Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO

Entwurf – alle Stellen in eckigen Klammern sind Platzhalter und vor dem Abschluss auszufuellen und anwaltlich zu pruefen.

Vertragsparteien

Dieser Vertrag wird geschlossen zwischen

[PLATZHALTER: Firma des Kunden, Anschrift, vertreten durch] – nachfolgend „Verantwortlicher“ –

und

[PLATZHALTER: Firmenname des Anbieters, Anschrift, vertreten durch] – nachfolgend „Auftragsverarbeiter“ –

gemeinsam „Parteien“. Er konkretisiert die Pflichten aus dem zugrunde liegenden Hauptvertrag über die Nutzung der Software Boxenplan (nachfolgend „Hauptvertrag“).

§ 1 Gegenstand, Dauer und Weisungsbindung

1. Gegenstand ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Verantwortlichen im Rahmen der Bereitstellung und des Betriebs der Software Boxenplan.
2. Die Laufzeit entspricht der Laufzeit des Hauptvertrags. Endet der Hauptvertrag, endet auch dieser Vertrag; die Pflichten zur Löschung und Rückgabe nach § 10 bleiben bestehen.
3. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats zur Verarbeitung verpflichtet; in diesem Fall teilt er dem Verantwortlichen die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.
4. Weisungen erfolgen in Textform. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Der Hauptvertrag samt Leistungsbeschreibung und die Einstellungen, die der Verantwortliche in der Software selbst vornimmt, gelten als Weisung.
5. Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen Datenschutzrecht verstößt, informiert er den Verantwortlichen unverzüglich. Er darf die Ausführung aussetzen, bis der Verantwortliche die Weisung bestätigt oder ändert.

§ 2 Art und Zweck der Verarbeitung, Datenarten, betroffene Personen

Art und Zweck

Erhebung, Speicherung, Ordnung, Auslesen, Verwendung, Übermittlung an das Endgerät der Beschäftigten, Einschränkung und Löschung personenbezogener Daten zum Zweck der internen Organisation des Autohauses: Dienstplanung, Urlaubsverwaltung, Aufgabenverteilung, Essensbestellung, Leihwagenverwaltung einschließlich Schadensdokumentation sowie Benachrichtigungen.

Arten der verarbeiteten Daten

- Stammdaten der Beschäftigten: Name, Rolle, Abteilung, persönlicher Zugangscode, Sitzungs-Token
- Dienst- und Abwesenheitsdaten: Diensteinteilung, erledigte Checklistenpunkte, Strafwochen, Urlaubsanträge mit Zeiträumen und Status
- Aufgabendaten: Aufgabentext, zugewiesene Person, Ersteller, Fälligkeit, Erledigungsstatus
- Bestelldaten: bestellte Artikel, Optionen, Sonderwünsche, Preis, Bezahlstatus

• Leihwagendaten: Fahrzeug- und Vertragsdaten sowie Kundendaten der Mieter (Name, Anschrift, Telefon, E-Mail, Auftragsnummer, Führerschein-/Ausweisprüfung als Ja/Nein), Übernahme- und Rücknahmedaten, Schadensbeschreibungen und Schadensfotos

• Technische Daten: Server-Protokolle, Push-Adressen (Endpoints) der Geräte

• [PLATZHALTER: weitere Datenarten, falls der Kunde zusätzliche Felder nutzt]

Kategorien betroffener Personen

• Beschäftigte des Verantwortlichen (einschließlich Auszubildender und Aushilfen)

• Kundinnen und Kunden des Verantwortlichen, die ein Leihfahrzeug übernehmen

• [PLATZHALTER: weitere Kategorien, z. B. Leiharbeitnehmer]

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Gegenstand des Auftrags. Der Verantwortliche stellt sicher, dass solche Daten nicht in Freitextfelder eingegeben werden.

§ 3 Rechte und Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen allein verantwortlich.

2. Er erteilt alle Weisungen und benennt eine weisungsberechtigte Ansprechperson: [PLATZHALTER: Name, Funktion, Kontaktdaten].

3. Er informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Auftragsverarbeitung feststellt.

4. Er prüft eigenverantwortlich, ob Beteiligungsrechte einer Arbeitnehmervertretung bestehen, und holt erforderliche Zustimmungen ein.

5. Er ist berechtigt, sich vor Beginn und danach regelmäßig von der Einhaltung der getroffenen Maßnahmen zu überzeugen (§ 8).

§ 4 Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verarbeitet die Daten ausschließlich im Rahmen des Auftrags und der Weisungen (§ 1). Kopien oder Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt; ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

2. Er stellt sicher, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, und dass sie in den einschlägigen Datenschutzvorschriften unterwiesen werden.

