

Vertrag über eine Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO

der Muster GmbH
 Musterstraße 12
 12345 Musterhausen
 Auftraggeber (im Folgenden „AG“ genannt)

und

der Mensch und Maschine Deutschland GmbH
 Argelsrieder Feld 5
 82234 Wessling
 Auftragnehmer (im Folgenden „AN“ genannt)

alle gemeinsam im Folgenden „Parteien“ genannt.

1. Begriffsdefinitionen

1.1. Personenbezogene Daten sind Informationen im Sinne des Art. 4 Nr. 1 DSGVO.

1.2. Verarbeitung ist jeder Vorgang im Sinne des Art. 4 Nr. 2 DSGVO.

1.3. Weisung ist eine von AG erlassene und an den AN gerichtete Anordnung hinsichtlich der Verarbeitung von personenbezogenen Daten. Bestehende Weisungen (z.B. aus diesem Vertrag) können vom AG durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

2. Gegenstand und Dauer des Auftrags

2.1. Dieser Vertrag regelt den Rahmen der datenschutzrechtlichen Rechte und Pflichten bei der Verarbeitung personenbezogener Daten (im Folgenden „AG-Daten“) durch den AN für den AG in dessen Auftrag und nach dessen Weisungen im Sinne des Art. 28 DSGVO.

2.2. Der Auftragnehmer nutzt die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

2.3. Der AG, oder der jeweilige Auftraggeber des AG, ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er entscheidet über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten.

2.4. Der AN wird AG-Daten entsprechend der Weisungen des AG im Auftrag des AG, unter Einhaltung der organisatorischen und technischen Vorgaben i.S.d. Ziff. 4 verarbeiten. Hierbei verpflichtet sich der AN besonders zu beachten:

- die technischen und organisatorischen Maßnahmen (Ziff. 4)
- die Wahrung der Betroffenenrechte (Ziff. 5)
- die besonderen datenschutzrechtlichen Pflichten (Ziff. 6)
- die Vorgaben zu Unterauftragsverhältnissen (Ziff. 7)
- die Kontrollrechte des AG und eines anderen Verantwortlichen (Ziff. 8)
- die Mitteilungspflichten (Ziff. 9)
- das allgemeinen Weisungsrechts des AG (Ziff. 10)
- die Rückgabe- und Löschpflichten (Ziff. 11)

2.5. Der Vertrag wird auf unbestimmte Zeit geschlossen sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

2.6. Die Parteien können diesen Vertrag jederzeit ohne Einhaltung von Kündigungsfristen aus wichtigem Grund kündigen. Ein wichtiger Grund liegt insbesondere vor,

- wenn ein schwerwiegender Verstoß des AN gegen gesetzliche Vorgaben oder gegen Pflichten aus diesem Vertrag vorliegt.
- wenn der AN eine Weisung des AG missachtet.
- wenn der AN den Zugang des AG, des AG des AG, eines entsprechenden Beauftragten oder einer Datenschutzaufsichtsbehörde zu den Betriebsräumen, in denen AG-Daten aufgrund dieses Vertrages verarbeitet werden, vertrags- oder weisungswidrig verweigert.

3. Umfang, Art und Zweck der vorgesehenen Verarbeitung, Datenarten und Kreis der Betroffenen

3.1. Art der Verarbeitung (Art. 4 Nr. 2 DSGVO):

Unterstützung beim Betrieb der bei uns erworbenen Software, bei Störungen, bei der Installation sowie bei der Ausbildung.

3.2. Art der personenbezogenen Daten (Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

- 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)

3.3. Kategorien betroffener Personen (Art. 4 Nr. 1 DSGVO):

- Kunden

4. Gewährleistung der technischen und organisatorischen Maßnahmen

4.1. Der AN bietet nach Maßgabe des Art. 28 Abs. 1 und 5 DSGVO hinreichende Garantien dafür, dass geeignete technische und organisatorische Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit der DSGVO und den Rechten der Betroffenen steht.

4.2. Der AN trifft geeignete technische und organisatorische Maßnahmen, die den Vorgaben des Art. 32 DSGVO entsprechen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und unterstützt den AG bei der Einhaltung der in Art. 32 DSGVO genannten Pflichten. Der AN unterstützt nach Maßgabe des Art. 28 Abs. 3 f) DSGVO bei den Pflichten des AG gemäß den Artikeln 32 bis 36 DSGVO. Er hat dem AG die erforderlichen Angaben und Dokumente auf Anfrage zur Verfügung zu stellen. Der AN erstellt ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO.

4.3. Sofern die Auftragsverarbeitung vor Ort beim AG, beim Kunden oder per Fernwartung erfolgt, treffen die Pflichten aus dieser Ziffer 4 den AN nur soweit die technischen und organisatorischen Maßnahmen in seinem Machtbereich liegen.

