

Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO

Fassung 2.6 · Stand 15.10.2026

Vertragsparteien

Zwischen dem Auftraggeber als Verantwortlichem und der KHTC-Consulting GmbH als Auftragsverarbeiter wird folgender Vertrag zur Auftragsverarbeitung (AVV) geschlossen.

Angabe	Auftraggeber (Verantwortlicher)	Auftragnehmer (Auftragsverarbeiter)
Firma		KHTC-Consulting GmbH
Anschrift		Basbecker Straße 7, 21769 Lamstedt
Handelsregister		Amtsgericht Tostedt, HRB 208097
Vertreten durch		Paul Kohlstock, Patrick Heilmann (Geschäftsführer)
Kontakt Datenschutz		info@khtc-consulting.de, Tel. 04773 2110

Nachfolgend „Auftraggeber“ und „Auftragnehmer“, gemeinsam „Parteien“.

Präambel

Der Auftragnehmer berät und betreut den Auftraggeber in den Bereichen Telekommunikation und Digitalisierung auf Grundlage eines oder mehrerer Verträge, Aufträge oder Servicevereinbarungen (jeweils „Hauptvertrag“). Soweit er dabei personenbezogene Daten im Auftrag des Auftraggebers verarbeitet, regelt dieser AVV die Rechte und Pflichten der Parteien nach Art. 28 der Datenschutz-Grundverordnung (DSGVO).

Der AVV gilt für alle bestehenden und künftigen Hauptverträge zwischen den Parteien, ohne dass er neu abgeschlossen werden muss.

§ 1 Gegenstand, Geltungsbereich und Laufzeit

(1) Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers bei Erbringung der im Hauptvertrag vereinbarten Leistungen. Die Leistungen sind in Anlage 1 als Leistungsmodule beschrieben. Es gelten jeweils die Module, die der Auftraggeber beauftragt hat.

(2) Dieser AVV gilt nicht, soweit der Auftragnehmer personenbezogene Daten als eigener Verantwortlicher verarbeitet. Das betrifft insbesondere Anbahnung, Abschluss, Abrechnung und Verwaltung des Vertragsverhältnisses, die Kommunikation mit den Ansprechpartnern des Auftraggebers sowie die Vermittlung neuer Verträge, Vertragsverlängerungen und Anbieterwechsel als Vertriebspartner von Netzbetreibern und Anbietern einschließlich der Übermittlung der Auftragsdaten an diese und der Provisionsabrechnung. Hierfür darf der Auftragnehmer Vertrags- und Bestandsdaten aus den Modulen A und B verwenden, soweit der Auftraggeber ihn mit der Vermittlung beauftragt. Insoweit gilt die Datenschutzerklärung des Auftragnehmers.

(3) Netzbetreiber und Anbieter von Telekommunikations-, Cloud- und Softwarediensten, mit denen der Auftraggeber eigene Verträge geschlossen hat, sind keine Unterauftragsverarbeiter des Auftragnehmers. Übermittelt der Auftragnehmer Daten auf Weisung an diese Vertragspartner des Auftraggebers, etwa für Bestellungen, Portierungen, Anbieterwechsel, Kündigungen oder Störungsmeldungen, handelt er im Namen und auf Weisung des Auftraggebers.

(4) Der AVV beginnt mit seinem Abschluss und läuft, solange der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Er endet nicht vor dem letzten Hauptvertrag. Pflichten zu Vertraulichkeit, Löschung und Rückgabe gelten fort, solange dem Auftragnehmer Daten des Auftraggebers vorliegen.

(5) Das Recht zur außerordentlichen Kündigung bleibt unberührt. Ein wichtiger Grund liegt insbesondere bei einem schwerwiegenden Verstoß gegen diesen AVV oder gegen Datenschutzvorschriften vor. Wer diesen AVV aus wichtigem Grund kündigt, kann zugleich die Hauptverträge kündigen, soweit deren Erfüllung eine Verarbeitung im Auftrag erfordert.

(6) Begriffe wie „personenbezogene Daten“, „Verarbeitung“ oder „Verantwortlicher“ werden im Sinne von Art. 4 DSGVO verwendet.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen sind je Leistungsmodul in Anlage 1 beschrieben. Einzelheiten ergeben sich aus dem Hauptvertrag sowie aus Angeboten, Auftragsbestätigungen und Leistungsbeschreibungen (jeweils „Einzelauftrag“).

(2) Eine planmäßige Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO ist nicht vorgesehen. Inhalte von Gesprächen, E-Mails und Dokumenten können solche Daten im Einzelfall enthalten. Will der Auftraggeber solche Daten gezielt verarbeiten lassen, teilt er dies vorher in Textform mit; die Parteien vereinbaren dann ergänzende Schutzmaßnahmen.

(3) Die Verarbeitung findet grundsätzlich in der Europäischen Union oder im Europäischen Wirtschaftsraum statt. Eine Verarbeitung in einem Drittland, auch durch Unterauftragsverarbeiter oder durch Zugriff aus einem Drittland, erfolgt nur unter den Voraussetzungen der Art. 44 ff. DSGVO (§ 6 Abs. 7, Anlage 3).

