Auftrag zur Datenverarbeitung gemäß Artikel 28 DSGVO

VEREINBARUNG

zwischen

– nachstehend Auftraggeber genannt –

und
P4 MobileMedia GmbH, Marktplatz 13, 65183 Wiesbaden
– nachstehend Auftragsverarbeiter genannt –

1. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags zur Datenverarbeitung ist die Durchführung folgender Aufgaben durch den Auftragsverarbeiter:

Verwaltung von *Mitarbeiterdaten* (Name, Vorname, Bild, Kommunikationsdaten).
Funktion in einem webgesteuerten Portal mit Zugangsbeschränkungen.
Das Portal läuft im Rechenzentrum 1&1 United Internet, Berlin.
Die Daten sind bereits zugänglich über die Webseite des Auftraggebers.

Verwaltung von *Kundenkarten** (Kundenname, Kennzeichen, EZ, Kilometerstand).
Funktion in einem gesonderten, webgesteuerten Portal mit Zugangsbeschränkungen
Das Portal läuft im Rechenzentrum 1&1 United Internet, Berlin

* Falls das Autohaus das Modul Kundenkarten gebucht hat.

Die Daten werden redundant gehalten und sind vor externen Zugriffen geschützt.
Die Daten dienen zur Darstellung innerhalb des Produktes Autohaus-App.

Die Dauer dieses Vertrages (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

Die Beendigung des Vertragsverhältnisses zur Autohaus-App zwischen Auftraggeber und Auftragsverarbeiter (erstmals möglich nach einem vollen Kalenderjahr unter Einhaltung einer dreimonatigen Kündigungsfrist schriftlich jeweils zum Jahresende) führt zur Beendigung des Auftrags zur Datenverarbeitung bzw. Datenhaltung.

2. Auftragsinhalte

Nähere Beschreibung des Auftragsgegenstandes bezüglich Umfang, Art und Zweck der festgelegten Aufgaben des Auftragsverarbeiters:

Erfassung der Mitarbeiterdaten in einer webbasierten Datenbank.
Datenbank steuert die Anzeige der Mitarbeiter innerhalb des Produktes Autohaus-App.

Die Verarbeitung sowie Nutzung der Daten durch den Auftragsverarbeiter findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland statt. Jede Verlagerung der Datenverarbeitung oder Nutzung in ein Drittland bedarf der Zustimmung des Auftraggebers und darf nur erfolgen, sofern die Vorgaben der Art. 44 ff. DSGVO zutreffen.

Gegenstand der Speicherung, Verarbeitung und Nutzung personenbezogener Daten sind folgende Datenarten und Kategorien:

- Mitarbeiterdaten des Autohauses
- Name, Vorname, Bild, Funktion, Kommunikationsdaten.

Die Daten werden dem Auftragsverarbeiter durch den Auftraggeber zur Verfügung gestellt.
Die Daten werden sowohl vom Auftragsverarbeiter als auch von berechtigten Mitarbeitern des Auftraggebers verwaltet und aktualisiert.

- Falls Kundenkarten-System gebucht:
  Kundenname, Kfz-Kennzeichen, Erst-Zulassung, Kilometerstand.

Die Daten werden ausschließlich von Mitarbeitern des Auftraggebers erfasst und verwaltet .

3. Technisch-organisatorische Maßnahmen

Der Auftragsverarbeiter ist verpflichtet, die Umsetzung der bei Auftragsvergabe vereinbarten technischen und organisatorischen Maßnahmen noch vor Auftragsdurchführung umfassend zu dokumentieren bzw. zu erläutern. Eine Dokumentation seitens des Auftragsverarbeiters entfällt, da der Auftraggeber jederzeit Zugriff auf die gespeicherten Daten hat und diese jederzeit selbst verändern und auch löschen kann. Akzeptiert der Auftraggeber die Maßnahmen, bilden diese die Grundlage des Auftrags. Etwaige Anpassungen sind einvernehmlich vorzunehmen.

4. Berichtigung, Einschränkung und Löschung von Daten

Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragsverarbeiter sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- *Benennung von Ansprechpartnern*
  Der Auftragsverarbeiter benennt folgende Ansprechpartner:

  Herrn Raimund Pfeiffer, P4 Vertrieb
  Tel. 0611 5058891, E-Mail: r.pfeiffer@p4-mobilemedia.de

  Herrn Frank Pütter, P4 Entwicklung
  Tel. 02331 4833449, E-Mail: f.puetter@p4-mobilemedia.de).

  Zur Bestellung eines Datenschutzbeauftragten ist der Auftragsverarbeiter gemäß §38 Abs.1 BDSG-neu nicht verpflichtet.