4.4. Die technischen und organisatorischen Maßnahmen unterliegen dem sich fortwährend entwickelnden Stand der Technik. Falls gesetzliche oder vertragliche Regelungen eine Anpassung bzw. Überarbeitung der in der Anlage 1 aufgeführten Maßnahmen des AN erforderlich machen, wird dieser die Maßnahmen auf eigene Kosten unverzüglich anpassen bzw. überarbeiten.

4.5. Kommt trotz entsprechendem Verlangen des AG keine Einigung über die Angemessenheit der technischen und organisatorischen Maßnahmen zustande, kann der AG alle zwischen den Parteien geschlossenen Verträge, die eine Verarbeitung von AG-Daten vorsehen, mit einer Frist von 14 Tagen zum Monatsende kündigen. Die verbleibenden Vertragsbestandteile können gleichermaßen gekündigt werden, wenn das Festhalten an ihnen aufgrund der Kündigung eine unzumutbare Härte für eine Vertragspartei darstellen würde.

5. Betroffenenrechte und Betroffenenklagen

5.1. Der AN erhält die Weisung, dem AG unverzüglich mitzuteilen, wenn ein Betroffener seine Rechte gemäß Art. 15 - 21 DSGVO i.V.m. §§ 34, 35, 36 BDSG geltend macht. Ebenso wird der AN dem AG unverzüglich darüber informieren, wenn ihm eine Klage auf Grundlage des Art. 82 DSGVO zugeht.

5.2. Der AN wird ausschließlich nach Weisung des AG auf Betroffenenanfragen dieser Art reagieren.

5.3. Die Regelungen der Ziffern 5.1 und 5.2 gelten analog bei Anfragen und Prüfungen der Datenschutzaufsichtsbehörden, soweit AG-Daten mindestens mittelbar von solch einer Anfrage oder Prüfung berührt sind.

5.4. Der AN stellt sicher, dass Sperrungen von Daten sowie untersagte Verarbeitungen rechtskonform umgesetzt werden.

6. Besondere datenschutzrechtliche Pflichten des AN

6.1. Vertraulichkeit und Datenschutzschulung: Den mit der Verarbeitung der AG-Daten beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Diese Personen werden bei der Aufnahme ihrer Tätigkeit in geeigneter Weise und nachprüfbar auf Vertraulichkeit verpflichtet. Die Vertraulichkeit muss auch nach Beendigung der Tätigkeit fortbestehen. Soweit andere Geheimhaltungsverpflichtungen (Fernmeldegeheimnis, Sozialgeheimnis, etc.) zu wahren sind, wird der AN seine Beschäftigten entsprechend verpflichten. Der AN wird die an der Verarbeitung beteiligten Personen regelmäßig, jedoch nicht seltener als einmal im Jahr zum Datenschutzrecht schulen.

Der AN hat bei der Auswahl und dem Einsatz der Beschäftigten sicherzustellen, dass diese die gesetzlichen Bestimmungen über den Datenschutz beachten und die aus der Sphäre des AG erlangten Informationen nicht an Dritte weitergeben oder zu einem anderen Zweck als dem Beauftragten verarbeiten (Art. 29 DSGVO).

Der AN wird auf Anforderung für den AG innerhalb von fünf Werktagen einen verifizierbaren Nachweises über die Verpflichtung auf Vertraulichkeit sowie Schulungsnachweise für alle an der Verarbeitung beteiligten Beschäftigten bereitstellen.

6.2. Der AN hat bei der Erstellung und Aktualisierung der Verarbeitungsübersicht der AG mitzuwirken. Dies umfasst nur Verarbeitungstätigkeiten, die im Rahmen der Auftragsverarbeitung für den AG vorgenommen werden.

6.3. Der AN unterstützt den AG gemäß Art. 28 Abs. 3 e) DSGVO mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine Pflichten gegenüber den Betroffenen i.S.d. Kapitel 3 der DSGVO erfüllen kann.

6.4. Beauftragter für den Datenschutz oder Vertreter:

Der AN hat nach Maßgabe des § 38 BDSG i.V.m. Art. 37 DSGVO einen Beauftragten für den Datenschutz benannt und stellt sicher, dass dieser seine Tätigkeit gesetzeskonform ausüben kann.

Eva-Daniela Jung | my-dsb.com UG (haftungsbeschränkt)
Neue Mainzer Straße 6-10 | 60311 Frankfurt am Main
Telefon: +49 172 25 27 359 | E-Mail: jung@my-dsb.com

Soweit der AN seinen Unternehmenssitz außerhalb der EU hat und somit keinen Datenschutzbeauftragten bestellen muss, benennt er einen Vertreter innerhalb der EU nach Maßgabe des Art. 27 DSGVO.

