



# Vertrag zur Auftragsverarbeitung

zwischen

**Kadda Peters – Virtuelle Assistentin für moderne Rechtsanwälte**  
**Inhaberin Katharina Peters**  
**Altendorfer Grenzweg 2, 21706 Drochtersen**

als Auftragsverarbeiter **-Auftragnehmer-**

und

**Vorname, Name/Firmierung**  
**Spezifizierung/ Inhaber Name**  
**Vollständige Adresse**

als Verantwortlicher **-Auftraggeber-**

## 1 Präambel

Im Rahmen der Leistungserbringung nach dem **Angebot/VA-Vertrag** vom **Datum** und auf Grundlage der Allgemeinen Geschäftsbedingungen des Auftragnehmers (im Folgenden Hauptvertrag genannt), arbeitet der Auftragnehmer mit personenbezogenen Daten. Für diese Daten ist der Auftraggeber die verantwortliche Stelle im Sinne des Datenschutzrechts.

Dieser Auftragsverarbeitungsvertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der beiden Parteien.

## 2 Allgemeines

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Auftraggeber ist der datenschutzrechtliche Verantwortliche.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Der Auftraggeber entscheidet selbst, welche Leistungen er vom Auftragsverarbeiter im Einzelnen in Anspruch nehmen möchte.

Der Auftragnehmer ist Auftragsverarbeiter.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.



(4) Verarbeitung ist gem. Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Nämlich das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(5) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

### **3 Vertragsgegenstand**

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich Backoffice/Social-Media-Marketing auf der Grundlage **des Angebotes vom DATUM und den Allgemeinen Geschäftsbedingungen des Auftragnehmer / unseres Vertrags vom DATUM** etc. in der jeweils aktuellen Fassung (im Folgenden als „Hauptvertrag“ bezeichnet). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers.

(2) Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag und den Leistungen, die der Auftraggeber in Anspruch nimmt.

(3) Der Auftragnehmer kann von der Möglichkeit Gebrauch machen, die Auftraggeber-Daten zu anonymisieren oder derart zusammenzutragen, dass keine Identifizierung betroffener Personen mehr möglich ist. Diese Daten darf der Auftragnehmer zur Erfüllung und Weiterentwicklung der nach Maßgabe des Hauptvertrages vereinbarten Dienste verwenden. Die Parteien sind sich darüber einig, dass anonymisierte bzw. aggregierte Auftraggeber-Daten nicht mehr als Auftraggeber-Daten im Sinne dieser Vereinbarung gelten.

(4) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei dem Auftragnehmer, bei dem Auftragnehmer Beschäftigten oder durch den Auftragnehmer Beauftragten mit personenbezogenen Daten in Berührung kommen und die von dem Auftraggeber stammen oder für ihn erhoben wurden.

(5) Der Auftragnehmer verpflichtet sich, die Verarbeitung der Auftraggeber-Daten durch Auftragnehmer grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) durchzuführen. Die Verarbeitung von Auftraggeber-Daten -unter Einhaltung der Bestimmungen dieses Vertrags- in einem Drittland, ist gestattet, wenn er den Auftraggeber vorab in Textform per E-Mail über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44 - 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

Der Auftraggeber kann in diesem Fall in einer angemessenen Frist (14 Tage) Einspruch einlegen.

Verstreicht diese Frist, ohne einen Einspruch, ist dies als eine Genehmigung zu sehen.

Erfolgt ein Einspruch hat der Auftragnehmer das Recht den Hauptvertrag mit einer Frist von 3 Monaten zum Monatsende zu kündigen.

### **4 Weisungsrecht**

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen in diesem Vertrag vom Auftraggeber erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug



auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation.

(2) Die Weisungen des Auftraggebers werden durch den Hauptvertrag festgelegt und können danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist zu jeder Zeit berechtigt, eine solche Weisung zu erteilen. Insbesondere werden davon Weisungen im Hinblick auf die Berichtigung, Löschung und Sperrung von Daten erfasst.