- *Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. c, 29, 32 Abs. 4 DS-GVO*
  Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- *Umsetzung und Einhaltung* aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO
  (s. Anlage 1).

- *Zusammenarbeit mit der Aufsichtsbehörde*
  Auftraggeber und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
  Der Auftraggeber wird unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informiert, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.
  Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

- *Regelmäßige Kontrollen*
  Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

- *Nachweisbarkeit*
  Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse erfolgt nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

Die Erteilung von Unterauftragsverhältnissen durch den Auftragsverarbeiter ist nur nach Weisung und Zustimmung durch den Auftraggeber zulässig. Werden diese nach Ansicht des Auftragsverarbeiters notwendig, informiert der Auftragsverarbeiter den Auftraggeber unverzüglich schriftlich darüber (s. Anlage 2).

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unteraufauftrag-nehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform).

7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

Der Auftragsverarbeiter stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten nach Art. 28 DS-GVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Nachweis von Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:
- Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
- Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO
- Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Revision, Wirtschaftsprüfer, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren)
- Geeignete Zertifizierung durch IT-Sicherheits-/Datenschutzaudit (z.B. nach BSI Grundschutz).

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragsverarbeiter einen Vergütungsanspruch geltend machen.

8. Unterstützung des Auftraggebers

Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u. a.:

Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.

Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.

Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.

Für die Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

Der Datenumgang erfolgt ausschließlich im Rahmen der hier getroffenen Vereinbarungen und entsprechend der Weisung des Auftraggebers. Unabhängig von dieser Vereinbarung behält sich der Auftraggeber ein umfassendes Weisungsrecht vor. Veränderungen bezüglich des Gegenstandes und der Verarbeitungsverfahren bedürfen der einvernehmlichen Abstimmung.

Weisungen des Auftraggebers werden dem Auftragsverarbeiter stets in schriftlicher Form erteilt (E-Mail, Fax, Brief usw.). Mündliche Weisungen werden umgehend schriftlich verfasst. Es bedarf der umgehenden Mitteilung durch den Auftragsverarbeiter, wenn dieser annimmt, dass die erfolgte Weisung gegen datenschutzrechtliche Bestimmungen verstößt.

Der Auftragsverarbeiter verwendet die Daten zu keinem anderen Zweck und ist auch nicht zur Weitergabe von Daten, die Gegenstand des Auftrages sind, an Dritte berechtigt.

10. Löschung von Daten und Rückgabe von Datenträgern

Kopien oder Duplikate der 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.

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Vereinbarungen zum Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragsverarbeiter i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der evtl. zugehörigen Datenträger ausgeschlossen wird.

12. Einwilligungserklärung der Mitarbeiter

Mit Unterschrift bestätigt der Auftraggeber das Vorliegen der Einwilligungserklärung der Mitarbeiterinnen und Mitarbeiter zur Nutzung von Fotos und personenbezogenen Daten für die Präsentation in der Autohaus-App (s. Muster Anlage 3)

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Auftraggeber	Auftragsverarbeiter

Anlage 1 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 2 – Unterauftragnehmer

Anlage 3 – Einwilligungserklärung zur Nutzung von Fotoaufnahmen von Mitarbeiterinnen und Mitarbeitern in der Autohaus-App (Muster)

V. 1.0.1.

Anlage 1 – Technische und organisatorische Maßnahmen des Auftragsverarbeiters

Zugangskontrolle
Gewährleistung, dass Unbefugten der Zugang zu Anlagen, mit denen die Datenverarbeitung durchgeführt wird, verwehrt ist.
Im Unternehmen wird Clean Desk Politik gelebt. Die mit personenbezogenen Daten befassten Personen sind dazu angehalten, kundenrelevante Unterlagen mit besonderer Vorsicht zu behandeln. Durch wiederkehrende Schulungen (Datenschutz und Informationssicherheit) wird auf die Awareness der Mitarbeiter hingewirkt.

Datenträgerkontrolle
Gewährleistung, dass Unbefugte Datenträger nicht Lesen, Kopieren, Verändern und Löschen können. Die Zugänge im System sind reglementiert. Durch regelmäßige Datensicherung wird sichergestellt, dass die Verfügbarkeit der Daten gewährleistet wird.

Speicherkontrolle
Gewährleistung, dass die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten verhindert wird. Durch regelmäßige Schulungen und Überprüfung der Verfahrensanweisungen wird sichergestellt, dass personenbezogene Daten ausschließlich und in einem angemessenen Verhältnis gespeichert werden (Notwendigkeit und Verhältnismäßigkeit der Datenspeicherung).