(4) Beschäftigte des Auftragnehmers dürfen Daten auch außerhalb der Geschäftsräume verarbeiten, etwa im Außendienst oder im Homeoffice, sofern die Maßnahmen nach Anlage 2 eingehalten werden.

§ 3 Weisungen des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, auch bei Übermittlungen an ein Drittland oder eine internationale Organisation (Art. 28 Abs. 3 lit. a DSGVO). Ausgenommen sind Verarbeitungen, zu denen ihn das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, verpflichtet. In diesem Fall teilt er dem Auftraggeber die rechtlichen Anforderungen vorher mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die anfänglichen Weisungen ergeben sich aus diesem AVV, dem Hauptvertrag und dem Einzelauftrag. Weitere Weisungen erteilt der Auftraggeber in Textform, etwa per E-Mail oder Service-Ticket. Mündliche Weisungen dokumentiert der Auftragnehmer unverzüglich im Service-Ticket; der Auftraggeber kann diese Dokumentation auf Anfrage einsehen.

(3) Weisungsempfänger beim Auftragnehmer sind die Geschäftsführer und die benannten Ansprechpartner im Service (support@khtc-consulting.de). Weisungsberechtigt sind die gesetzlichen Vertreter des Auftraggebers und die von ihm benannten Personen. Der Auftragnehmer darf Weisungen von Beschäftigten des Auftraggebers ausführen, die erkennbar im Rahmen des beauftragten Leistungsumfangs liegen, solange der Auftraggeber nichts anderes mitteilt. Ausgenommen sind die Herausgabe oder Auswertung von Verbindungsdaten, Einzelverbindungsnachweisen, Gesprächsaufzeichnungen und Standortdaten, die Ortung und Fernlöschung von Geräten sowie Änderungen von Berechtigungen; diese erfolgen nur auf Weisung einer weisungsberechtigten Person.

(4) Hält der Auftragnehmer eine Weisung für datenschutzwidrig, informiert er den Auftraggeber unverzüglich (Art. 28 Abs. 3 UAbs. 2 DSGVO). Er darf die Ausführung aussetzen, bis der Auftraggeber die Weisung bestätigt oder ändert. Offensichtlich rechtswidrige Weisungen führt er nicht aus.

(5) Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, behandeln die Parteien als Wunsch nach Leistungsänderung. Der Auftragnehmer kann ihre Ausführung von einer gesonderten Vereinbarung abhängig machen.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet die Daten nur im Rahmen der Weisungen und für die vereinbarten Zwecke. Er nutzt sie nicht für eigene Zwecke, insbesondere nicht zum Training von KI-Modellen, und verpflichtet seine Unterauftragsverarbeiter entsprechend. An Dritte gibt er Daten nur nach § 6 oder auf Weisung weiter.

(2) Er stellt sicher, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Die Verpflichtung gilt über das Ende der Tätigkeit hinaus. Soweit Beschäftigte Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation erhalten, verpflichtet er sie zusätzlich auf das Fernmeldegeheimnis (§ 3 TDDDG).

(3) Er trifft die technischen und organisatorischen Maßnahmen nach § 5 und Anlage 2 (Art. 28 Abs. 3 lit. c, Art. 32 DSGVO).

(4) Er hält die Bedingungen für Unterauftragsverarbeiter nach § 6 ein (Art. 28 Abs. 3 lit. d DSGVO) und unterstützt den Auftraggeber nach § 7 und § 8 (Art. 28 Abs. 3 lit. e und f DSGVO).

(5) Er führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

(6) Er benennt einen Datenschutzbeauftragten, soweit Art. 37 DSGVO oder § 38 BDSG dies verlangen, und teilt dem Auftraggeber dessen Kontaktdaten mit. Ist keiner zu benennen, ist die Geschäftsführung Ansprechpartner für Datenschutzfragen (info@khtc-consulting.de).

(7) Kopien der Daten erstellt er nur, soweit dies für die Leistung erforderlich ist, insbesondere für Datensicherungen, oder gesetzliche Aufbewahrungspflichten es verlangen.

(8) Systeme des Auftraggebers, etwa Verwaltungsportale der Telefonanlage, Kundenkonten bei Netzbetreibern, die Verwaltung des Mobile-Device-Managements (MDM) oder von Microsoft 365, nutzt er nur mit den eingeräumten Rechten und nur im erforderlichen Umfang. Partnerzugänge des Auftragnehmers bei Herstellern und Anbietern nutzt er für Daten des Auftraggebers nur im Rahmen dieses AVV.

(9) Er informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen einer Aufsichtsbehörde, die diesen AVV betreffen. Gleiches gilt für Ermittlungen und Auskunftersuchen von Behörden zu Daten des Auftraggebers, soweit eine Information rechtlich zulässig ist.

