

Auftragsverarbeitungsvertrag

zwischen

Bezeichnung Auftraggeber

Anschrift Auftraggeber

vertreten durch

_____, ebenda,
Vertreter Auftraggeber

-nachfolgend: **Auftraggeber-**

und

der **carzilla GmbH**, Essener Straße 99c, 46047 Oberhausen,

vertreten durch den einzelvertretungsberechtigten Geschäftsführer Michael Kessel, ebenda

-nachfolgend: **Auftragnehmer-**

1. Gegenstand und Dauer des Auftrags

1.1. Der Auftragnehmer bietet datenbankbasierte Suchservices für Fahrzeugbestände gewerblicher Automobilhändler an. Die Fahrzeugbestände sind sowohl über die Domain www.carzilla.de abruf- und filterbar als auch optional als Modul in Händlerseiten zu integrieren. Interessenten können bezüglich des betreffenden Fahrzeugs Kontakt zum Händler aufnehmen. Ziel ist die Generierung von Leads zur Fahrzeugvermarktung.

1.2. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart beziehungsweise entsprechend den Weisungen des Auftraggebers, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

1.3. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

1.4. Dauer und Bestand dieses Vertrages richten sich nach dem Hauptvertrag zur Leistungserbringung gemäß Ziffer 1.1.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen

2.1. Der Zweck der Verarbeitung ergibt sich aus Ziffer 1.1. Dabei verarbeitet der Auftragnehmer ausschließlich Daten, die der Auftraggeber oder sonstige autorisierte Nutzer in die Datenbank einbringen. Sämtliche eingebrachten Daten werden entweder vom Auftraggeber oder nach dessen Weisung erhoben. Die vertragliche Verarbeitung besteht im Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassung, Veränderung, Auslesen, Abfragen, Verwendung, Übermittlung, Verbreitung, Bereitstellung, Abgleich, Verknüpfung, Einschränken und Löschen von Daten.

2.2. Gegenstand der Verarbeitung können Anreden, Namen, Arbeitgeberbezeichnungen, Telefonnummern, Emailadressen, Erreichbarkeitsmitteilungen und Nachrichten sein.

2.3. Von der Verarbeitung sind Kunden, deren Beschäftigte, etwaige Kommunikationspartner sowie Interessenten betroffen.

3. Rechte, Pflichten und Weisungsbefugnisse des Auftraggebers

3.1. Für die Beurteilung der Zulässigkeit der Verarbeitung im Sinne des Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Artt. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle entsprechenden Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

3.2. Der Auftraggeber erteilt, bzw. übermittelt alle Aufträge, Teilaufträge und Weisungen jedenfalls in Form des Portable Document Format (PDF). Sollte ihm dies aus technischen Gründen nicht möglich sein, in einem vergleichbaren anderen Format, welches geeignet ist, die jeweilige Erklärung unverändert wiederzugeben. Mündliche oder fernmündliche Weisungen sind unverzüglich durch Erklärungen in dem vorgenannten Format zu bestätigen.

3.3. Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

3.4. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

3.5. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

3.6. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 h) DSGVO).

4. Weisungsbefugnis des Auftraggebers, Weisungsempfänger des Auftragnehmers

4.1. Weisungen des Auftraggebers sind nur beachtlich und rechtmäßig, wenn sie von einem seiner Weisungsberechtigten an einen empfangsberechtigten Adressaten des Auftragnehmers gerichtet werden.

4.2. Weisungsberechtigter des Auftraggebers ist ausschließlich sein im Rubrum dieses Vertrages benannter Vertreter.

4.3. Weisungsempfänger des Auftragnehmers sind:

Nachname, Vorname	Emailadresse	Telefonnummer
Giesen, Sebastian	support@cargate.biz	0208 – 69 64 02 22
Schröer, Christian	support@cargate.biz	0208 – 69 64 02 22

4.4. Bei einem Wechsel oder einer Verhinderung der jeweiligen Ansprechpartner von mehr als einer Woche sind dem Vertragspartner unverzüglich jedenfalls im in Ziffer 3.2. genannten Format Nachfolger bzw. Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

5.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 a) DSGVO).

5.2. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

5.3. Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 e) und f) DSGVO). Er hat die dazu erforderlichen Angaben nach entsprechender Aufforderung unverzüglich an den Auftraggeber zu übermitteln.

5.4. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Diese Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Ziffer 4.5. gilt entsprechend.

5.5. Der Auftragnehmer darf personenbezogene Daten aus dem Auftragsverhältnis nur nach Weisung des Auftraggebers berichtigen, löschen oder in ihrer Verarbeitung einzuschränken.

5.6. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

5.7. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren, welche nach Beendigung des Vertrages fortbesteht.

5.8. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb. Er sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 b), 29 DSGVO).

5.9. Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 f) DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

5.10. Beim Auftragnehmer ist als Beauftragter für den Datenschutz bestellt:

Nachname, Vorname	Emailadresse	Telefonnummer
Keller, Friedrich	datenschutz@carzilla.de	0208 – 69 64 02 60

Ein Wechsel des Datenschutzbeauftragten wird dem Arbeitgeber unverzüglich jedenfalls im in Ziffer 3.2. genannten Format mitgeteilt.