3. Er trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO gemäß Anlage 1 und hält sie während der Vertragslaufzeit aufrecht. Maßnahmen dürfen an den technischen Fortschritt angepasst werden, solange das vereinbarte Schutzniveau nicht unterschritten wird; wesentliche Änderungen dokumentiert er und teilt sie mit.

4. Er unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Erfüllung der Betroffenenrechte (§ 7) sowie bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen (Art. 32 bis 36 DSGVO), soweit dies erforderlich ist und dem Auftragsverarbeiter die nötigen Informationen vorliegen.

5. Er meldet Verletzungen des Schutzes personenbezogener Daten nach § 9 unverzüglich.

6. Er verarbeitet die Daten in einem Mitgliedstaat der EU oder in einem Vertragsstaat des EWR; hiervon abweichende Verarbeitungen bei Unterauftragsverarbeitern sind in Anlage 2 benannt und nur unter den Voraussetzungen der Art. 44 ff. DSGVO zulässig.

7. Er benennt als Ansprechperson für Datenschutzfragen: [PLATZHALTER: Name und Kontaktdaten; falls ein Datenschutzbeauftragter benannt ist, hier nennen].

8. Er führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

§ 5 Unterauftragsverarbeiter

1. Der Verantwortliche stimmt dem Einsatz der in Anlage 2 aufgeführten Unterauftragsverarbeiter zu.

2. Weitere Unterauftragsverarbeiter darf der Auftragsverarbeiter im Wege der allgemeinen schriftlichen Genehmigung hinzuziehen. Er informiert den Verantwortlichen mindestens [PLATZHALTER: z. B. vier Wochen] vorher in Textform über beabsichtigte Änderungen.

3. Der Verantwortliche kann einer Änderung innerhalb von [PLATZHALTER: z. B. zwei Wochen] aus wichtigem, datenschutzrechtlichem Grund widersprechen. Lässt sich der Widerspruch nicht ausräumen, kann der Verantwortliche den Hauptvertrag zum Zeitpunkt der Umstellung außerordentlich kündigen.

4. Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die den Pflichten dieses Vertrags entsprechen (Art. 28 Abs. 4 DSGVO), und prüft ihn vor Beauftragung sowie danach regelmäßig.

5. Nebenleistungen wie Telekommunikationsdienste, Reinigung, Bewachung oder die Entsorgung von Datenträgern gelten nicht als Unterauftragsverarbeitung; der Auftragsverarbeiter trifft dort angemessene Schutzvorkehrungen.

§ 6 Technische und organisatorische Maßnahmen

Die vom Auftragsverarbeiter getroffenen Maßnahmen nach Art. 32 DSGVO sind in Anlage 1 beschrieben. Sie sind Vertragsbestandteil.

§ 7 Rechte betroffener Personen

1. Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet er das Anliegen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst.

2. Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Zumutbaren bei Auskunft, Berichtigung, Einschränkung, Löschung, Datenübertragbarkeit und Widerspruch, insbesondere durch geeignete Funktionen in der Software.

3. Berichtigung, Löschung und Einschränkung nimmt der Auftragsverarbeiter nur auf Weisung des Verantwortlichen vor, soweit er dies nicht selbst gesetzlich zu tun hat.

§ 8 Nachweise und Überprüfungen

1. Der Auftragsverarbeiter weist die Einhaltung der Pflichten aus Art. 28 DSGVO auf Anfrage nach, insbesondere durch Auskunft, aktuelle Beschreibungen der Maßnahmen nach Anlage 1 oder geeignete Zertifikate und Prüfberichte.

2. Der Verantwortliche kann sich nach vorheriger Ankündigung mit angemessener Frist – in der Regel [PLATZHALTER: z. B. zwei Wochen] – während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs von der Einhaltung überzeugen, auch durch beauftragte Prüfer, die keine Wettbewerber des Auftragsverarbeiters sein dürfen.

3. Vor-Ort-Kontrollen beschränken sich auf das erforderliche Maß und erfolgen höchstens [PLATZHALTER: z. B. einmal jährlich], es sei denn, es besteht ein besonderer Anlass. Der Auftragsverarbeiter kann für den Aufwand einer Prüfung, die über die Vorlage von Nachweisen hinausgeht, eine angemessene Vergütung verlangen, sofern kein Anlass in seiner Sphäre besteht.

4. Prüfende Personen sind zur Vertraulichkeit zu verpflichten.

§ 9 Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch innerhalb von [PLATZHALTER: z. B. 24 Stunden] nach Kenntnis, in Textform an die in § 3 benannte Ansprechperson.

