
Auftragsverarbeitungsvertrag (AVV)

01.08.2026

Zwischen dem Kunden (im Folgenden „**Auftraggeber**“ genannt) und der **MBCOM IT-Systemhaus GmbH**, Königsseer Straße 20, 83471 Berchtesgaden (im Folgenden „**Auftragnehmer**“ genannt) wird gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) folgende Vereinbarung geschlossen.

1. Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem SaaS-Rahmenvertrag für MBCOM ConnectCLOUD (nachfolgend „Hauptvertrag“) sowie weiteren vom Auftraggeber gebuchten Cloud-Dienstleistungen ergeben. Diese Vereinbarung findet Anwendung auf alle Tätigkeiten, die mit der Bereitstellung, dem Betrieb und der Nutzung der MBCOM ConnectCLOUD in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

2. Gegenstand und Dauer des Auftrags

2.1 Gegenstand

Der Gegenstand des Auftrags und damit der Zweck, die Art und der Umfang der Verarbeitung personenbezogener Daten ist die Durchführung der in Anlage 1 (Beschreibung der Verarbeitung und Weisungsberechtigte) näher beschriebenen Aufgaben durch den Auftragnehmer.

Die Verarbeitung der Daten findet grundsätzlich in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Eine Verarbeitung in einem Drittland ist nur nach Maßgabe der besonderen Voraussetzungen der Art. 44 ff. DSGVO und des Abschnitts 7 dieses AVV zulässig. Die eingesetzten Subunternehmer sind in Anlage 2 (Subunternehmer) aufgeführt.

2.2 Dauer

Die Dauer dieser Vereinbarung (Laufzeit) richtet sich nach der Laufzeit des Hauptvertrages. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

3. Konkretisierung des Auftragsinhalts

3.1 Art und Zweck der vorgesehenen Datenverarbeitung

Art der Verarbeitung: Erheben, Erfassen, Ordnen, Speichern, Auslesen, Abfragen, Übermitteln, Abgleichen, Verknüpfen, Einschränken und Löschen personenbezogener Daten, soweit dies für die vereinbarten Leistungen erforderlich ist. Zweck der Verarbeitung: Bereitstellung der SaaS-Plattform „MBCOM ConnectCLOUD“, technischer Support, Integration mit Drittsystemen, Automatisierung von Workflows sowie temporäre Speicherung, Archivierung und Backup im Rahmen des Cloud-Betriebs.

3.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind Daten aus folgenden Datenartenkategorien:

- Personenstammdaten
- Kommunikationsdaten
- Vertragsstammdaten
- Kundenhistorie
- Vertragsabrechnungs- und Zahldaten
- Fernwartungsdaten
- Fernwartungsaufzeichnungen
- Systemdaten
- Inhaltsdaten (z. B. Dokumente aus ERP-/DMS-Systemen, Metadaten)
- Logdaten und Audit-Trails
- Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sowie Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO, soweit solche Daten in den vom Auftraggeber übermittelten Dokumenten oder Datenbeständen enthalten sind und ihre Verarbeitung für die vereinbarten Leistungen erforderlich ist

Der Auftraggeber stellt sicher, dass für die Übermittlung und Verarbeitung von Daten nach Art. 9 oder 10 DSGVO eine Rechtsgrundlage besteht, und weist den Auftragnehmer vorab auf Verarbeitungen hin, die wegen Art, Umfang, Umständen oder Zwecken ein gegenüber der üblichen Leistung erhöhtes Risiko aufweisen. Die Parteien stimmen hierfür erforderliche zusätzliche Schutzmaßnahmen vor Beginn der betreffenden Verarbeitung ab.

3.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Mitarbeiter des Auftraggebers
- Kunden des Auftraggebers
- Interessenten und potenzielle Kunden des Auftraggebers
- Lieferanten des Auftraggebers
- Beschäftigte, Organmitglieder, Ansprechpartner und sonstige Kontaktpersonen der vorgenannten Personengruppen
- Sonstige Personen, deren personenbezogene Daten in den vertragsgemäß verarbeiteten Dokumenten oder Datenbeständen enthalten sind

4. Rechte und Pflichten des Auftraggebers

4.1 Beurteilung der Zulässigkeit

Für die Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, Anfragen von Betroffenen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

4.2 Aufträge und Weisungen

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen schriftlich oder in einem dokumentierten elektronischen Format.

4.3 Überprüfung der TOMs

Der Auftraggeber ist berechtigt, sich wie unter Abschnitt 9 festgelegt, vor Beginn der Datenverarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen.

4.4 Meldung von Fehlern

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

4.5 Informationspflichten

Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4.6 Vertraulichkeit

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

5. Pflichten des Auftragnehmers

5.1 Weisungsgebundene Verarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers, sofern er nicht durch das Recht der Europäischen Union oder eines Mitgliedstaats, dem er unterliegt, zu einer Verarbeitung verpflichtet ist. In diesem Fall teilt der Auftragnehmer dem Auftraggeber die rechtlichen Anforderungen vor der Verarbeitung mit, soweit das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2 Informationspflicht bei Rechtsverstößen

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine vom Auftraggeber erteilte Weisung gegen gesetzliche Vorschriften verstößt.