6. Unterauftragsverhältnisse mit Subunternehmern

6.1. Zur Leistungserbringung bedient sich der Auftragnehmer unter Umständen Subunternehmern. Zurzeit sind für den Auftragnehmer die in Anlage 1, Ziffer 1 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragnehmer hat mit diesen Subunternehmern vertragliche Abreden getroffen, die ihnen die gleichen Datenschutzpflichten auferlegen, welche der Auftragnehmer auf der Grundlage dieses Vertrages zu erfüllen hat.

6.2. Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO). Die Hinzuziehung neuer oder Austausch bestehender Subunternehmer ist zulässig, wenn der Auftragnehmer die beabsichtigte Änderung 4 Wochen vor dem Eintritt der Änderung dem Auftraggeber anzeigt und der Auftraggeber nicht 2 Wochen vor dem Eintritt der Änderung Einspruch gegen die beabsichtigte Änderung erhebt.

6.3. Anzeigen, Einsprüche und Vertragsabschlüsse im Sinne der Ziffer 6 haben jedenfalls in der in Ziffer 3.2. genannten Form zu erfolgen.

7. Technische und organisatorische Maßnahmen

7.1. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

7.2. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

7.3. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber das Sicherheitsniveau der festgelegten Maßnahmen (Anlage 1, Ziffer 2) nicht unterschreiten. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form im in Ziffer 3.2. genannten Format abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

8. Verpflichtung nach Beendigung des Auftrags

8.1. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen bzw. zu vernichten.

8.2. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe jedenfalls in dem Format im Sinne der Ziffer 3.2. zu bestätigen.

9. Sonstiges

9.1. Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

9.2. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

9.3. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

9.4. Änderungen dieses Vertrages sind von Auftraggeber und Auftragnehmer jedenfalls in dem in Ziffer 3.2. genannten Format zu vereinbaren.

9.5. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Auftraggeber

carzilla GmbH
Essener Str. 99c
46047 Oberhausen
fon: 0208 - 69 64 02 - 0
fax: 0208 - 69 64 02 - 20
www.carzilla.de

Auftragnehmer



Anlage 1

1. Subunternehmer des Auftragnehmers (Ziffer 6)

- dotzilla GmbH & Co. KG, Essener Straße 99c, 46047 Oberhausen – Rechnungslegung
- OVH GmbH, Dudweiler Landstraße 5, 66123 Saarbrücken – Hosting

2. Technische- und organisatorische Maßnahmen des Auftragnehmers (Ziffer 7), Kurzdarstellung

- **Zutrittskontrolle:**

Der Zugang zu den Geschäftsräumen ist durch ein mit einem abgestuften Berechtigungssystem ausgestattetes elektronisches Schlüsselsystem gesichert. Bei Verlust eines Schlüssels oder Ausscheiden eines Mitarbeiters werden die Schlüssel deaktiviert.

- **Zugangskontrolle**

Der Auftragnehmer hat für seine Datenverarbeitungssysteme eine Benutzerordnung realisiert, nach der neue Benutzer nur auf Antrag bei der Personalleitung angelegt werden können. Ebenso wurden Passwortkonventionen sowie geregelte Lösungsabläufe für deaktivierte und ungenutzte Benutzerkonten realisiert.

- **Zugriffskontrolle**

Es wurde ein Berechtigungssystem implementiert. Berechtigungen werden dabei durch den Vorgesetzten vergeben. Dabei erhält jeder Benutzer nur die für die Erbringung seiner Arbeitsleistung zwingend erforderlichen Berechtigungen. Spezielle Berechtigungen mit besonders hoher Sicherheitsrelevanz, etwa solche für die Server-/Datenbankverwaltung und -administration können nur direkt bei der Geschäftsführung beantragt werden.

- **Trennungskontrolle**

Die Datenverarbeitungssysteme sind mandantenfähig. Entwicklungsumgebungen sind von Produktivsystemen getrennt.

- **Weitergabekontrolle**

Externe Datenzugriffe finden ausschließlich über verschlüsselte Tunnelverbindungen statt.

- **Eingabekontrolle**

Eingaben, Änderungen und Löschungen erfolgen auf der Grundlage des Berechtigungskonzepts.

- **Verfügbarkeitskontrolle**

Alle relevanten Daten werden auf ortsverschiedenen Sicherungsmedien gespeichert. Das Datendelta wird täglich gesichert. Zusätzlich erfolgen wöchentliche Komplettsicherungen. Die Wiederherstellung der

Datenverarbeitungssysteme erfolgt nach Maßgabe des Notfallhandbuches und des darin befindlichen Disaster-Recovery-Konzepts.

Die Produktivsysteme verfügen über RAID-Konfigurationen und unterbrechungsfreie Stromversorgung.

Sowohl Server als auch Clients befinden sich hinter Firewalls und sind mit Virenschutzsoftware ausgestattet. Die Virensignaturen werden automatisiert täglich geprüft und erforderlichenfalls aktualisiert.

- **Wiederherstellbarkeit**

Bei dem Auftragnehmer ist ein Notfallmanagement realisiert, welches bei Unterbrechungen des Betriebsablaufes ein schnelle Wiederinbetriebnahme der Datenverarbeitungssysteme gewährleistet.

- **Auftragskontrolle**

Beauftragung und Informationsaustausch zwischen Auftraggeber und Auftragnehmer erfolgen über webbasierte Anwendungen und standardisierte Auftragsformulare. Für die Sicherstellung der weisungsgemäßen Verarbeitung sind Verfahrensabläufe implementiert und Arbeitsanweisungen vorhanden. Deren Einhaltung wird regelmäßig vom internen Qualitätsmanagement überwacht.