Anfragen durch den Auftraggeber sind an die folgende E-Mail-Adresse zu richten:

**datenschutz@kaddapeters.de**

(3) Änderungen, Ergänzungen oder Ersetzungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt und bedürfen der vorherigen Zustimmung in Textform per E-Mail durch den Auftragnehmer.

(4) Die Weisungen werden dokumentiert und gespeichert.

(5) Der Auftragnehmer gewährleistet die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen in Bezug auf die auftragsgemäße Verarbeitung von personenbezogenen Daten.

(6) Verstößt nach Ansicht des Auftragnehmers eine Weisung des Auftraggebers gegen das geltende Datenschutzrecht oder gegen den Hauptvertrag, ist er- nach einer entsprechenden Mitteilung an den Auftraggeber- berechtigt, die Durchführung der Weisung, bis zu einer Bestätigung oder Änderung des Auftraggebers auszusetzen. Die Bestätigung bzw. Änderung des Auftraggebers muss in Textform per E-Mail erfolgen.

(7) Der Auftraggeber trägt die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeber-Daten.

## **5 Verantwortlichkeit des Auftraggebers**

(1) Der Auftraggeber ist Verantwortlicher gem. Art. 4 Abs. 7 DSGVO. Sowohl für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten als auch für die Wahrung der Rechte Betroffener.

(2) Sollten Dritte gegen den Auftragnehmer aufgrund der weisungsgemäßen Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen diesbezüglichen Ansprüchen nach Aufforderung freistellen.

(3) Der Auftraggeber muss dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Verfügung stellen, damit die Erfüllung des Hauptvertrages möglich ist. Er ist darüber hinaus auch für die Qualität der Auftraggeber-Daten verantwortlich.

(4) Sollte der Auftraggeber Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seiner Weisungen feststellen, muss der Auftraggeber den Auftragnehmer umfassend und unverzüglich darüber informieren.

(5) Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Artikel 30 Absatz 2 DSGVO aufgeführten Angaben zur Verfügung zu stellen, soweit sie im Auftragnehmer nicht selbst vorliegen.

## **6 Anforderungen an Personal/Geheimhaltungsvereinbarung**

Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten. Um dieses zu gewährleisten hat der Auftragnehmer mit den entsprechenden Personen



Verschwiegenheitserklärungen nach der DSGVO abgeschlossen. Auf Anfrage des Auftraggebers wird das Vorliegen der entsprechenden Vereinbarung nachgewiesen.

### **7 Art der verarbeiteten Daten und Kreis der Betroffenen**

(1) Im Rahmen der Durchführung des Hauptvertrags erhält Auftragnehmer Zugriff auf die **in Anlage 2** näher spezifizierten personenbezogenen Daten.

Diese Daten umfassen keine besonderen Kategorien personenbezogener Daten.

#### **Alternativ:**

Diese Daten umfassen besondere Kategorien personenbezogener Daten. Diese werden **in Anlage 2** aufgelistet.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist ebenfalls in **Anlage 2** dargestellt.

### **8 Schutzmaßnahmen des Auftragnehmers**

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht ohne Auftrag an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Standes der Technik zu sichern.

(2) Der Auftragnehmer gestaltet seinen Verantwortungsbereich und die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO. Insbesondere die in **Anlage 3** aufgeführten Maßnahmen.

(3) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei sichergestellt werden muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(4) Ansprechpartner für den Datenschutz ist **Katharina Peters, zu erreichen unter [datenschutz@kaddapeters.de](mailto:datenschutz@kaddapeters.de)**.

### **9 Informationspflichten**

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei dem Auftragnehmer im Rahmen des Auftrags beschäftigten Personen oder durch Dritte, wird der Auftraggeber in Textform per E-Mail informieren. Dasselbe gilt für Prüfungen von Auftragnehmer durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.



(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und informiert den Auftraggeber hierüber.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit die Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 8 Abs. 2 wird Auftragnehmer den Auftraggeber zeitnah unterrichten.

(5) Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält.

#### **10 Einsatz von weiteren Auftragsverarbeitern (Subunternehmer)**

(1) Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Alle zum Vertragschluss bereits hinzugezogenen und durch den Auftraggeber genehmigten weiteren Auftragsverarbeiter ergeben sich aus **Anlage 4**.