2. Die Meldung enthält, soweit bekannt: Beschreibung des Vorfalls, betroffene Datenkategorien und

ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen sowie ergriffene oder vorgeschlagene Gegenmaßnahmen.

3. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei dessen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO und dokumentiert Vorfälle nachvollziehbar.

§ 10 Löschung und Rückgabe nach Beendigung

1. Nach Beendigung des Auftrags stellt der Auftragsverarbeiter dem Verantwortlichen die Daten auf Wunsch in einem gängigen, maschinenlesbaren Format bereit oder löscht sie, jeweils nach Wahl des Verantwortlichen.

2. Die Herausgabe erfolgt innerhalb von [PLATZHALTER: z. B. 30 Tagen] nach Vertragsende. Danach löscht der Auftragsverarbeiter die Daten einschließlich der Schadensfotos innerhalb von [PLATZHALTER: z. B. weiteren 30 Tagen] datenschutzgerecht und bestätigt die Löschung auf Verlangen in Textform.

3. Sicherungskopien werden im Rahmen der regulären Rotation nach spätestens [PLATZHALTER: z. B. 90 Tagen] überschrieben; bis dahin bleiben sie durch die Maßnahmen der Anlage 1 geschützt.

4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, darf der Auftragsverarbeiter entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren.

§ 11 Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Innenverhältnis gelten ergänzend die Haftungsregelungen des Hauptvertrags, soweit sie zwingendem Recht nicht entgegenstehen.

§ 12 Schlussbestimmungen

1. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen in Datenschutzfragen die Regelungen dieses Vertrags vor.

2. Änderungen und Ergänzungen bedürfen der Textform; das gilt auch für die Aufhebung dieser Klausel.

3. Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

4. Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist [PLATZHALTER: Ort], soweit gesetzlich zulässig.

Unterschriften

Ort, Datum: _____ Ort, Datum: _____

Verantwortlicher: _____ Auftragsverarbeiter: _____

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Die folgenden Maßnahmen sind vor der Verwendung an den tatsächlichen Betrieb anzupassen. [PLATZHALTER: Angaben prüfen und ergänzen, insbesondere Serverstandort, Sicherungsintervalle und Aufbewahrungsdauer.]

1. Verschlüsselung (Art. 32 Abs. 1 lit. a)

• Transportverschlüsselung: Der Zugriff auf Website und App erfolgt ausschließlich über HTTPS (TLS 1.2 oder höher). Unverschlüsselte Aufrufe werden auf HTTPS umgeleitet.

• Die Verbindung zwischen dem Server und dem vorgelagerten Netzwerkdienst läuft über einen ausgehenden, verschlüsselten Tunnel; der Server ist nicht direkt aus dem Internet erreichbar und benötigt keine offenen eingehenden Ports.

• Push-Nachrichten werden Ende-zu-Ende verschlüsselt an den Push-Dienst des Browserherstellers übergeben (Web-Push mit VAPID).

• Verschlüsselung ruhender Daten: [PLATZHALTER: z. B. „Festplattenverschlüsselung mit BitLocker“ – Ist-Zustand angeben].

2. Vertraulichkeit – Zutritt, Zugang, Zugriff

• Zutrittskontrolle: [PLATZHALTER: Beschreibung des Serverstandorts, z. B. Rechenzentrum mit Zutrittskontrolle oder abschließbarer Raum].

• Zugangskontrolle: Anmeldung in der App ausschließlich über persönliche, zufällig erzeugte Zugangscodes; jede Anmeldung erzeugt ein zufälliges Sitzungs-Token, das jederzeit von der Leitung zurückgesetzt werden kann.

• Administrativer Zugang zum Server nur für benannte Personen mit eigenen Konten und starken Passwörtern [PLATZHALTER: ergänzen, falls Zwei-Faktor-Authentisierung im Einsatz ist].

• Zugriffskontrolle: abgestuftes Rollenkonzept (Admin, Vorgesetzte, Fuhrpark, Mitarbeitende); fachliche Funktionen wie das Verwalten von Fahrzeugen, das Freigeben von Urlaub oder das Verteilen von Aufgaben sind an Rollen und Abteilungen gebunden und werden bei jedem Aufruf serverseitig geprüft.

• Dateien mit Schadensfotos werden nur nach erfolgreicher Authentifizierung ausgeliefert.

3. Trennung und Mandantentrennung

• Jeder Kunde erhält eine eigene Instanz mit eigener Datenbankdatei und eigenem Dateiablageordner; ein Zugriff über Mandantengrenzen hinweg ist technisch nicht vorgesehen.