Benutzerkontrolle
Gewährleistung, dass im Unternehmen sichere Verbindungen zu Kundensystemen sowie zu Daten hergestellt werden, die in Rechenzentren gespeichert sind und auf die zugegriffen werden kann.
Die Benutzerkennungen für die Mitarbeiterinnen und Mitarbeiter – sowohl beim Auftragsverarbeiter als auch beim Auftraggeber – werden vom Auftragsverarbeiter verwaltet und im Normalfall alle 12 Monate geändert.

Zugriffskontrolle
Gewährleistung, dass die zur Benutzung eines automatisierten Systems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.
Die Berechtigungen werden entsprechend der organisatorischen Struktur des Unternehmens und der Notwendigkeit (Sparsamkeit der Daten) vergeben.

Übertragungskontrolle
Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.
Der Zugriff auf die Datenbanken sowie die Systemdateien ist über Benutzerkennungen – Mandant, Kennung, Passwort – klar reglementiert.

Eingabekontrolle
Gewährleistung beim Kundenkarten-System, dass nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert wurden.

Transportkontrolle
Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird. Löschen von Datensätzen sind nur von einem eingeschränkten und definierten Personenkreis durchführbar.
Mit Partnern werden ADV-Verträge abgeschlossen, so dass eine Datensicherheit im Sinne der DS-GVO gewährleistet werden kann. Datensicherungen werden im Rechenzentrum durchgeführt und auf externen Festplatten gespeichert. Diese werden regelmäßig durch definierte Personen extern aufbewahrt.

Wiederherstellbarkeit
Gewährleistung, dass eingesetzte Systeme im Störungsfall durch Backups im Rechenzentrum wiederhergestellt werden können.

Zuverlässigkeit
Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden. Durch die Beauftragung des IT-Dienstleisters 1&1 Internet SE wird sichergestellt, dass die Systeme den Verfügbarkeitsanforderungen von P4 entsprechen.
P4 ist als Softwaredienstleister sehr sensibel für Fehlfunktionen. Die Mitarbeiter sind angehalten, Auffälligkeiten direkt zu melden und diese mit den verantwortlichen Personen im Unternehmen abzustimmen.

Datenintegrität
Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.
Der Zugriff auf die Datenbanken sowie die Systemdateien ist klar reglementiert.

Auftragskontrolle
Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

Verfügbarkeitskontrolle
Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind Lizenzdaten sind nur von einem eingeschränkten und definierten Personenkreis änderbar. Das Rechenzentrum ist mit einer Klimaanlage und einer USV ausgestattet.

Trennbarkeit
Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Die Trennung der Fachbereiche (z. B. Buchhaltung, Personal, Geschäftsführung) ist über das Berechtigungssystem geregelt.

Anlage 2 - Unterauftragnehmer

Zwischen P4 MobileMedia und dem Auftraggeber besteht ein „Vertrag zur Auftragsdatenverarbeitung“. P4 nimmt für die Verarbeitung von personenbezogenen Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die im Auftrag von P4 diese Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um folgende Dienstleister:

Partner	**Prozess**
1&1 Internet SE Elgendorfer Str. 57, 56410 Montabaur	RZ - Services
Frank Pütter – Perfect Apps Am Fleyer Bach 45, 58093 Hagen	Projekt-Manager
PAR Consult GmbH, Raimund Pfeiffer Rheingaustr. 167, 65203 Wiesbaden	Projekt-Manager

Anlage 3 – Einwilligungserklärung zur Nutzung von Fotoaufnahmen von Mitarbeiterinnen und Mitarbeitern in der Autohaus-App (Muster)

Autohaus _____

Herr/Frau _____

Name, Vorname _____

Geburtsdatum _____

Anschrift _____

im Folgenden „die/der Fotografierte“ genannt.

Gegenstand
Fotografische Aufnahmen der/des Fotografierten

Verwendungszweck
Veröffentlichung auf der Webseite des Unternehmens und in der Autohaus-App zur bildlichen Darstellung des Ansprechpartners für die Dauer des Arbeitsverhältnisses inkl. Funktionsbeschreibung der Stelle.

Erklärung
Der Unterzeichner erklärt sein Einverständnis mit der Verwendung der fotografischen Aufnahmen seiner Person für die oben beschriebenen Zwecke. Eine Verwendung der fotografischen Aufnahmen für andere als die beschriebenen Zwecke oder ein Inverkehrbringen durch Überlassung der Aufnahmen an Dritte ist unzulässig. Diese Einwilligung ist freiwillig. Wird sie nicht erteilt, entstehen keine Nachteile. Diese Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Ort, Datum **Unterschrift**