(2) Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die als reine Nebenleistungen in Anspruch genommen werden. Dies sind beispielsweise Leistungen, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann. Der Auftragnehmer hat insofern angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten zu treffen.

(3) Der Auftragnehmer hat die Verpflichtung, den Auftraggeber über die Hinzuziehung oder Änderung weiterer Auftragsverarbeiter zu informieren, wobei die Information per E-Mail in Textform ausreichend ist.

(4) Sofern der Auftraggeber mit der Änderung oder Hinzuziehung nicht einverstanden ist, hat er das Recht, Einspruch gegen die Änderung oder Hinzuziehung zu erheben.

(5) Das Einspruchsrecht erlischt, sofern der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung über die Änderung oder Hinzuziehung Einspruch erhebt.

(6) Im Falle eines Einspruchs durch den Auftraggeber, hat der Auftragnehmer das Recht, den Hauptvertrag sowie diesen Auftragsverarbeitungsvertrag mit einer Frist von 3 Monaten zu kündigen.

(7) Der Auftragnehmer ist verpflichtet sicherzustellen, dass der Vertrag zwischen dem Auftragnehmer und einem weiteren Auftragsverarbeiter denselben Regelungen und ggf. ergänzenden Weisungen des Auftraggebers unterliegt, wie sie dem Auftragnehmer Kraft dieses Vertrages obliegen. Diese Voraussetzungen ist gegeben, wenn der Vertrag zwischen dem Auftragnehmer und dem Auftragsverarbeiter den Voraussetzungen des Art. 28 DSGVO entspricht.

(8) Der Auftragnehmer wählt jeden zusätzlichen Auftragsverarbeiter sorgfältig nach dessen Eignung und Zuverlässigkeit aus.

(9) Der Auftragnehmer hat dafür Sorge zu tragen, dass der Auftraggeber seine Rechte -insbesondere seine Prüf- und Kontrollrechte- auch gegenüber dem Subunternehmer ausüben kann.

Der Auftraggeber ist verpflichtet, den Auftragnehmer über anstehende Maßnahmen zu informieren.

(10) Sofern eine Einbeziehung von Auftragsverarbeitern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass bei dem jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-



Standarddatenschutzklauseln). Der Auftragnehmer wird dem Kunden auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Auftragsverarbeitern nachweisen.

(11) Die Mitteilungsverpflichtung des Auftragnehmers, das Einspruchsrecht des Auftraggebers und ein gegebenenfalls bestehendes besondere Kündigungsrecht des Auftragnehmers gelten entsprechend der Absätze 2-9 auch für die Einbeziehung von Subunternehmern aus einem Drittland.

## **11 Rechte Betroffener**

(1) Für die Wahrung der Rechte Betroffener ist der Auftraggeber allein verantwortlich.

(2) Der Auftragnehmer ist dazu verpflichtet, im Rahmen des technisch und organisatorisch Zumutbaren, dem Auftraggeber die notwendigen Informationen, die zur Bearbeitung von Anträgen Betroffener benötigt werden, zugänglich zu machen, damit dieser seinen Pflichten nach Art. 12 Abs. 3 DSGVO nachkommen kann.

Soweit ein Betroffener einen Antrag auf Wahrnehmung seiner ihm zustehenden Rechte nach Art. 12 Abs. 3 DSGVO unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

(3) Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Auftraggeber-Daten und deren Empfänger, an die der Auftragnehmer sie auftragsgemäß weitergibt, geben. Ferner wird er den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht schon selbst vorliegen oder er sich diese selbst beschaffen kann.

(4) Sollten Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken sein, wird der Auftragnehmer dies im Rahmen des Zumutbaren und Erforderlichen und gegen Erstattung der hierdurch entstehenden Aufwendungen und Kosten ermöglichen. Soweit dem Auftraggeber die Vornahme der Berichtigung, der Löschung oder der Einschränkung der weiteren Verarbeitung unmöglich oder nur eingeschränkt möglich ist, wird der Auftragnehmer diese Maßnahmen gegen Erstattung der hierdurch entstehenden Aufwendungen und Kosten vornehmen.