• Trennung von Produktiv- und Testumgebung; Tests laufen ausschließlich auf Kopien oder mit Testdaten.

• Getrennte Verarbeitung von Daten unterschiedlicher Zwecke innerhalb der Anwendung (z. B. Bestell-, Dienst- und Leihwagendaten).

4. Integrität – Eingabe- und Weitergabekontrolle

• Änderungen an Schäden, Ausleihen und Aufgaben werden mit Zeitpunkt und handelnder Person gespeichert.

• Weitergabekontrolle: Datenübertragung ausschließlich verschlüsselt; kein Versand personenbezogener Daten an Analyse- oder Werbedienste; keine externen Einbettungen auf Website und in der App.

• Serverseitige Prüfung aller eingehenden Daten; Schreibrechte nur nach Rollenprüfung.

5. Verfügbarkeit und Belastbarkeit

• Automatische Sicherung der Datenbank und der Schadensfotos [PLATZHALTER: z. B. täglich um 3:00 Uhr] auf ein getrenntes Speicherziel; Datenbanksicherung im laufenden Betrieb ohne Sperrzeiten.

• Aufbewahrung der Sicherungen: [PLATZHALTER: z. B. 30 Tage rollierend]; Ablage: [PLATZHALTER: Ort/Medium, z. B. zweiter Datenträger im Haus / verschlüsselter externer Speicher].

• Wiederherstellung wird [PLATZHALTER: z. B. halbjährlich] getestet und dokumentiert.

• Schutz vor Überlastung und Angriffen aus dem Internet durch den vorgelagerten Netzwerkdienst (Cloudflare), inklusive Schutz vor verteilten Überlastangriffen.

• Aktualisierungen von Betriebssystem und Anwendung werden [PLATZHALTER: z. B. monatlich] eingespielt.

6. Löschkonzept

• Beschäftigtendaten: Löschung des Kontos durch die Leitung des Kunden; damit entfallen Zugangscode und Token unmittelbar.

• Aufgaben und Bestellungen werden nach Erledigung bzw. Tagesabschluss nur noch für den laufenden Betrieb vorgehalten; ältere Ausleihen verschwinden nach [PLATZHALTER: z. B. 60 Tagen] aus der Anwendungsansicht.

• Schadensfotos werden mit dem zugehörigen Schaden gelöscht; die Datei wird dabei vom Datenträger entfernt.

• Server-Protokolle werden nach [PLATZHALTER: z. B. 7 Tagen] automatisch gelöscht.

• Vertragsende: Herausgabe und Löschung nach § 10 dieses Vertrags.

• Datenträger werden vor der Aussonderung sicher gelöscht oder physisch zerstört.

7. Organisation und Überprüfung

- Verpflichtung aller mit der Verarbeitung befassten Personen auf Vertraulichkeit; Unterweisung zum Datenschutz [PLATZHALTER: z. B. jährlich].
- Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.
- Verfahren zur Meldung von Datenschutzvorfällen gemäß § 9 dieses Vertrags.
- Regelmäßige Überprüfung und Bewertung der Maßnahmen [PLATZHALTER: z. B. jährlich und anlassbezogen].
- Auftragskontrolle: schriftliche Verträge mit allen Unterauftragsverarbeitern, Auswahl nach Eignung und Prüfung der Nachweise.

Anlage 2 – Genehmigte Unterauftragsverarbeiter

- Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA – Content-Delivery-Network, Reverse Proxy und verschlüsselter Tunnel für die Erreichbarkeit aus dem Internet. Drittlandtransfer in die USA; Garantien: Zertifizierung nach dem EU-US Data Privacy Framework sowie Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914) nebst Auftragsverarbeitungsvertrag.
- [PLATZHALTER: Hosting-Anbieter mit Firma, Anschrift und Leistung – entfällt, wenn der Server in eigenen Räumen betrieben wird.]
- [PLATZHALTER: weitere Unterauftragsverarbeiter, z. B. Anbieter des Sicherungsspeichers oder des E-Mail-Postfachs.]

Die Push-Dienste der Browserhersteller (z. B. Google, Apple, Mozilla) stellen die Zustellung der Benachrichtigungen sicher. Sie erhalten die Push-Adresse des Geräts und den verschlüsselten Nachrichteninhalt und handeln dabei nicht als Unterauftragsverarbeiter des Auftragsverarbeiters, sondern als eigenständige Anbieter des jeweiligen Endgeräte-Ökosystems.

Stand: [PLATZHALTER: Datum]