7. Begründung von Unterauftragsverhältnissen (Subunternehmer)

7.1. Dem AN ist es gestattet Subunternehmer zur Erfüllung seiner vertraglichen Pflichten einzusetzen, sofern er den AG rechtzeitig (grundsätzlich 6 Wochen) vor der Datenverarbeitung hierüber informiert (Art. 28 Abs. 2 DSGVO). Zudem muss der AN

dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat (Art. 28 Abs. 1 DSGVO).

7.2. Eine Einsetzung von in Drittländern ansässigen Subunternehmern darf nur erfolgen, wenn zusätzlich die besonderen Voraussetzungen der Art. 44 – 50 DSGVO erfüllt sind.

7.3. Widerspricht der AG nicht innerhalb von 4 Wochen nach Erhalt der Information, akzeptiert er die Einsetzung als genehmigt im Sinne dieses Vertrages. Der AG kann der Einsetzung eines Subunternehmers nur dann widersprechen, wenn dies ansonsten eine objektive Verschlechterung des bestehenden Datenschutzniveaus zur Folge hätte.

7.4. Der AN stellt sicher, dass der Subunternehmer gegenüber dem AN in entsprechender Weise verpflichtet ist, wie der AN gegenüber dem AG nach dieser Vereinbarung verpflichtet ist. Der AN hat die Einhaltung dieser Pflichten des Subunternehmers, insbesondere die Einhaltung der dort vereinbarten technischen und organisatorischen Maßnahmen, vor Beginn der Datenverarbeitung und sodann regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

7.5. Der AN stellt ferner sicher, dass der AG gegenüber dem Subunternehmer die gleichen Kontrollrechte eingeräumt bekommt wie der AG sie gegenüber dem AN selbst hat.

7.6. Der AN haftet gegenüber dem AG dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den AN im Einklang mit 7.3, 7.4 sowie 7.5 vertraglich auferlegt wurden.

7.7. Zurzeit verarbeiten folgende Subunternehmer, personenbezogenen Daten im Auftrag des AN:

- Mensch und Maschine Software SE, Argelsrieder Feld 5, 82234 Wessling (Supporttätigkeiten, Unterstützung Kunde)
- Mensch und Maschine Management AG, Argelsrieder Feld 5, 82234 Wessling (Supporttätigkeiten, Unterstützung Kunde)
- TeamViewer Germany GmbH, Bahnhofsplatz 2, 73033 Göppingen (Fernwartung)

Der AG gestattet den Einsatz dieser Subunternehmer, soweit jeweils die Pflichten aus 7.3, 7.4 sowie 7.5 erfüllt wurden.

8. Kontrollrechte des AG, Mitwirkungs- und Duldungspflichten des AN

8.1. Der AG, der Auftraggeber des AG oder dessen schriftlich Beauftragter haben das Recht, die Befolgung sämtlicher Weisungen und Bestimmungen dieser Vereinbarung durch den AN zu verlangen und nach schriftlicher Vorankündigung von vierzehn (14) Werktagen (mit sachlichem Grund - insbesondere nach Beschwerdefällen auch ohne schriftliche Ankündigung), zu den üblichen Geschäftszeiten zeitlich und räumlich unbeschränkt, auf dem Grundstück und in den Geschäftsräumen des AN zu kontrollieren.

8.2. Dies umfasst insbesondere die Überprüfung der technischen und organisatorischen Maßnahmen vor Beginn der Datenverarbeitung und weitere regelmäßige Überprüfungen, insbesondere der geforderten Datenschutz- und Sicherheitsmaßnahmen.

8.3. Der AN verpflichtet sich entsprechende Überprüfungen zu dulden, Zugang, Auskunft und Einsicht in alle dazu erforderlichen Unterlagen und Datenverarbeitungssysteme zu gewähren.

8.4. Über die Kontrolle und deren Ergebnisse ist ein Protokoll anzufertigen, das vom AG, dem Auftraggeber des AG und AN bzw. deren Beauftragte zu unterzeichnen ist.

9. Mitteilungspflichten des AN

9.1. Der AN wird den AG unverzüglich von jedem Empfang von Anfragen, oder Aufforderungen von einem Betroffenen, oder einer Datenschutzaufsichtsbehörde bezüglich des Gegenstandes dieses Vertrages, insbesondere nach Ziff. 5.3, informieren.

