussbestimmungen

8.1 Im Übrigen gelten Hauptvertrag und wirksam einbezogene B2B-AGB. Bei Widersprüchen gehen datenschutzrechtlich zwingende Regelungen und diese Vereinbarung für die Auftragsverarbeitung vor.

8.2 Änderungen und Ergänzungen einschließlich Weisungen bedürfen mindestens der Textform, soweit keine strengere Form gesetzlich vorgeschrieben ist.

Anlage 1 - Beschreibung der Verarbeitung

Merkmal	Beschreibung
Gegenstand	Technische Bereitstellung und vereinbarte Unterstützung beim digitalen Fuhrpark-, Fahrer-, Dokument-, Aufgaben-, Kosten-, Übergabe- und gegebenenfalls Vermietungsmanagement.
Zwecke	Verwaltung, Organisation, Dokumentation, Fristensteuerung, Kommunikation, Berichterstellung, Support und Sicherheit entsprechend den Weisungen des Auftraggebers.
Verarbeitungsvorgänge	Erheben, Erfassen, Ordnen, Speichern, Abrufen, Anzeigen, Abgleichen, Übermitteln an angewiesene Empfänger, Einschränken, Exportieren, Löschen und Protokollieren.
Betroffene Personen	Beschäftigte, Fahrer, Ansprechpartner, Benutzer, Bewerber oder Aushilfen, Kunden und Mietkunden des Auftraggebers, externe Dienstleister sowie sonstige vom Auftraggeber erfasste Personen.
Datenarten	Stamm- und Kontaktdaten; Benutzer- und Berechtigungsdaten; Fahrer-, Führerschein-, Kontroll- und Unterweisungsdaten; Fahrzeug-, Standort-, Werkstatt-, Schaden-, Vertrags-, Kosten- und Dokumentdaten; Aufgaben, Fristen, Übergaben und Notizen; Kommunikations-, Versand-, Nutzungs- und Sicherheitsprotokolle.
Besondere Kategorien	Nicht vorgesehen. Der Auftraggeber darf besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO nur nach vorheriger schriftlicher Vereinbarung und bei geeigneter Rechtsgrundlage einstellen.
Dauer	Laufzeit des Hauptvertrags zuzüglich Export-, Lösch- und gesetzlicher Aufbewahrungszeiträume.



Anlage 2 - Technische und organisatorische Maßnahmen

Die Maßnahmen werden unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie von Art, Umfang, Umständen, Zwecken und Risiken regelmäßig überprüft und bei Bedarf angepasst. Gleichwertige oder stärkere Maßnahmen können einzelne Maßnahmen ersetzen.

1. Organisation und Datenschutzmanagement

- Festgelegte Verantwortlichkeiten für Betrieb, Berechtigungen, Support und Datenschutz.
- Vertraulichkeitsverpflichtung und bedarfsgerechte Berechtigungen für zugriffsberechtigte Personen.
- Dokumentierte Prozesse für Benutzeranlage, Rollenwechsel, Sperrung und Entzug von Berechtigungen.
- Regelmäßige Prüfung von Dienstleistern, Verträgen, Unterauftragsverarbeitern und Sicherheitsmaßnahmen.

2. Zutritts- und physische Sicherheit

- Produktivsysteme werden in professionellen Rechenzentren der eingesetzten Infrastrukturprovider betrieben.
- Physische Zutrittskontrollen, Energie-, Brand- und Umgebungsschutz werden durch die Rechenzentrumsanbieter umgesetzt und nach deren Nachweisen kontrolliert.

