

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung

zwischen

der Verantwortliche gemäß Art. 4 Nr. 7 DSGVO, nachfolgend "Auftraggeber" genannt
und der

AHB Systeme GmbH
Innstraße 28
68199 Mannheim

eingetragen im Handelsregister des AG Mannheim (HRB 732642), vertreten durch ihren
Geschäftsführer Dr. Wolfgang Zuck, der Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO,
nachfolgend "Auftragnehmer" genannt.

Präambel

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 Datenschutz-Grundverordnung (DSGVO) als Dienstleister ausgewählt. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung im Sinne des Art. 28 DSGVO und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.
- (2) Sofern in diesem Vertrag der Begriff "Datenverarbeitung" oder "Verarbeitung" (von Daten) benutzt wird, wird damit allgemein die Verwendung von personenbezogenen Daten verstanden. Eine Verwendung personenbezogener Daten umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung sowie das Anonymisieren, Pseudonymisieren, Verschlüsseln oder die sonstige Nutzung von Daten.

1. Gegenstand des Auftrags

- (1) Der Auftragnehmer speichert und verarbeitet im Rahmen des mit dem Auftraggeber geschlossenen Vertrages über Online-Zeitwirtschaft (im weiteren "Hauptvertrag" genannt) die von dem Kunden erhobenen und in die Software eingespeisten betrieblichen Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers.
Der Auftrag des Auftraggebers an den Auftragnehmer umfasst dabei folgende Arbeiten und/oder Leistungen:

- a) Verwaltung, Hosting, Betreuung und Wartung der Zeitwirtschaft
- b) Erhebung bzw. Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch den Auftragnehmer für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO in dessen Auftrag und nach dessen Weisung im Zusammenhang mit Personaldaten.

2. Konkretisierung des Auftragsinhalts

- (1) Die Art der durch den Auftragnehmer und seine Subunternehmer vorgenommenen Datenverarbeitung beschränkt sich auf die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, den Abgleich, die Einschränkung, sowie das Löschen. Das Erheben und Erfassen der Daten erfolgt durch den Auftraggeber.
- (2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.
- (3) Der Auftragnehmer erhält Zugriff auf die personenbezogenen Daten, die von dem Auftraggeber über die Software erfasst werden. Dies sind personenbezogene Daten, wie sie in einer Zeitwirtschaft üblicherweise erfasst werden, wie Namen, Personalnummer, Geburtstag, Buchungen, Urlaubsansprüche, Abwesenheiten etc. von Arbeitnehmern. Die Einspeisung genetischer oder biometrischer Daten von natürlichen Personen durch den Auftragnehmer in die Software ist generell unzulässig.
- (4) Der Kreis der betroffenen Personen umfasst jene Personen, deren personenbezogene Daten üblicherweise in einer Zeitwirtschaft erfasst werden, insbesondere Arbeitnehmer sowie Ansprechpartner in Unternehmen. Umfang und Zweck der Datenverarbeitung ergeben sich aus dem Hauptvertrag.

3. Weisungsrecht des Auftraggebers

- (1) Der Auftragnehmer speichert, verarbeitet und nutzt die Daten ausschließlich gemäß den Weisungen des Auftraggebers, sofern keine Ausnahme im Sinne von Absatz (4) oder (5) vorliegt. Die Weisungen werden durch Eingabe in der Software erteilt, sie sind vom Auftragnehmer elektronisch zu dokumentieren.
- (2) Der Auftragnehmer hat dem Auftraggeber die Person(en) und/oder Stellen zu benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind.
Die weisungsempfangsberechtigte Stelle des Auftragnehmers ist:

Hotline der AHB Systeme, 0180 3-242 222, hotline@ahb-systeme.de
- (3) Die Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO obliegt allein dem Auftraggeber.
- (4) Wird der Auftragnehmer auf der Grundlage von deutschem oder europäischem Recht zu einer von den Weisungen abweichenden Verarbeitung verpflichtet (z. B. aufgrund

einer gerichtlichen Anordnung), teilt er dies dem Auftraggeber vor der Verarbeitung mit, sofern ihm eine Mitteilung nicht durch das betreffende Recht untersagt ist.

- (5) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer rechtswidrigen Weisung ablehnen.