(10) Ist der Auftraggeber Berufsgeheimnisträger nach § 203 StGB, wirkt der Auftragnehmer als sonstige mitwirkende Person im Sinne von § 203 Abs. 3 Satz 2 StGB mit. Er nimmt von fremden Geheimnissen nur Kenntnis, soweit die Leistung es erfordert, und wahrt sie. Er ist hiermit zur Geheimhaltung verpflichtet und auf die Strafbarkeit nach § 203 Abs. 4 StGB hingewiesen; von ihm herangezogene Personen verpflichtet er ebenfalls zur Geheimhaltung.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO). Er berücksichtigt dabei den Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie das Risiko für die Rechte und Freiheiten der betroffenen Personen.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie durch gleichwertige oder bessere Maßnahmen ersetzen, ohne das vereinbarte Schutzniveau zu unterschreiten. Wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber auf Anfrage mit.

(3) Er überprüft die Wirksamkeit der Maßnahmen regelmäßig, mindestens einmal im Kalenderjahr, sowie bei wesentlichen Änderungen der Verarbeitung.

§ 6 Unterauftragsverarbeiter und Drittlandübermittlung

- (1) Der Auftraggeber erteilt die allgemeine schriftliche Genehmigung, weitere Auftragsverarbeiter („Unterauftragsverarbeiter“) einzusetzen (Art. 28 Abs. 2 DSGVO). Die in Anlage 3 aufgeführten Unterauftragsverarbeiter gelten mit Abschluss dieses AVV als genehmigt. Einem Leistungsmodul zugeordnete Unterauftragsverarbeiter werden nur eingesetzt, wenn der Auftraggeber dieses Modul beauftragt.
- (2) Im Einzelauftrag ausdrücklich benannte Unterauftragsverarbeiter, etwa die Plattform eines Mobile-Device-Managements oder ein Dienstleister für die zertifizierte Datenlöschung von Altgeräten, gelten mit Erteilung des Einzelauftrags als genehmigt.
- (3) Will der Auftragnehmer einen Unterauftragsverarbeiter hinzuziehen oder ersetzen, informiert er den Auftraggeber mindestens 30 Tage vorher in Textform, etwa per E-Mail. Kündigt der Unterauftragsverarbeiter eine Änderung kürzer an, informiert er unverzüglich nach eigener Kenntnis. Der Auftraggeber kann innerhalb von 14 Tagen nach Zugang aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Ohne fristgerechten Widerspruch gilt die Änderung als genehmigt; auf Frist und Folge weist der Auftragnehmer in der Mitteilung hin.
- (4) Widerspricht der Auftraggeber, erbringt der Auftragnehmer die betroffene Leistung ohne den neuen Unterauftragsverarbeiter oder bietet eine zumutbare Alternative an. Ist beides nicht möglich, kann jede Partei die betroffene Leistung zum Zeitpunkt des geplanten Einsatzes in Textform kündigen.
- (5) Erfordern die Abwehr einer Gefahr für die Datensicherheit oder der Wegfall eines Unterauftragsverarbeiters einen kurzfristigen Wechsel, darf der Auftragnehmer ihn nach vorheriger Information des Auftraggebers in Textform vornehmen. Soweit möglich, setzt er bis zum Ablauf der Widerspruchsfrist bereits genehmigte Unterauftragsverarbeiter ein; Absatz 4 gilt entsprechend.
- (6) Der Auftragnehmer erlegt Unterauftragsverarbeitern vertraglich im Wesentlichen dieselben Datenschutzpflichten auf wie in diesem AVV, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Bei standardisierten Diensten genügen deren Auftragsverarbeitungsbedingungen, wenn sie Art. 28 Abs. 3 DSGVO entsprechen und ein gleichwertiges Schutzniveau gewährleisten; Fristen dieses AVV laufen insoweit ab Kenntnis des Auftragnehmers. Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für deren Einhaltung wie für eigenes Verschulden; es gilt § 12.
- (7) Übermittlungen in ein Drittland erfolgen nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Grundlage ist insbesondere ein Angemessenheitsbeschluss der EU-Kommission, etwa das EU-US Data Privacy Framework für dort zertifizierte Empfänger, oder die Standardvertragsklauseln der EU-Kommission. Die jeweilige Grundlage ist in Anlage 3 angegeben.
- (8) Keine Unterauftragsverarbeitung sind Nebenleistungen ohne planmäßigen Zugriff auf Daten des Auftraggebers, etwa reine Transport- und Telekommunikationsleistungen, Post- und Kurierdienste oder Hardwarewartung ohne Datenzugriff. Der Auftragnehmer trifft auch hierfür angemessene Schutzvorkehrungen.

