



## Vereinbarung zur Auftragsverarbeitung

zwischen

[Firma

Adresse]

- Verantwortlicher -

nachstehend *Auftraggeber* genannt

und

[Firma

Adresse]

- Auftragsverarbeiter -

nachstehend *Auftragnehmer* genannt

### 1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

### 2. Gegenstand und Dauer des Auftrags

#### (1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/SLA/ vom \_\_\_\_\_ auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung) / Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

---

---

---

---

---

#### (2) Dauer

Der Auftrag ist unbefristet / befristet bis zum \_\_\_\_\_ erteilt. Er kann von beiden Parteien mit einer Frist von \_\_\_\_\_ gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.



### 3. Durch die Verarbeitung betroffene Personen und Arten der personenbezogenen Daten

(1) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Abonnenten
- Beschäftigte
- Lieferanten
- Handelsvertreter
- Ansprechpartner
- \_\_\_\_\_
- \_\_\_\_\_

(2) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- \_\_\_\_\_
- \_\_\_\_\_

### 4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer nimmt die Datenverarbeitung entsprechend der diesem Auftragsverhältnis zugrundeliegenden Leistungsvereinbarung vor. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich danach und/oder ggf. vom Auftraggeber erteilten ergänzenden Weisungen.

(2) Von Abs. 1 ausgenommen sind Verarbeitungen, zu denen der Auftragnehmer im Rahmen von abweichenden gesetzlichen Regelungen verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.



(4) Der Auftragnehmer soll die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(5) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

### 5. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht im Falle von Datenschutzverletzungen nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer unterstützt den Auftraggeber dabei und bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen.

### 6. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer trifft technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO, die den gesetzlichen Anforderungen genügen. Hierbei sind die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

(2) Der Auftragnehmer ist verpflichtet, die technischen und organisatorischen Maßnahmen an den Stand der Technik anzupassen, soweit dies erforderlich und wirtschaftlich zumutbar ist.



(3) Beauftragt der Auftragnehmer zur Erfüllung seiner vertraglichen Pflichten einen Unterauftragnehmer, stellt er sicher, dass die erforderlichen technischen und organisatorischen Maßnahmen vom Unterauftragnehmer getroffen werden und dem Stand der Technik entsprechen.

#### 7. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist. Er ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte sowie die Beurteilung der Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte im Zusammenhang mit dieser Verarbeitung von Daten im Auftrag gegenüber dem Auftragnehmer geltend machen.

(3) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(5) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(6) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, erfolgt dies schriftlich. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

#### 8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien



getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren. Das Ergebnis von Überprüfungen ist zu dokumentieren.

(2) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen.

#### 9. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Die Berichtigung, Löschung oder Sperrung von Betroffenenendaten gehört nicht zum Inhalt der Leistungsvereinbarung zwischen Auftragnehmer und Auftraggeber. Der Auftragnehmer darf diese Verarbeitungen im gegebenen Falle nur auf konkrete Weisung des Auftraggebers durchführen. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zur Geltendmachung seiner Rechte aus Art. 12-23 DSGVO wendet, leitet der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiter. Das gleiche gilt für Auskunftersuche.

(4) Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

#### 10. Vertraulichkeitsverpflichtung

(1) Beide Parteien verpflichten sich, alle im Rahmen des Vertragsverhältnisses erlangten Informationen, Kenntnisse von Geschäftsgeheimnissen sowie Datensicherheitsmaßnahmen zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.



(3) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht, zur Vertraulichkeit verpflichtet und über die Weisungen des Auftraggebers informiert.

#### 11. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer in seinen Besitz gelangte Unterlagen, Daten und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

(2) Kopien oder Duplikate der Daten werden nicht ohne Wissen des Auftraggebers 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.

#### 12. Vergütung

Etwaige Regelungen über Art und Umfang der Vergütung von Leistungen sind zwischen den Parteien gesondert zu vereinbaren.

#### 13. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

(3) Nebenabreden, Änderungen und Ergänzungen dieses Vertrages und aller seiner Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen der Schriftform.

(4) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

(5) Es gilt deutsches Recht. Gerichtsstand ist \_\_\_\_\_



**Mittelstand 4.0**  
Kompetenzzentrum  
Siegen

\_\_\_\_\_, den \_\_\_\_\_  
Ort Datum

\_\_\_\_\_, den \_\_\_\_\_  
Ort Datum

\_\_\_\_\_  
- Auftraggeber -

\_\_\_\_\_  
- Auftragnehmer -

## Anhang

Hinweis:

Als Anhang kann/sollte eine Übersicht der vereinbarten/zu treffenden TOM angefügt werden.