3. Zugangskontrolle

- Personenbezogene Benutzerkonten; gemeinsame Administrationskonten sollen vermieden werden.
- Mehrfaktor-Authentifizierung für privilegierte Rollen; sichere Passwort- und Wiederherstellungsprozesse.
- Cloudflare Turnstile und serverseitige Prüfungen gegen automatisierte oder missbräuchliche Anmeldeversuche.
- Produktive Sitzungen werden im Browser nicht bewusst dauerhaft gespeichert; Sitzungsbeendigung und Passwortänderung sind vorgesehen.
- TLS-verschlüsselte Übertragung; Sicherheitsheader und HSTS für entsprechend konfigurierte Domains.

4. Zugriffskontrolle und Mandantentrennung

- Rollen- und Berechtigungskonzept für Inhaber, Verwaltung, Sachbearbeitung, Kundenadministratoren und Kundenmitarbeiter.
- Mandantentrennung durch Row Level Security und kundengebundene Datenbankfunktionen/RPCs.
- Kunden dürfen nur auf den eigenen Mandanten und freigeschaltete Module zugreifen.
- Generische direkte Schreibrechte von Kunden auf zentrale Tabellen werden vermieden; kritische Aktionen werden serverseitig validiert.
- Dokumente liegen in privaten Speicherbereichen; Abrufe erfolgen über kurzlebige signierte URLs.
- Dateityp und Dateigröße werden für Uploads begrenzt; Berechtigungen gelten auch für Download und Vorschau.

5. Weitergabe- und Transportkontrolle

- Verschlüsselte Übertragung über HTTPS/TLS.



- E-Mail-Empfänger werden entsprechend der gewählten Versandregel gesteuert; bei mehreren Empfängern erfolgt der Versand getrennt, soweit vorgesehen.
- Exporte und Supportzugriffe erfolgen nur auf Weisung oder aufgrund dokumentierter Berechtigung.
- Drittlandübermittlungen werden über Angemessenheitsbeschlüsse, EU-US Data Privacy Framework oder Standardvertragsklauseln abgesichert, soweit einschlägig.

6. Eingabe-, Änderungs- und Löschkontrolle

- Relevante Änderungen und Löschungen werden in einem kundenbezogenen Protokoll bzw. Archiv dokumentiert, soweit die Funktion betroffen ist.
- Zeitstempel, Benutzerbezug und fachlicher Kontext werden entsprechend dem jeweiligen Modul gespeichert.
- Löschungen erfolgen nur über vorgesehene Funktionen und unter Beachtung von Aufbewahrungs- und Nachweispflichten.

7. Verfügbarkeit, Sicherung und Wiederherstellung

- Betrieb auf redundant ausgelegter Infrastruktur der eingesetzten Provider im Rahmen der gebuchten Dienste.
- Datensicherungen und Wiederherstellungsmechanismen entsprechend der produktiven Provider- und Systemkonfiguration.
- Überwachung wesentlicher Fehler, Prüfung von Datenbank- und Anwendungsänderungen sowie dokumentierte Wiederherstellung im Störfall.
- Regelmäßige Aktualisierung sicherheitsrelevanter Komponenten und zeitnahe Behandlung kritischer Schwachstellen.

8. Trennungsgebot und Zweckbindung

- Trennung öffentlicher Website, Kundenportal, Datenbankzugriff und administrativer Funktionen.
- Logische Trennung der Kundenmandanten und Rollen; produktive und testbezogene Datenbestände werden kenntlich gemacht.
- Verarbeitung von Kundendaten ausschließlich für vereinbarte Zwecke und Weisungen.



Ansprechpartner des Auftraggebers

Weisungsberechtigte Personen

Datenschutz-/Sicherheitskontakt des Auftragnehmers

Die Parteien bestätigen den Abschluss dieser Vereinbarung einschließlich ihrer Anlagen.

Hinweis zur Verwendung: Der Download allein schließt noch keinen AV-Vertrag. Die Vereinbarung muss vor Beginn der Auftragsverarbeitung nachweisbar mit dem jeweiligen Kunden abgeschlossen und zusammen mit dem Hauptvertrag sowie den aktuellen Unterauftragsverarbeiter-Informationen aufbewahrt werden.