§ 7 Betroffenenrechte und Unterstützung

- (1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen nach Kapitel III DSGVO (Art. 28 Abs. 3 lit. e DSGVO). Das betrifft insbesondere Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch.
- (2) Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet er das Anliegen unverzüglich an den Auftraggeber weiter. Er beantwortet es nur auf Weisung des Auftraggebers.
- (3) Er unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen bei den Pflichten aus Art. 32 bis 36 DSGVO (Art. 28 Abs. 3 lit. f DSGVO). Dazu gehören insbesondere Datenschutz-Folgenabschätzungen und vorherige Konsultationen der Aufsichtsbehörde.
- (4) Für Unterstützung nach diesem Paragraphen und für Kontrollen nach § 9, die nicht auf einem Verstoß des Auftragnehmers beruhen, kann der Auftragnehmer nach vorheriger Ankündigung eine angemessene Vergütung seines Aufwands verlangen, soweit dieser zwei Stunden je Kalenderjahr übersteigt.

§ 8 Meldung von Datenschutzverletzungen

- (1) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten, die Daten des Auftraggebers betrifft, unverzüglich nach Kenntnis (Art. 33 Abs. 2 DSGVO), möglichst innerhalb von 24 Stunden, spätestens nach 48 Stunden. Die Meldung erfolgt in Textform an den nach § 10 Abs. 4 benannten Ansprechpartner; bei voraussichtlich hohem Risiko ruft der Auftragnehmer zusätzlich an.
- (2) Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, Name und Kontaktdaten einer Anlaufstelle für weitere Informationen, wahrscheinliche Folgen sowie ergriffene und vorgeschlagene Maßnahmen. Fehlende Angaben reicht der Auftragnehmer unverzüglich nach.
- (3) Er ergreift unverzüglich die erforderlichen Maßnahmen, um die Daten zu sichern und nachteilige Folgen zu mindern, und stimmt sie soweit möglich mit dem Auftraggeber ab.
- (4) Meldungen an die Aufsichtsbehörde und Benachrichtigungen betroffener Personen nach Art. 33 und 34 DSGVO obliegen dem Auftraggeber. Der Auftragnehmer nimmt sie nur auf Weisung vor.
- (5) Absatz 1 gilt entsprechend für den hinreichend konkreten Verdacht einer solchen Verletzung und für Verletzungen bei Unterauftragsverarbeitern, sobald der Auftragnehmer davon Kenntnis erhält.

§ 9 Nachweise und Kontrollrechte

- (1) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO erforderlich sind (Art. 28 Abs. 3 lit. h DSGVO). Als Nachweis genügen in der Regel aktuelle Selbstauskünfte, die Dokumentation der Maßnahmen nach Anlage 2 sowie Zertifikate und Prüfberichte der Unterauftragsverarbeiter.
- (2) Der Auftraggeber darf Überprüfungen einschließlich Inspektionen selbst oder durch einen beauftragten Prüfer durchführen; der Auftragnehmer ermöglicht sie und wirkt daran mit. Der Prüfer darf kein Wettbewerber des Auftragnehmers sein und ist zur Verschwiegenheit zu verpflichten.
- (3) Vor-Ort-Kontrollen sind mindestens 14 Tage vorher anzukündigen, finden während der Geschäftszeiten statt und dürfen den Betrieb nicht unverhältnismäßig stören. Ohne konkreten Anlass sind sie höchstens einmal je Kalenderjahr zulässig. Rechte der Aufsichtsbehörden bleiben unberührt.
- (4) Jede Partei trägt die eigenen Kosten einer Kontrolle; § 7 Abs. 4 bleibt unberührt.

§ 10 Pflichten des Auftraggebers

- (1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, einschließlich der Zulässigkeit der Übermittlung an den Auftragnehmer und der Wahrung der Betroffenenrechte. Er informiert die betroffenen Personen, insbesondere seine Beschäftigten, nach Art. 13 und 14 DSGVO.
- (2) Nutzt der Auftraggeber Gesprächsaufzeichnung, Transkription, KI-Gesprächszusammenfassungen, Einzelverbindungsnachweise, Anrufstatistiken je Beschäftigtem oder die Ortung von Geräten, stellt er die Rechtsgrundlage dafür sicher. Dazu gehören insbesondere die Einwilligung aller Gesprächsteilnehmer vor einer Aufzeichnung (§ 201 StGB), bei Einzelverbindungsnachweisen die Erklärung gegenüber dem Netzbetreiber nach § 11 Abs. 3 TDDDG und, falls ein Betriebs- oder Personalrat besteht, dessen Beteiligung (§ 87 Abs. 1 Nr. 6 BetrVG oder Personalvertretungsrecht). Der Auftragnehmer weist auf ihm bekannte Bedenken hin.
- (3) Er informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.
- (4) Er benennt einen Ansprechpartner für Datenschutzfragen und teilt Änderungen unverzüglich mit.
- (5) Er räumt dem Auftragnehmer nur die Zugriffsrechte ein, die für die beauftragten Leistungen erforderlich sind.

