KI Kurt

KI KURT · VERTRAGSTEXTE, FASSUNG VOM 29.10.2026

# Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO, gehostete Form

zwischen

_____ *(Name oder Firma)*

_____ *(Anschrift)*

vertreten durch _____ *(Name, Funktion)*

nachfolgend „Auftraggeber" (Verantwortlicher)

und

**Kurt König, KI Kurt**

Wittelsbacher Straße 2, 97074 Würzburg

kurt@ki-kurt.de

nachfolgend „Auftragnehmer" (Auftragsverarbeiter)

## § 1 Gegenstand und Dauer

(1) Der Auftragnehmer betreibt für den Auftraggeber eine Arbeitsumgebung mit KI-Assistenz auf einer Rechnerinstanz, die der Auftragnehmer bei einem Rechenzentrumsbetreiber anmietet (nachfolgend „Maschine"). Der Auftraggeber und die von ihm benannten Personen arbeiten in dieser Umgebung ausschließlich über die Oberfläche der Assistenz. Gegenstand ist:

- [ ] Bürogeselle oder Bürokompagnon, Arbeitsumgebung für eine Person
- [ ] Firmengedächtnis, Arbeitsumgebung für einen Betrieb mit _____ Plätzen

(2) Dieser Vertrag gilt für die Dauer des Hauptvertrags Nutzungsvertrag Bürogeselle, Bürokompagnon und Firmengedächtnis, Fassung 2 vom 29.10.2026, und darüber hinaus, bis die Löschung nach § 10 abgeschlossen ist. Er erfasst den zunächst vereinbarten Zugang und alle später nach dem Hauptvertrag eingerichteten Zugänge.

## § 2 Art und Zweck der Verarbeitung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich, um die Arbeitsumgebung bereitzustellen: Speichern der Unterlagen und Arbeitsergebnisse des Auftraggebers auf der Maschine, Verarbeitung durch ein KI-Sprachmodell auf Anfrage der Nutzer, Einsortieren und Erschließen eingebrachter Unterlagen, Sicherung, Wartung, Störungsbehebung, Einspielen neuer Fassungen des Regelwerks, und Herausgabe der Daten bei Vertragsende.

(2) Die Maschine verarbeitet Anfragen an das Sprachmodell über den in Anlage 2 benannten Dienst. Welcher Weg gilt, ist dort angekreuzt.

(3) Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt. Insbesondere werden Inhalte des Auftraggebers nicht zum Verbessern des Produkts, zum Trainieren eines Modells oder für andere Kunden verwendet. Für Produktverbesserungen darf der Auftragnehmer allgemeine Fehlerbeschreibungen und Funktionswünsche verwenden, sofern sie keine personenbezogenen Daten, Dokumente oder vertraulichen Inhalte des Auftraggebers enthalten. Eine Supportanfrage oder ein Verbesserungsvorschlag erweitert den Verarbeitungsauftrag nicht.

**(4) Ist in Anlage 2 die Internetrecherche angekreuzt, übermittelt die Assistenz auf Anfrage eines Nutzers Suchbegriffe an den dort genannten Suchdienst und ruft öffentlich zugängliche Webseiten ab. Vollständige Dokumente des Auftraggebers werden dabei nicht als Suchunterlagen übermittelt. Die Assistenz ist angewiesen, keine Namen von Personen und keine Inhalte aus Unterlagen in Suchbegriffe zu setzen; diese Anweisung ist keine technische Sperre, und Suchbegriffe sowie Adressen können personenbezogene oder vertrauliche Angaben enthalten. Ist die Internetrecherche nicht angekreuzt, findet beides nicht statt.**

## § 3 Art der Daten und betroffene Personen

(1) Verarbeitet werden die Daten, die der Auftraggeber und seine Nutzer in die Umgebung einbringen oder dort erzeugen. Typisch sind: Namen, Kontaktdaten und Rollen von Beschäftigten, Kunden, Lieferanten und sonstigen Beteiligten; Inhalte von Schriftverkehr, Angeboten, Protokollen, Projekt- und Vorgangsakten; Notizen und Aufgaben der Nutzer. Welche Unterlagen eingebracht werden, bestimmt der Auftraggeber.