(5) Hat der Betroffene gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Artikel 20 DSGVO, wird der Auftragnehmer dem Auftraggeber die entsprechenden Daten zugänglich machen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

(6) Die Zugänglichmachung nach Absatz 5 erfolgt in zumutbarem und erforderlichem Maße und gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwendungen und Kosten.

## **12 Dauer des Vertrages und besonderes Kündigungsrecht**

(1) Sowohl die Laufzeit als auch die normale Kündigung dieses Vertrages richten sich nach den diesbezüglichen Bestimmungen Hauptvertrages.

(2) Das besondere Kündigungsrecht des Auftragnehmers, bei einer Nichtgenehmigung von weiteren Auftraggebern, oder der Nichtgenehmigung von Datenspeicherungen etc. in einem Drittland wirkt sich auf den Hauptvertrag bzw. die Einzelvereinbarung aus.

Die Kündigung des Auftragnehmers kann in Textform per E-Mail erfolgen. Die Kündigungsfrist beträgt 3 Monate.

In diesem Fall wird sowohl dieser Auftragsverarbeitungsvertrag als auch der Hauptvertrag beendet.



### **13 Datenlöschung**

(1) Der Auftragnehmer wird die Auftraggeber-Daten nach Beendigung dieses Vertrags löschen. Etwaige gesetzliche Verpflichtungen des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten bleiben unberührt.

(2) Die Löschung ist zu dokumentieren. Die Dokumentationen, die dem Nachweis des Auftrags und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende für einen angemessenen Zeitraum aufbewahrt werden.

### **14 Nachweise und Kontrollen**

(1) Der Auftraggeber ist berechtigt, den Auftragnehmer in erforderlichem Umfang bezüglich der Einhaltung der gesetzlichen Vorschriften, der vertraglichen Vereinbarungen zwischen den Parteien und der Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer zu kontrollieren.

(2) Der Auftragnehmer wird dem Auftraggeber auf dessen Begehren hin alle erforderlichen Informationen, die der Durchführung der Kontrolle in Absatz 1 dienen, zur Verfügung stellen. Er hat das Recht, Informationen dann zurückzuhalten, wenn er durch die Herausgabe gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Die Zurückbehaltung erfolgt nach Ermessen des Auftragnehmers unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers.

(3) Der Auftraggeber hat das Recht zu den üblichen Geschäftszeiten auf eigene Kosten die Kontrolle nach Absatz 1 in erforderlichem Umfang vorzunehmen. Er hat dafür zu sorgen, dass der Betriebsablauf nicht unverhältnismäßig gestört wird und die Betriebs- und Geschäftsgeheimnisse gewahrt werden.

(4) Der Auftraggeber hat den Auftragnehmer rechtzeitig, unter einer angemessenen Fristsetzung über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren.

(5) Eine Überprüfung darf nur einmal pro Kalenderjahr erfolgen. Zusätzliche Prüfungen können nach Abstimmung mit dem Auftragnehmer und gegen Kostenerstattung vorgenommen werden.

(6) Bei Beauftragung eines Dritten zur Vornahme der Kontrolle muss der Dritte durch den Auftraggeber ebenso verpflichtet werden, wie wenn der Auftraggeber verpflichtet wäre, wenn er selbst die Kontrolle durchführen würde.

Sollte der Dritte nicht ohnehin einer beruflichen Verschwiegenheit unterliegen, hat der Auftraggeber diesen zur Verschwiegenheit und Geheimhaltung schriftlich zu verpflichten. Die Vorlage dieser Verpflichtungsvereinbarung kann der Auftragnehmer jederzeit verlangen.

(7) Mit der Kontrolle darf kein Wettbewerber des Auftragnehmers beauftragt werden.

### **15 Haftungsbeschränkung**

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen





ersetzt der Auftragnehmer dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

(3) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subunternehmer im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

(4) Die Absätze (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

## 16 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(2) Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarung zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

(3) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt.

Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Artikels 28 DSGVO genügt.