4. Technisch-organisatorische Maßnahmen

- (1) Die technischen und organisatorischen Maßnahmen zum Datenschutz sind in Anlage 1 zum Hauptvertrag beschrieben.
- (2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].
- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.
- (4) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen, insbesondere mit Informationen auf der Homepage, sowie mit Auskünften bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 bis 36 DSGVO.

5. Berichtigung, Einschränkung und Löschung von Daten

- (1) Der Auftragnehmer 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 Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- (2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

6. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

- (1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:
- a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird
Dr. Wolfgang Zuck, Geschäftsführer, zuck@ahb-systeme.de, 0621-150202-0 benannt.
 - b) Der Auftragnehmer verpflichtet sich, Daten ausschließlich auf Servern innerhalb der europäischen Union zu speichern und zu verarbeiten.
 - c) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer 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. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.
Der Auftragnehmer und jede dem Auftragnehmer 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.
 - d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
 - e) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
 - f) Der Auftragnehmer 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.
 - g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach 8 dieses Vertrages.

7. Unterauftragsverhältnisse

- (1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder

die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

- (2) Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- (3) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
- (4) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Fa. IONOS SE	Elgendorfer Str. 57, 56410 Montabaur	Daten-Hosting im Rechenzentrum

- (5) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
 - a) der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
 - b) der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
 - c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.
- (6) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- (7) Die Einbeziehung von Unterauftragnehmern außerhalb der Europäischen Union ist ausgeschlossen.
- (8) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Information und Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

8. Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig, mindestens 14 Tage vorher, anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.
- (3) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

9. Mitteilung bei Verstößen des Auftragnehmers

- (1) Der Auftragnehmer unterstützt den Auftraggeber 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. Hierzu gehören u.a.:
 - a) Die 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.
 - b) Die Verpflichtung des Auftragnehmers, 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 mitzuteilen, soweit sie sich auf diesen Auftrag beziehen. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO.
 - c) Die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
 - d) Die Zusicherung des Auftragnehmers, 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 durchführen.

- e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, 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 Auftragnehmer ermittelt.
 - f) 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 Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
 - g) Die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.
- (2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

10. Löschung und Rückgabe von personenbezogenen Daten

- (1) 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.
- (2) Der Auftragnehmer wird mit dem Auftraggeber nach Kündigung des Hauptvertrags oder jederzeit auf dessen Anforderung eine Vereinbarung treffen, ob die Daten bei Beendigung des Hauptvertrages an ihn oder einen Dritten herausgegeben werden sollen oder ob auf eine Herausgabe der Daten verzichtet wird. Nach Beendigung des Hauptvertrages oder jederzeit auf Anforderung des Auftraggebers wird der Auftragnehmer alle ihm überlassenen Daten – sofern keine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen, nachdem die Herausgabe der Daten gemäß Satz 1 erfolgt ist, oder der Auftraggeber auf eine Herausgabe der Daten verzichtet hat. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.
- (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Kündigung, Dauer des Vertrages

- (4) Die Dauer dieses Vertrages ist abhängig von der Dauer des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.
- (5) Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt, einen Unterauftragnehmer bestellen will, gegen dessen Bestellung der Auftraggeber gemäß 7 (3) Einspruch eingelegt hat oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

12. Schlussbestimmungen

- (1) Auf diesen Vertrag findet deutsches Recht Anwendung.
- (2) Gerichtsstand ist Mannheim.
- (3) Änderungen und Ergänzungen dieser Zusatzvereinbarung und aller ihrer Bestandteile bedürfen der Schriftform. Dies gilt auch für den Verzicht auf die Schriftformerfordernis.
- (4) Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam sein oder werden, oder sollte sich in dem Vertrag eine Lücke befinden, so soll hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt werden. Anstelle der unwirksamen Bestimmung oder zur Ausfüllung der Lücke soll eine angemessene Regelung treten, die, soweit rechtlich möglich, dem am nächsten kommt, was die Vertragsparteien gewollt haben oder nach dem Sinn und Zweck dieses Vertrags gewollt haben würden, wenn sie den Punkt bedacht hätten.
- (5) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung oder Beschlagnahmung oder durch sonstige Ereignisse gefährdet sein, hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Der Auftragnehmer weist die Dritten darauf hin, dass die Verantwortlichkeit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

Ort, Datum

Ort, Datum

Auftraggeber

Auftragnehmer (AHB Systeme GmbH)