(2) Betroffen sind die Nutzer der Umgebung und die Personen, die in den eingebrachten Unterlagen genannt sind.

(3) Besondere Kategorien nach Art. 9 DSGVO, Daten nach Art. 10 DSGVO und Geheimnisse, die einer beruflichen Schweigepflicht nach § 203 StGB unterliegen, sind nicht Gegenstand dieses Vertrags. Der Auftraggeber bringt sie nicht ein. Sollen sie verarbeitet werden, vereinbaren die Parteien das vorab gesondert in Textform.

(4) Gilt nach Anlage 2 der Weg *eigener Firmenvertrag des Auftraggebers bei Anthropic*, schließt der Auftraggeber vor Beginn auf eigenen Namen einen Vertrag mit Anthropic in einem Tarif für Unternehmen ab, für den Anthropics Geschäftsbedingungen für Unternehmen (Commercial Terms) mit dem Datenverarbeitungszusatz (Data Processing Addendum) gelten. Das sind derzeit Claude Team, Claude

Enterprise oder ein Konto in der Claude Console. Tarife für Verbraucher (Free, Pro, Max) genügen nicht. **Beim Konto in der Claude Console richtet der Auftraggeber je Nutzer einen eigenen Arbeitsbereich mit eigenem Schlüssel ein und trägt den Schlüssel selbst in die Arbeitsfläche ein; bei Claude Team oder Enterprise** meldet sich jeder Nutzer mit einem eigenen Platz aus diesem Vertrag an. Anthropic ist auf diesem Weg Auftragsverarbeiter des Auftraggebers und nicht Unterauftragsverarbeiter des Auftragnehmers. **Mit der Wahl dieses Wegs weist der Auftraggeber den Auftragnehmer an, Anfragen und die dafür nötigen Inhalte aus der Umgebung an Anthropic zu übermitteln. Anthropic verarbeitet sie auch in den USA. Für diese Übermittlung und für den Vertrag mit Anthropic ist der Auftraggeber verantwortlich. Ein Wechsel zu einem anderen Bezugs- oder Anmeldeverfahren als dem in Anlage 2 angekreuzten bedarf einer vorherigen Vereinbarung in Textform einschließlich der nötigen Anpassung dieses Vertrags.**

## § 4 Weisungen und Verantwortung des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, auch was eine Übermittlung in ein Drittland betrifft, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats dazu verpflichtet; dann teilt er dem Auftraggeber diese Pflicht vorher mit, soweit das Recht es nicht verbietet.

(2) Die Nutzung der Umgebung durch den Auftraggeber und seine Nutzer gilt als Weisung. Weitere Weisungen erteilt der Auftraggeber in Textform, eine E-Mail genügt. Weisungsberechtigt ist _____ *(Name)*.

(3) Hält der Auftragnehmer eine Weisung für datenschutzrechtswidrig, unterrichtet er den Auftraggeber unverzüglich unter Angabe seiner Gründe und setzt ihre Ausführung bis zur Klärung aus. Eine rechtswidrige Verarbeitung führt er auch nach Bestätigung der Weisung nicht durch. Seine eigenen gesetzlichen Pflichten bleiben unberührt.

**(4) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung und für die Rechte der betroffenen Personen verantwortlich. Er informiert die Personen, deren Daten er einbringt, soweit Art. 13 und 14 DSGVO das verlangen, holt erforderliche Einwilligungen selbst ein und prüft selbst, ob er für die Verarbeitung eine Datenschutz-Folgenabschätzung braucht.**

## § 5 Vertraulichkeit

Der Auftragnehmer setzt für die Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet sind. Zum Zeitpunkt dieses Vertrags ist das allein Kurt König. Kommt eine Person hinzu, teilt der Auftragnehmer das vorher in Textform mit.