5.3 Zweckbindung

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

5.4 Kopien und Duplikate

Kopien oder Duplikate der personenbezogenen Daten wird der Auftragnehmer ohne Wissen des Auftraggebers nicht erstellen, außer für Sicherungskopien oder zur Einhaltung gesetzlicher Aufbewahrungspflichten.

5.5 Vertragsgemäße Abwicklung

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu.

5.6 Datentrennung

Der Auftragnehmer sichert zu, dass die für den Auftraggeber verarbeiteten Daten durch wirksame logische Mandantentrennung von sonstigen Datenbeständen getrennt werden. Einzelheiten ergeben sich aus den TOMs.

5.7 Unterstützungspflichten

Bei der Erfüllung der Rechte der betroffenen Personen sowie bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten wird der Auftragnehmer den Auftraggeber auf Anforderung soweit möglich angemessen unterstützen. Dies umfasst insbesondere die Unterstützung bei Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO sowie bei der vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO, soweit dies im Zusammenhang mit der beauftragten Verarbeitung erforderlich ist.

5.8 Wahrung der Vertraulichkeit

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Er stellt sicher, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

6. Mitteilungspflichten bei Störungen und Verletzungen

6.1 Meldepflichten nach Art. 33 DSGVO

Dem Auftragnehmer ist bekannt, dass im Falle von Verletzungen des Schutzes personenbezogener Daten für den Auftraggeber eine Meldepflicht nach Art. 33 DSGVO bestehen kann.

6.2 Mitteilung von Verletzungen

Der Auftragnehmer wird dem Auftraggeber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Bekanntwerden, jede Verletzung des Schutzes personenbezogener Daten (Data Breach) sowie einen hinreichend konkreten Verdacht auf eine solche Verletzung in Textform mitteilen. Zum Zeitpunkt der Erstmeldung noch nicht verfügbare Informationen werden ohne unangemessene Verzögerung schrittweise nachgereicht. Schwerwiegende Betriebsstörungen ohne Bezug zu personenbezogenen Daten werden nach Maßgabe der SLA mitgeteilt.

6.3 Inhalt der Mitteilung

Die Mitteilung muss mindestens folgende Informationen enthalten (Art. 33 Abs. 3 DSGVO):

- Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- Den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- Eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

6.4 Sicherungsmaßnahmen

Der Auftragnehmer trifft unverzüglich angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen.

6.5 Unterstützung bei Meldepflichten

Der Auftragnehmer wird den Auftraggeber bei dessen Meldepflichten gegenüber Aufsichtsbehörden oder Betroffenen (Art. 33, 34 DSGVO) umfassend unterstützen.

7. Unterauftragsverhältnisse mit Subunternehmern

7.1 Definition

Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO zur Vertragserfüllung einzusetzen.

7.2 Liste der Subunternehmer

Eine Liste der bei Vertragsschluss eingesetzten Subunternehmer wird in Anlage 2 (Subunternehmer) zur Verfügung gestellt. Die allgemeine Genehmigung für weitere Subunternehmer gilt nur als erteilt, wenn die nachfolgenden Bestimmungen erfüllt sind.

7.3 Wechsel von Subunternehmern

Der Auftragnehmer hat den Auftraggeber aktiv und in Textform über den geplanten Einsatz eines neuen Subunternehmers mindestens zwei Wochen vor dessen erstmaligem Tätigwerden zu informieren. Der Auftraggeber hat das Recht, innerhalb von zwei Wochen nach Zugang der Information in Textform Einspruch gegen die beabsichtigte Änderung einzulegen. Ein Einspruch darf nur aus wichtigem datenschutzrechtlichem Grund erfolgen. Im Fall des Einspruchs steht dem Auftraggeber ein Sonderkündigungsrecht für den betroffenen Teil der Leistung oder den Hauptvertrag mit einer Frist von einem Monat zum Monatsende zu, sofern der Auftragnehmer die Leistung nicht ohne den geplanten Subunternehmer erbringen kann.

7.4 Auswahl und Prüfung

Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung sicherzustellen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Er muss sich insbesondere zusichern lassen, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen getroffen hat.

7.5 Drittlandstransfer

Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet.

7.6 Weitergabe von Pflichten

Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten bzw. entsprechend weitergegeben werden.

7.7 Vertragsform

Der Vertrag mit dem Unterauftragnehmer muss in Textform abgefasst werden. Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers müssen deutlich voneinander abgegrenzt werden.

7.8 Nachweis der Einhaltung

Der erforderliche Nachweis der Einhaltung der datenschutzrechtlichen Pflichten durch den Subunternehmer kann insbesondere durch Auditberichte, Zertifikate u. Ä. erfolgen.

7.9 Voraussetzungen der Datenweitergabe

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

8. Technisch-organisatorische Maßnahmen

8.1 Risikoorientiertes Schutzniveau

Der Auftragnehmer gewährleistet für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau.