9.2. Dem AN ist bekannt, dass der AG verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und gegebenenfalls der Datenschutzaufsichtsbehörde binnen 72 Stunden und u.U. den Betroffenen unverzüglich zu melden (Art. 33 und 34 DSGVO). Der AN wird den AG bei der Einhaltung dieser Meldepflichten unterstützen. Nimmt der AN Kenntnis von einer Datenschutzverletzung, wird er dies dem AG melden und Informationen gem. den Anforderungen aus Art. 28 Abs. 3 f) DSGVO bereitstellen.

9.3. Mitteilungen nach Ziff. 9.1 und 9.2 müssen unverzüglich, jedoch nicht später als 24 Stunden ab Kenntnisnahme durch den AN, in Textform (z.B. Brief, Telefax oder E-Mail) an den AG übermittelt werden.

10. Weisungsrecht des AG

10.1. Der AN verarbeitet AG-Daten ausschließlich im Rahmen dieser vertraglichen Vereinbarung und weiterer Weisungen des AG.

10.2. Der AG wird weitere Weisungen (fern-)mündlich, per Brief, Fax oder E-Mail erteilen. (fern-)mündlich erteilte Weisungen sind vom AN zu dokumentieren.

10.3. Weisungsberechtigt sind die Geschäftsführer des AG sowie die jeweiligen Kontaktpersonen des AN beim AG.

10.4. Ist der AN der Ansicht, dass eine Weisung gegen die DSGVO oder sonstige Datenschutzvorschriften der Europäischen Union bzw. der Bundesrepublik Deutschland verstößt, weist der AN den AG unverzüglich per Brief, Telefax oder E-Mail darauf hin. Der AN ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie vom AG ausdrücklich bestätigt wird.

10.5. Der AN darf Verarbeitungen von AG-Daten nur dann ohne Weisung des AG durchführen, wenn er aufgrund einer Vorschrift der DSGVO oder einer sonstigen Rechtsvorschrift der Europäischen Union bzw. eines Mitgliedsstaates der Europäischen Union, der der AN unterliegt, hierzu verpflichtet ist. Der AN informiert den AG hierüber bevor er mit der Verarbeitung beginnt, soweit ihm eine solche Mitteilung nicht durch eine anwendbare Rechtsvorschrift untersagt ist.

11. Rückgabe- und Löschungspflichten

11.1. Sofern keine gegenteilige Weisung erteilt wird, hat der AN dem AG bei Beendigung des Auftrags die ihm überlassenen Datenträger und Dokumente herauszugeben.

11.2. Weiterhin sind bei Beendigung des Auftrags vom AN verwendete AG-Daten – wenn nicht bereits zuvor geschehen – zu löschen, zu vernichten oder dem AG zu übergeben.

11.3. Auf Anfrage des AG bestätigt der AN, dass der AN die überlassenen Daten vollständig zurückgegeben, vernichtet bzw. unwiederbringlich gelöscht hat.

11.4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind vom AN für mindestens drei Jahre nach Ende Ihrer Geltungsdauer aufzubewahren. Der AN kann bei Vertragsende die Dokumentationen zu seiner Entlastung dem AG übergeben.

11.5. Die Pflicht zur Löschung bzw. Vernichtung besteht nicht, solange eine gesetzliche Aufbewahrungspflicht entgegensteht.

12. Haftung und Schadensersatz

Es kommen die Regelungen des Art. 82 DSGVO zur Anwendung.

13. Schlussbestimmungen

13.1. Sollte Eigentum des AG beim AN durch Maßnahmen Dritter (z.B. Pfändung, Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet sein, so hat der AN den AG unverzüglich hierrüber in Kenntnis zu setzen. Ein Zurückbehaltungsrecht in Bezug auf Datenträger oder Datenbestände des AG ist ausgeschlossen. Der AN wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim AG als Verantwortlichem im Sinne der DSGVO liegen.

13.2. Die Einrede des Zurückbehaltungsrechts i.S.d. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der dazugehörigen Datenträger ausgeschlossen.

13.3. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des AN – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Die Änderung bzw.

Ergänzung kann auch in einem elektronischen Format (Textform) erfolgen (Art. 28 Abs. 9 DSGVO).

13.4. Diese Vereinbarung hat Vorrang gegenüber allen sonstigen Vereinbarungen soweit diese widersprüchliche Regelungen zum Datenschutz enthalten. Sollte eine der vorliegenden Regelungen unwirksam sein, so berührt dies nicht die Wirksamkeit der übrigen Bestimmungen.

13.5. Die Anlage 1 (Technische und organisatorische Maßnahmen) ist Bestandteil dieses Vertrags.

13.6. Es gilt deutsches Recht.

.....
Ort, Datum

.....
Wessling, den

.....
Auftraggeber

.....
Mensch und Maschine Deutschland GmbH