## § 6 Zugriff des Auftragnehmers

(1) Der Auftragnehmer verwaltet die Maschine. Er kann deshalb technisch auf die Daten des Auftraggebers zugreifen.

(2) Er greift auf die Daten außerhalb der Assistenz nur zu, soweit es für einen dieser Zwecke erforderlich ist: Einrichtung, Umzug in die Umgebung, Behebung einer Störung, Herausgabe und Löschung nach § 10, oder eine Weisung des Auftraggebers. Jeder solche Zugriff wird mit Datum, Anlass und Dauer **in Textform** festgehalten und dem Auftraggeber auf Anfrage vorgelegt.

(3) Die Assistenz arbeitet nur im Auftrag der Person, die sie gerade benutzt. Sie liest **persönliche** Bereiche anderer Nutzer nicht. **Gruppen- und gemeinsame Bereiche nach Anlage 1 liest sie nur für die Nutzer, die dafür freigegeben sind.**

**(4) Bei einem Zugriff nach Absatz 2 setzt der Auftragnehmer kein Werkzeug ein, das Inhalte des Auftraggebers an einen Dienst übermittelt, der nicht in Anlage 2 genannt ist.**

## § 7 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die Maßnahmen nach **Anlage 1**.

(2) Er darf sie durch andere ersetzen, wenn das Schutzniveau nicht sinkt. Eine wesentliche Änderung teilt er dem Auftraggeber in Textform mit.

## § 8 Unterauftragsverarbeiter

(1) Der Auftraggeber genehmigt die in **Anlage 2** genannten Unterauftragsverarbeiter.

(2) Der Auftraggeber erteilt eine allgemeine Genehmigung für weitere Unterauftragsverarbeiter nach folgendem Verfahren: Der Auftragnehmer teilt ihm mindestens 30 Kalendertage vor dem vorgesehenen Einsatz in Textform Unternehmen, Tätigkeit, Orte der Verarbeitung und Datenschutzgrundlagen mit. Der Auftraggeber kann binnen 14 Kalendertagen aus begründeten datenschutzrechtlichen Bedenken widersprechen. Bis zur Klärung eines solchen Widerspruchs erhält der beanstandete Unterauftragsverarbeiter keine Daten des Auftraggebers. Finden die Parteien keine Lösung, kann der Auftraggeber den Hauptvertrag vor dem vorgesehenen Einsatz ohne zusätzliche Kosten beenden.

(3) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Pflichten, die diesem Vertrag entsprechen. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer dem Auftraggeber gegenüber für deren Einhaltung.

## § 9 Unterstützung, Meldung von Pannen

(1) Der Auftragnehmer unterstützt den Auftraggeber bei Anfragen Betroffener nach Kapitel III DSGVO. Erreicht ihn eine solche Anfrage direkt, leitet er sie unverzüglich weiter und beantwortet sie nicht selbst.

(2) Er unterstützt den Auftraggeber bei den Pflichten nach Art. 32 bis 36 DSGVO, soweit es ihm mit den ihm verfügbaren Informationen möglich ist.

(3) Eine Verletzung des Schutzes personenbezogener Daten meldet er dem Auftraggeber unverzüglich, in der Regel binnen 48 Stunden nach Kenntnis, mit den Angaben, die er zu diesem Zeitpunkt hat.

## § 10 Ende: Herausgabe und Löschung

(1) Der Auftraggeber kann seine Daten während der Laufzeit jederzeit selbst als ZIP-Datei herunterladen. Bei Vertragsende stellt der Auftragnehmer ihm die vollständigen Daten in derselben Form bereit, auf Wunsch getrennt nach Bereichen.