8.2 Ziele der Datensicherheit

Bei den zu treffenden Maßnahmen handelt es sich um Maßnahmen der Datensicherheit im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste.

8.3 Dokumentation und Prüfung

Die in Anlage 3 (TOMs), Version 1.0, Stand 01.08.2026 dokumentierten Maßnahmen stellen die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko dar. Der Auftragnehmer gewährleistet, dass die TOMs jährlich sowie bei wesentlichen Änderungen der Verarbeitungsprozesse auf ihre Wirksamkeit geprüft und ggf. angepasst werden.

8.4 Evaluation der Wirksamkeit

Der Auftragnehmer hat bei gegebenem Anlass eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen durchzuführen.

8.5 Abstimmung organisatorischer Entscheidungen

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

8.6 Fortentwicklung der Maßnahmen

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

9. Kontrollrechte des Auftraggebers

9.1 Durchführung von Kontrollen

Der Auftraggeber ist - grundsätzlich nach Terminvereinbarung - berechtigt, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit beim Auftragnehmer im angemessenen und erforderlichen Umfang selbst oder durch Dritte zu kontrollieren.

9.2 Rücksichtnahme auf Betriebsabläufe

Der Auftraggeber wird Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers nicht unverhältnismäßig zu stören.

9.3 Unterstützungspflicht

Der Auftragnehmer sichert zu, dass er bei diesen Kontrollen unterstützend mitwirkt. Er wird dem Auftraggeber auf Anforderung die erforderlichen Auskünfte erteilen und die Umsetzung der TOMs nachweisen.

9.4 Vergütung von Kontrollen

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer eine angemessene Vergütung nach tatsächlichem Aufwand zu dem im angenommenen Angebot genannten Standard-Stundensatz verlangen, sofern die Kontrolle anlasslos erfolgt und im laufenden Kalenderjahr bereits eine Kontrolle stattgefunden hat. Ist dort kein einschlägiger Stundensatz genannt, wird der Aufwand nur nach vorheriger Vereinbarung des Stundensatzes in Textform berechnet. Kontrollen aufgrund eines vom Auftragnehmer zu vertretenden Datenschutzverstoßes werden nicht berechnet.

10. Berechtigung, Einschränkung und Löschung von Daten

10.1 Weisungsgebundene Korrekturen

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken.

10.2 Weiterleitung von Anfragen

Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

11. Verpflichtungen nach Beendigung des Auftrags

11.1 Rückgabe oder Löschung

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer nach Wahl des Auftraggebers sämtliche in seinen Besitz gelangten personenbezogenen Daten sowie alle im Zusammenhang mit dem Auftragsverhältnis erstellten Kopien oder Duplikate zurückzugeben oder datenschutzgerecht zu löschen bzw. zu vernichten. Bei Vertragsbeendigung gelten für Rückgabe, Abruf und produktive Löschung die Fristen der Datenexport-, Exit- und Löschregelung; die Löschung erfolgt unmittelbar nach Ablauf der dort vorgesehenen Abruffrist, sofern der Auftraggeber nicht eine frühere Löschung verlangt. Backup-Kopien werden spätestens 90 Tage nach der produktiven Löschung durch den regulären Rotationszyklus überschrieben, sind bis dahin gesperrt und werden nur zur Wiederherstellung nach einem Sicherheits- oder Verfügbarkeitsvorfall verarbeitet.

11.2 Bestätigung der Löschung

Die Löschung bzw. Vernichtung ist dem Auftraggeber unaufgefordert mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

11.3 Gesetzliche Aufbewahrungspflichten

Gesetzliche Aufbewahrungspflichten des Auftragnehmers bleiben unberührt. Zurückbehaltene Daten werden für andere Verarbeitungen gesperrt und nach Wegfall der Aufbewahrungspflicht gelöscht.

12. Haftung

Eine zwischen den Parteien im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, es sei denn, es ist ausdrücklich etwas anderes vereinbart.

13. Schlussbestimmungen

13.1 Schriftformerfordernis

Änderungen und Ergänzungen dieser Vereinbarung bedürfen einer Vereinbarung in Textform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist.

13.2 Rangfolge

Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung einschließlich ihrer Anlagen den Regelungen des Hauptvertrages vor. Die Datenexport-, Exit- und Löschregelung konkretisiert die Rückgabe- und Löschfristen nach Abschnitt 11.1; im Übrigen gehen innerhalb dieser Vereinbarung die Anlagen dem Vertragstext vor.

13.3 Rechtswahl

Es gilt deutsches Recht unter Ausschluss des materiellen internationalen Privat- sowie Kollisionsrechts.

13.4 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein, bleibt davon die Wirksamkeit dieser Vereinbarung im Übrigen unberührt.

13.5 Geltung der AGB

Nachrangig zu den Regelungen dieser Vereinbarung gelten die bei Abschluss des Hauptvertrages wirksam einbezogenen allgemeinen Geschäftsbedingungen von MBCOM in der jeweils vereinbarten Fassung.