§ 11 Löschung und Rückgabe

- (1) Nach Abschluss der Leistungen oder auf Verlangen des Auftraggebers löscht der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten des Auftraggebers oder gibt sie zurück und löscht danach die vorhandenen Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Pflicht zur Speicherung besteht (Art. 28 Abs. 3 lit. g DSGVO). Die Rückgabe erfolgt in einem gängigen, maschinenlesbaren Format.
- (2) In den Produktivsystemen löscht der Auftragnehmer innerhalb von 30 Tagen nach Vertragsende oder Zugang des Verlangens. Kopien in Datensicherungen werden mit Ablauf des Sicherungszyklus gelöscht, spätestens nach sechs Monaten; archivierte E-Mails, die gesetzlichen Aufbewahrungspflichten unterliegen (§ 257 HGB, § 147 AO), mit Ablauf dieser Fristen. Bis dahin bleiben sie gesperrt und werden nicht weiter verarbeitet.
- (3) Dokumentationen zum Nachweis der ordnungsgemäßen Verarbeitung darf der Auftragnehmer bis zum Ende der regelmäßigen Verjährungsfrist (§§ 195, 199 BGB) aufbewahren, Unterlagen mit gesetzlichen Aufbewahrungspflichten bis zum Ablauf der jeweiligen Frist.
- (4) Daten in Systemen, die der Auftraggeber aufgrund eigener Verträge nutzt, etwa seiner Telefonanlage oder seinem Microsoft-365-Mandanten, bleiben dort. Der Auftragnehmer gibt bei Vertragsende seine Zugriffsrechte auf diese Systeme auf oder lässt sie entfernen.
- (5) Der Auftragnehmer bestätigt die Löschung auf Verlangen in Textform. Für zurückgenommene Altgeräte erhält der Auftraggeber einen Löschnachweis (Anlage 1, Modul D).

§ 12 Haftung

- (1) Gegenüber betroffenen Personen haften die Parteien nach Art. 82 DSGVO.
- (2) Hat eine Partei nach Art. 82 Abs. 4 DSGVO vollständigen Schadenersatz geleistet, kann sie von der anderen Partei den Teil zurückfordern, der deren Anteil an der Verantwortung für den Schaden entspricht (Art. 82 Abs. 5 DSGVO).
- (3) Im Übrigen, auch im Fall des § 6 Abs. 6, gelten die Haftungsregelungen des Hauptvertrags; § 13 Abs. 3 gilt insoweit nicht. Enthält der Hauptvertrag keine Regelung, haftet der Auftragnehmer unbeschränkt bei Vorsatz, grober Fahrlässigkeit und Verletzung von Leben, Körper oder Gesundheit. Bei leicht fahrlässiger Verletzung wesentlicher Vertragspflichten haftet er nur für den vertragstypischen, vorhersehbaren Schaden; im Übrigen ist die Haftung für leichte Fahrlässigkeit ausgeschlossen.

§ 13 Schlussbestimmungen

- (1) Dieser AVV kommt durch Unterzeichnung beider Parteien zustande, auch in einem elektronischen Format, etwa per Docusign (Art. 28 Abs. 9 DSGVO). Er wird außerdem Bestandteil eines Hauptvertrags, wenn dieser oder ein Einzelauftrag auf eine bestimmte Fassung dieses AVV verweist und der Auftraggeber in Textform annimmt.
- (2) Änderungen und Ergänzungen bedürfen der Textform; § 305b BGB bleibt unberührt. Maßgeblich ist die bei Vertragsschluss vereinbarte Fassung. Spätere Fassungen gelten nur nach Zustimmung des Auftraggebers in Textform; Anlage 3 ändert sich nach § 6. Alle Fassungen bleiben unter khtc-consulting.de/avv/ abrufbar.
- (3) Bei Widersprüchen zwischen diesem AVV und anderen Vereinbarungen der Parteien geht in Fragen des Datenschutzes dieser AVV vor.
- (4) Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam. An ihre Stelle treten die gesetzlichen Vorschriften.
- (5) Es gilt deutsches Recht. Ist der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist Gerichtsstand der Sitz des Auftragnehmers.
- (6) Die Anlagen 1 bis 3 sind Bestandteil dieses AVV.

Unterschriften

Angabe	Auftraggeber	Auftragnehmer
Firma		KHTC-Consulting GmbH
Ort, Datum		Lamstedt,
Name, Funktion		
Unterschrift	Auftraggeber	KHTC-Consulting GmbH

Bitte das unterschriebene Exemplar an info@khtc-consulting.de senden. Sie erhalten das von uns gegengezeichnete Exemplar zurück. Auf Wunsch senden wir den AVV auch zur elektronischen Unterschrift per DocuSign.

Anlage 1 – Leistungsmodule, Datenarten und betroffene Personen

Es gelten nur die Module, die der Auftraggeber beauftragt hat (§ 1 Abs. 1). Die Buchstaben werden in Anlage 3 verwendet.