(2) Der Auftraggeber wählt die Rückgabe seiner Daten mit anschließender Löschung. Das vollständige Paket steht ab Vertragsende 30 Kalendertage zum Abruf bereit; nach Ablauf dieser Frist löscht der Auftragnehmer die Maschine mit allen Datenträgern und Sicherungen, sofern der Auftraggeber nicht vorher die Löschung verlangt, und bestätigt das in Textform. Hat der Auftraggeber die Herausgabe bis dahin nicht abgerufen, erinnert der Auftragnehmer einmal in Textform, mindestens 7 Tage vor der Löschung. **Verlangt der Auftraggeber vor der Löschung in Textform mehr Zeit für den Abruf, verschiebt der Auftragnehmer die Löschung einmal um bis zu 30 Tage. Kopien außerhalb der Maschine, die beim Auftragnehmer bei Einrichtung, Umzug oder Störungsbehebung entstanden sind, löscht er in derselben Frist. Das Protokoll nach § 6 Abs. 2 und die Nachweise nach § 11 enthalten nur Datum, ausführende Person, Anlass, Umfang und Dauer, keine Inhalte des Auftraggebers; der Auftragnehmer bewahrt sie zur eigenen Rechenschaft für die Vertragsdauer und danach bis zum Ablauf der regelmäßigen Verjährungsfrist auf, bei einem Rechtsstreit bis zu dessen Abschluss, und löscht sie dann.**

(3) Aufbewahrungspflichten des Auftraggebers für seine eigenen Unterlagen bleiben seine Sache. Er sichert die Herausgabe nach Absatz 1, bevor gelöscht wird.

## § 11 Nachweis und Kontrolle

(1) Der Auftragnehmer stellt dem Auftraggeber die Informationen zur Verfügung, die zum Nachweis der Pflichten nach Art. 28 DSGVO nötig sind, einschließlich des Protokolls nach § 6 Abs. 2.

(2) Der Auftraggeber darf die Einhaltung nach angemessener Vorankündigung prüfen oder durch einen zur Verschwiegenheit verpflichteten Prüfer prüfen lassen; der Auftragnehmer ermöglicht Überprüfungen einschließlich erforderlicher Inspektionen und wirkt daran mit. Bei Unterauftragsverarbeitern werden zunächst geeignete aktuelle Prüfberichte und Zertifikate herangezogen; reichen sie für den Nachweis nicht aus, wirkt der Auftragnehmer an ergänzenden Informationen und angemessenen weiteren Prüfmaßnahmen mit. Bei konkreten Anhaltspunkten für einen erheblichen Verstoß oder auf Verlangen einer Aufsichtsbehörde entfällt die Vorankündigung, soweit das für eine wirksame Prüfung erforderlich ist.

## § 12 Haftung, Rangfolge, Form

(1) Die Haftung **gegenüber betroffenen Personen** richtet sich nach Art. 82 DSGVO . **Im Verhältnis der Parteien zueinander gilt die Haftungsregel des Hauptvertrags. Ein Bußgeld trägt die Partei, gegen die es verhängt wird.**

(2) Widerspricht der Hauptvertrag diesem Vertrag in einer Frage des Datenschutzes, gilt dieser Vertrag.

(3) Änderungen in Textform. **Dieser Vertrag kommt zusammen mit dem Hauptvertrag zustande, auf demselben Weg: per E-Mail oder mit dem Klick auf der Bestellseite nach § 9 Abs. 3 des Nutzungsvertrags. Eine Unterschrift ist nicht erforderlich.** Es gilt deutsches Recht. Ist eine Bestimmung unwirksam, bleibt der Rest wirksam.

*Elektronisch vereinbart durch die beim Vertragsschluss bezeichneten Parteien. Maßgeblich sind die dabei festgehaltenen Erklärungen und Fassungen; Unterschriften sind nicht erforderlich.*

# Anlage 1: Technische und organisatorische Maßnahmen

**Getrennte Maschine je Auftraggeber.** Für jeden Auftraggeber wird eine eigene virtuelle Rechnerinstanz betrieben. Daten verschiedener Auftraggeber werden nicht in derselben virtuellen Instanz gespeichert. Die physische Technik des Rechenzentrums kann von mehreren Kunden von AWS gemeinsam genutzt werden.