(4) Gerichtsstand für alle Streitigkeiten aus dem Vertragsverhältnis zwischen dem Auftragnehmer und dem Auftraggeber ist der Sitz des Auftragnehmers in **Drochtersen**, sofern beide Parteien Kaufleute i.S.d. HGB, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen sind.

---

Ort, Datum

---

Ort, Datum

---

Unterschrift Auftragnehmer

---

Unterschrift Auftraggeber

## Anlagen

Anlage 1 – Leistungsbeschreibung

Anlage 2 - Beschreibung der Datenkategorien/ Beschreibung der Betroffenen/Betroffenengruppen

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 4 – Genehmigte Subunternehmer





## Anlage 1: Beschreibung der angebotenen Leistungen

Hier fügst du ein:  
Beschreibung der Tätigkeiten des Auftragsverarbeiters.  
Aufzählung mit Auswahlmöglichkeit für den Auftraggeber.

MUSTER



## Anlage 2 Datenkategorien und der gespeicherten Daten

### 1. Art der Daten (Datenkategorie):

Personenstammdaten (Name, Vorname, Adresse)

Kommunikationsdaten (E-Mail, Telefonnummer, Mobilfunknummer)

Rechnungsdaten

Zahlungsdaten

Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

Anonymisierte IP-Adressen

### 2. Zweck der Datenverarbeitung

Vertragsabwicklung zur Erfüllung der bei mir durch den Kunden gebuchten Leistungen – siehe Beschreibung unter Anlage 1

### 3. Betroffene Personen

Webseitenbesucher

Kunden

Kunden meiner Kunden

Lieferanten



## Anlage 3: Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

### 1. Teil

#### Vertraulichkeit

##### 1 Zutrittskontrolle

Das Gebäude befindet sich in einem ländlichen Randgebiet und ist ein privates Wohngebäude/Einfamilienhaus im Eigentum. Die Fenster sind isolierverglast. Es gibt keine Bewegungsmelder, Alarmanlage oder Videoüberwachung. Die Tür ist mit einer normalen Schließanlage versehen. Es gibt keinen Empfang. Besucher werden ausschließlich an der Tür abgeholt. Es wurde ein Audit durchgeführt und festgestellt, dass die Sicherungsmaßnahmen dem Schutzbedarf der Daten entsprechen.

##### 2 Zugangskontrolle

Es gibt keine Server vor Ort. Es wird Microsoft 365 Business eingesetzt.

Das Unternehmen/der Inhaber beschäftigt keine Mitarbeiter und hat somit alleinigen Zugang zu den genutzten Datenverarbeitungssystemen. Folgende Maßnahmen werden umgesetzt:

- Zugang zu dem System erfolgt über eine eindeutige User-ID und ein Passwort
- Eine Passwortrichtlinie ist vorhanden
- Es erfolgt eine Kontosperrung bei fehlerhaften Zugangsversuchen
- Eine Rechtersperre bei vorübergehender Abwesenheit ist aktiv
- Die systemeigene Firewall ist aktiv
- Als Virenschutzprogramm wird Kaspersky Plus eingesetzt
- Das W-LAN ist passwortgeschützt
- Datenverschlüsselung mobiler Endgeräte ist aktiv

Alle Dienstleister werden sorgfältig ausgewählt und überprüft. Der Einsatz von Dienstleistern wird protokolliert.

##### 3 Zugriffskontrolle

Nur der Inhaber selbst hat Zugriff auf die genutzten Datenverarbeitungssysteme. Die Administrationsrechte liegen beim Inhaber und sind somit auf das Notwendigste beschränkt. Nicht mehr verwendete Datenträger werden gemäß Schutzklasse vernichtet. Das bedeutet, dass Datenträger (Festplatten) physisch unbrauchbar gemacht werden. Hierfür gibt es ein Protokoll. Papierunterlagen werden durch einen Aktenvernichter vernichtet.



#### **4 Trennung**

Eine Trennung von Kundendaten ist nicht notwendig, da Kundendaten verschiedener Kunden nicht zeitgleich verarbeitet werden.