Modul	Zweck	Gegenstand der Verarbeitung	Arten personenbezogener Daten	Betroffene Personen
A – Mobilfunk, Internet und IoT/M2M	Verwaltung und Optimierung der Mobilfunk-, Internet- und IoT-Verträge	Bestandsaufnahme und Verwaltung von Verträgen, Anschlüssen, SIM-Karten und Rufnummern; Bestellungen, Vertragsänderungen und Portierungen im Auftrag, soweit keine Vermittlung nach § 1 Abs. 2 vorliegt	Namen, dienstliche Kontaktdaten und Kostenstellen der Nutzer; Rufnummern, SIM-/eSIM-Kennungen (ICCID), Gerätekennungen (IMEI); Tarif- und Vertragsdaten; Vollmachten und Unterschriften; Lieferanschriften	Beschäftigte und sonstige Nutzer des Auftraggebers; Ansprechpartner des Auftraggebers
B – Service und Vertragsmanagement	Bearbeitung von Störungen, Fristen, Kündigungen und Rechnungen	Service-Tickets, Störungsmanagement und Eskalation bei Anbietern; Fristenwacht; Kündigungs- und Wechselschreiben im Auftrag; Rechnungsprüfung mit Reklamation (zubuchbar); soweit beauftragt KI-gestützte Auswertung von Rechnungen und Tickets; Fernwartung im Einzelfall mit Zustimmung des Auftraggebers	Inhalte von Anfragen und Tickets, Kontaktdaten der Melder, Screenshots und Fehlerprotokolle; Rechnungs- und Verbrauchsdaten, für die Prüfung auch Verkehrsdaten aus Einzelverbindungen nachweisen; bei Fernwartung die angezeigten Daten	Beschäftigte und Nutzer des Auftraggebers; deren Kommunikationspartner; Dritte, deren Daten in Anfragen enthalten sind
C – Cloud-Telefonie und Telefonie-Integration	Betrieb, Verwaltung und Integration der Telefonie	Einrichtung, Migration und Administration der Telefonanlage (Nebenstellen, Rufnummern, Gruppen, Warteschlangen, Zeitsteuerungen, Ansagen, Telefonbücher) über Portale und Schnittstellen des Anbieters; Konfigurationssicherungen und Dokumentation der Anrufverteilung. Soweit beauftragt: Kontaktabgleich aus dem CRM, CTI- und CRM-Integration (KHTC Powertools), Browser- und App-Telefonie über das Gateway des Auftragnehmers, Anrufjournal und Anrufstatistiken, Gesprächsaufzeichnung, Transkription und KI-Zusammenfassung	Namen, Durchwahlen, E-Mail-Adressen und Weiterleitungsziele der Nutzer, auch Mobilnummern; Geräte- und Konfigurationsdaten; Telefonbuch- und CRM-Kontaktdaten; Verbindungsdaten (Rufnummern, Zeitpunkt, Dauer, Richtung, Status); Sprachnachrichten und Faxe im Störfall; soweit beauftragt Gesprächsinhalte (Audio, Transkript, Zusammenfassung)	Beschäftigte des Auftraggebers; Anrufer und Gesprächspartner wie Kunden, Lieferanten und Interessenten; Personen im Telefonbuch oder CRM
D – Hardware und Mobile-Device-Management	Bereitstellung, Absicherung und Rücknahme von Geräten	Beschaffung und Zero-Touch-Bereitstellung von Geräten (Apple Business Manager, Android Enterprise); Betrieb des MDM mit Richtlinien, App-Verteilung, Fernsperrung und Fernlöschung im Verlustfall; Neuzuweisung; Rücknahme und zertifizierte Datenlöschung von Altgeräten mit Löschnachweis	Namen und dienstliche Kontaktdaten der Nutzer; Geräte- und Inventardaten (Seriennummer, IMEI, Modell, Betriebssystem, dienstliche Apps, Sicherheitsstatus); Standortdaten nur bei aktivierter Ortung im Verlustfall; auf Altgeräten gespeicherte Daten bis zur Löschung	Beschäftigte und Gerätenutzer des Auftraggebers; Personen, deren Daten auf den Geräten gespeichert sind
E – Standortvernetzung und SD-WAN	Betrieb und Entstörung der Netze	Planung, Einrichtung und Störungsanalyse von Routern, Firewalls, VPN- und SD-WAN-Komponenten	Konfigurationsdaten; IP- und MAC-Adressen; Benutzer- und Gerätekennungen; Verbindungs- und Sicherheitsprotokolle im Störfall	Beschäftigte und sonstige Nutzer der Netze des Auftraggebers