#### **5 Pseudonymisierung & Verschlüsselung**

Die Daten werden SSL verschlüsselt. Eine Pseudonymisierung wird nicht durchgeführt, da nach Ablauf der gesetzlichen Löschrufen keine Daten weiterverarbeitet werden.

### **2. Teil**

#### **Integrität**

#### **6 Eingabekontrolle**

Eine Protokollierung über Eingabe, Veränderung oder Löschung von Daten findet nicht statt, da Daten ausschließlich vom Inhaber selbst eingegeben, verändert oder gelöscht werden.

Für E-Mails gilt seit dem 1. Januar 2017 eine besondere Aufbewahrungs- und Archivierungspflicht gemäß GoBD. Nach Beendigung des Vertragsverhältnisses und der gesetzlichen Aufbewahrungsfristen werden die Daten des Auftraggebers/Kunden gelöscht.

#### **7 Weitergabekontrolle**

Die Datenübertragung an den Auftraggeber/Kunden per E-Mail erfolgt über eine SSL-Verschlüsselung. Eine Weitergabe auf externen Datenträgern findet nicht statt. Der Datenaustausch erfolgt digital verschlüsselt, über mit dem Kunden abgestimmte Wege, z.B. Cloud-Services, Projektmanagement-Tools etc.

#### **8 Auftragskontrolle**

Die Sicherheitsmaßnahmen und deren Dokumentation der Auftragnehmer werden vor Auftragsvergabe geprüft. Eine sorgfältige Auswahl von Auftragnehmern ist gewährleistet. Das Vertragsverhältnis mit Auftragnehmern basiert auf Auftragsverarbeitungsverträgen. Es ist sichergestellt, dass nach Beendigung des Auftrages die Daten vernichtet werden. Bei einer längeren Zusammenarbeit wird das Schutzniveau regelmäßig überprüft.

### **3. Teil**

#### **Verfügbarkeit und Belastbarkeit**

Es gibt keine USV. Es sind keine Server im Einsatz. Es gibt eine Rauchmeldeanlage. Es gibt ein Datensicherungs- und Wiederherstellungskonzept. Es gibt einen Notfallplan. Eine rasche



Wiederherstellung ist gewährleistet.

Es wird eine Anti-Viren- und Anti-Schadsoftware eingesetzt. Eine Datensicherung auf externer Festplatte/in einer Cloud wird regelmäßig durchgeführt. Es findet ein Einsatz von webbasierten Tools statt, sowie verschlüsselte Datensicherung mit Cloud-Services.

#### **4. Teil**

#### **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

#### **9 Datenschutzmanagement**

Das Unternehmen/der Inhaber hat die Verantwortung für Datenschutz und Informationssicherheit übernommen. Es ist sichergestellt, dass Anfragen von Betroffenen fristgemäß beantwortet werden. Ein Verzeichnis der Verarbeitungstätigkeiten ist in Bearbeitung. Datenschutz wird im Unternehmen als kontinuierlicher Verbesserungsprozess gesehen und ständig weiterentwickelt.

#### **10 Incident-Response-Management**

Firewall, Spamfilter und Virens Scanner werden eingesetzt und regelmäßig aktualisiert. Diese Aktualisierungen werden auch protokolliert. Es gibt ein eigenes, abgesichertes W-LAN.

#### **11 Privacy by Design/Privacy by Default**

Es werden nicht mehr personenbezogene Daten erhoben, als für die Zweckerfüllung nötig ist. Dies entspricht dem Grundsatz der Datensparsamkeit. Bei der Prozessentwicklung wird darauf geachtet, dass die Rechte der betroffenen Personen möglichst früh berücksichtigt werden. Es findet eine transparente Information der betroffenen Personen statt.



#### Anlage 4 – Genehmigte Subunternehmer

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer im Sinne des Absatz 10:

Hier zählst du alle Subunternehmer auf:

Als Aufbau-Beispiel:

xyz GmbH  
Serverstraße. 25  
12345 Rechenstadt  
Deutschland  
Funktion: Server-Infrastruktur und Backup-Datenspeicher

MUSTER