Modul	Zweck	Gegenstand der Verarbeitung	Arten personenbezogener Daten	Betroffene Personen
F – KI-Assistenz (digitaler Mitarbeiter)	Betrieb eines KI-Assistenten zur Entlastung der Beschäftigten	Einrichtung, Betrieb und Pflege eines KI-Assistenten mit Anbindung an E-Mail, Microsoft 365, Website oder Ablagen	Inhalte von E-Mails, Dokumenten und Wissensquellen einschließlich darin enthaltener Kontaktdaten; Ein- und Ausgaben des Assistenten; Nutzer- und Protokolldaten	Beschäftigte des Auftraggebers; Kunden, Interessenten, Geschäftspartner und weitere in den Inhalten genannte Personen
G – Websites und SEO	Betrieb und Pflege der Website	Erstellung, technische Betreuung und Pflege von Websites einschließlich Formularen; Auswertung der Google Search Console	Formulareingaben wie Name, Kontaktdaten und Anliegen; Zugriffs- und Protokolldaten (IP-Adresse, Zeitpunkt, aufgerufene Seite); Zugangsdaten der Redakteure; zusammengefasste Suchdaten	Besucher und Interessenten der Website; Beschäftigte des Auftraggebers als Redakteure

Art der Verarbeitung in allen Modulen: Erheben, Erfassen, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Abgleichen und Verknüpfen, Übermitteln auf Weisung, Einschränken, Löschen und Vernichten. Dauer: Laufzeit des jeweiligen Einzelauftrags; für den AVV selbst gilt § 1 Abs. 4.

Anlage 2 – Technische und organisatorische Maßnahmen

Die Maßnahmen setzen Art. 32 DSGVO um. Daten werden überwiegend in Rechenzentren der Unterauftragsverarbeiter nach Anlage 3 verarbeitet; deren Zertifizierungen und Nachweise ergänzen diese Anlage.

1. Vertraulichkeit

Zutrittskontrolle

- Büroräume sind außerhalb der Geschäftszeiten verschlossen; Schlüssel haben nur Beschäftigte; Besucher werden begleitet.
- Verarbeitung in Rechenzentren mit Zutrittskontrolle und Zertifizierung nach ISO/IEC 27001 oder gleichwertigen Nachweisen wie BSI C5.

Zugangskontrolle

- Persönliche Benutzerkonten für jeden Beschäftigten; bei Kundensystemen persönliche Konten oder Partnerzugänge statt geteilter Zugangsdaten, soweit der Anbieter dies ermöglicht.
- Mehr-Faktor-Authentifizierung für Microsoft 365, das CRM und die Redaktionsoberfläche der Website sowie für Verwaltungsportale, soweit der Anbieter sie unterstützt.
- Serverzugänge nur per SSH-Schlüssel; automatische Sperre von Adressen nach wiederholten Fehlversuchen.
- Bildschirmsperre bei Inaktivität; Notebooks mit Festplattenverschlüsselung; dienstliche Mobilgeräte im Mobile-Device-Management mit Sperrcode und Fernlöschung.
- Zugangsdaten zu Diensten werden zugriffsgeschützt außerhalb öffentlich erreichbarer Verzeichnisse gespeichert; offengelegte Zugangsdaten werden unverzüglich ersetzt.

Zugriffskontrolle

- Berechtigungen nach Rolle und nach dem Prinzip der minimalen Rechte; Vergabe und Entzug durch die Geschäftsführung.
- Webanwendungen des Auftragnehmers nur nach Anmeldung; automatisierte Aufrufe nur mit geheimen, je Dienst getrennten Schlüsseln.
- Entzug aller Zugänge ausscheidender Beschäftigter spätestens am letzten Arbeitstag.

Trennungskontrolle

- Logische Trennung der Daten je Auftraggeber durch eigene Kundenkennung, getrennte Anlagen- und Portalzugänge und getrennte Ablage.
- Trennung von Test und Betrieb; neue Programmversionen laufen zunächst im Probelauf ohne Schreibzugriff auf Kundendaten.

Verschlüsselung und Datensparsamkeit

- Transportverschlüsselung (TLS) für Webanwendungen, Schnittstellen und E-Mail, soweit die Gegenstelle sie unterstützt; Telefonie über das Gateway mit TLS und SRTP.
- Datensicherungen werden vor der Übertragung clientseitig verschlüsselt (AES-256-GCM, Schlüssel durch RSA-4096-OAEP geschützt); der Schlüssel liegt ausschließlich beim Auftragnehmer.
- An KI-Dienste gehen nur die für die Aufgabe erforderlichen Daten; ein Training von Modellen mit Daten des Auftraggebers ist vertraglich ausgeschlossen.

2. Integrität

Weitergabekontrolle

- Datenübertragung nur über verschlüsselte Verbindungen (TLS, SSH/SFTP).
- E-Mail-Verkehr über ein Sicherheits-Gateway mit Spam- und Schadsoftwarefilter.
- Weitergabe an Dritte nur nach § 6 oder auf Weisung.

Eingabekontrolle

- Protokollierung von Anmeldungen und Änderungen in Microsoft 365, CRM und Verwaltungsportalen, soweit die Systeme dies bieten.
- Eigene Anwendungen protokollieren Verarbeitungsschritte mit Zeitpunkt und Programmversion; Änderungen an Kundendaten sind im CRM nachvollziehbar.

3. Verfügbarkeit und Belastbarkeit

- Betrieb in redundant ausgelegten Rechenzentren der Unterauftragsverarbeiter.
- Regelmäßige, verschlüsselte und versionierte Datensicherung der eigenen Anwendungen mit dokumentiertem Wiederherstellungsverfahren.
- Revisionssichere Archivierung des E-Mail-Verkehrs.
- Überwachung der Dienste und zeitgesteuerten Abläufe mit Benachrichtigung bei Fehlern.
- Server mit Firewall, zeitnahen Sicherheitsupdates und Sperre auffälliger Zugriffe; HTTP-Sicherheits-Header für die Webanwendungen.

4. Regelmäßige Überprüfung

- Überprüfung der Maßnahmen nach § 5 Abs. 3; das Ergebnis wird dokumentiert.
- Verpflichtung aller Beschäftigten auf Vertraulichkeit, Datenschutz und Fernmeldegeheimnis; Unterweisung bei Eintritt und danach regelmäßig.
- Beschäftigte melden Sicherheitsvorfälle sofort an die Geschäftsführung; die Meldung an den Auftraggeber folgt § 8.
- Auftragsverarbeitungsverträge mit allen Unterauftragsverarbeitern; Prüfung ihrer Nachweise vor Beauftragung.

5. Datenschutz durch Technikgestaltung und Voreinstellungen

- Aufzeichnung, Transkription und KI-Auswertung sind standardmäßig deaktiviert und werden nur nach Beauftragung eingeschaltet.
- Aufzeichnungen und Transkripte werden gelöscht, sobald der Zweck erreicht ist, spätestens nach 90 Tagen, soweit der Einzelauftrag nichts anderes bestimmt.

Anlage 3 – Unterauftragsverarbeiter

Mit Abschluss dieses AVV genehmigt der Auftraggeber die folgenden Unterauftragsverarbeiter (Stand 15.10.2026). Einträge mit Modulbuchstaben nach Anlage 1 gelten nur, wenn das Modul beauftragt ist.

Unterauftragsverarbeiter	Leistung	Module	Ort der Verarbeitung	Garantie bei Drittlandbezug
Microsoft Ireland Operations Ltd., Dublin, Irland	Microsoft 365: E-Mail, Kalender, Teams, Dateiablage, Benutzerverwaltung	alle	EU (EU Data Boundary)	Zugriffe aus den USA im Ausnahmefall: EU-US Data Privacy Framework, Standardvertragsklauseln
Hornetsecurity GmbH, Hannover	E-Mail-Sicherheits-Gateway mit Filter und Signaturen	alle	EU	–
ELOVADE Deutschland GmbH, Wetzlar	E-Mail-Archivierung (EL mailarchive, MailStore-Technologie)	alle	Deutschland	–
HubSpot Ireland Ltd., Dublin, Irland	CRM und Ticketsystem: Kontakte, Service-Tickets, Gesprächsnotizen, Dokumente	alle	EU	Zugriffe der HubSpot, Inc. (USA): EU-US Data Privacy Framework, Standardvertragsklauseln
STRATO GmbH, Berlin	Hosting der Website und der Webanwendungen des Auftragnehmers (Portal, Telefonie- und Synchronisationsdienste)	alle	Deutschland	–
Docusign International (EMEA) Ltd., Dublin, Irland	Elektronische Signatur von Aufträgen, Vollmachten und Kündigungen	A, B	EU	Verbindliche interne Datenschutzvorschriften (BCR), Standardvertragsklauseln
TeamViewer Germany GmbH, Göppingen	Fernwartung im Einzelfall mit Zustimmung des Auftraggebers	B	EU/EWR	–
NFON AG, München	Cloud-Telefonanlage, soweit über den Auftragnehmer bereitgestellt; Fax-Versand von Schreiben im Auftrag	B, C	Deutschland	–
Hetzner Online GmbH, Gunzenhausen	Server für Browser- und App-Telefonie (Gateway) und Zwischenspeicherung von Gesprächsaufzeichnungen	C	Deutschland (Nürnberg)	–
Mistral AI SAS, Paris, Frankreich	Transkription von Gesprächsaufzeichnungen	C	EU	–
Anthropic Ireland, Ltd., Dublin, Irland, mit Anthropic, PBC, USA	KI-Zusammenfassung und KI-Auswertung von Gesprächen, Rechnungen, Tickets und Dokumenten	B, C	USA	Standardvertragsklauseln

Für die Module D, E und F sowie für Push-Dienste der Telefonie-Apps (Modul C) werden eingesetzte Plattformen und Dienstleister, etwa MDM-Anbieter, Löschdienstleister, Verwaltungsportale von Netzwerkherstellern, Anbieter von KI-Modellen oder die Push-Dienste von Apple und Google, im Einzelauftrag benannt (§ 6 Abs. 2). Anbieter, mit denen der Auftraggeber eigene Verträge hat, sind nicht aufgeführt (§ 1 Abs. 3).

Die jeweils aktuelle und alle früheren Fassungen stehen unter khtc-consulting.de/avv/ bereit. Fragen zum AVV: info@khtc-consulting.de · 04773 2110