**Zugang nur über die Assistenz.** Nutzer melden sich über eine verschlüsselte Verbindung (HTTPS) an. Einen direkten Zugang zur Maschine haben sie nicht.

**Nutzeranmeldung. Jeder Nutzer meldet sich mit einem persönlichen Kennwort an. Nach fünf Fehlversuchen binnen 15 Minuten wartet die Anmeldung. Ein zweiter Faktor ist nicht eingerichtet.**

**Getrennte Bereiche.** Daten und Regelwerk liegen in getrennten Bereichen. Bei mehreren Nutzern hat jede Person einen eigenen Bereich, der für andere Nutzer gesperrt ist; Gruppen- und gemeinsame Bereiche werden ausdrücklich freigegeben. Die Trennung erfolgt über die Rechte des Betriebssystems.

**Verwalterzugang.** Innerhalb der Maschine hat auf Seiten des Auftragnehmers ausschließlich Kurt König Verwalterrechte, über einen persönlichen Schlüssel. Zugriffe des Rechenzentrumsbetreibers auf dessen Infrastruktur richten sich nach dessen Datenschutz- und Sicherheitsbedingungen. Jeder Zugriff auf Daten außerhalb der Assistenz wird nach § 6 Abs. 2 festgehalten.

**Datenträger.** Die Datenträger der Maschine und ihre Sicherungen werden durch AWS im Ruhezustand verschlüsselt; die Schlüssel dafür verwaltet AWS.

**Schlüssel für das Modell.** Der Zugangsschlüssel zum Sprachmodell liegt bei einem eigenen Dienst auf der Maschine, nicht in der Sitzung der Nutzer. **Beim Weg *eigener Firmenvertrag* mit Konto in der Claude Console trägt der Nutzer den Schlüssel des Auftraggebers selbst in die Arbeitsfläche ein; er liegt beim selben Dienst und wird dem Sprachmodell nicht als Inhalt übermittelt. Er kann in den Sicherungen der Maschine enthalten sein; diese unterliegen denselben Zugriffs- und Löschregeln. Verwalterzugriffe richten sich nach § 6. Mit Claude Team oder Enterprise meldet sich jeder Nutzer selbst bei Anthropic an; der Auftragnehmer sieht dabei keinen Anmeldecode.**

**Gesprächsverläufe.** Die Assistenz (Claude Code) legt die Verläufe der Sitzungen im Bereich des Nutzers auf der Maschine ab und löscht sie 30 Tage nach ihrer Erstellung. Soweit sie in zuvor erstellten Sicherungen enthalten sind, werden diese Kopien spätestens nach weiteren sieben Tagen überschrieben und bis dahin nur für eine erforderliche Wiederherstellung vorgehalten; nach einer Wiederherstellung werden zwischenzeitliche Löschungen erneut ausgeführt. **Optionale Telemetrie, automatische Fehlerberichte und Rückmeldeumfragen der Assistenz sind in ihrer Konfiguration abgeschaltet; die für die Modellnutzung erforderliche Verbindung zu Anthropic bleibt bestehen.**

**Sicherung.** Die auf der Maschine gespeicherten Dokumente, Notizen und Arbeitsergebnisse werden **täglich** gesichert, Sicherungen werden **sieben Tage** aufbewahrt und nach § 10 mit gelöscht. **Die Sicherung liegt in derselben Region wie die Maschine. Eine Wiederherstellung wird vor der Übergabe der Maschine und danach mindestens einmal im Kalendervierteljahr geprobt und festgehalten.**

**Herausgabe.** Jeder Nutzer kann seinen Bereich jederzeit als ZIP-Datei mit Prüfsummen herunterladen.

**Änderungen am Regelwerk** werden erst auf einer Prüfmaschine ohne Kundendaten eingespielt, dann beim Auftraggeber.

**Pflege.** Das Betriebssystem erhält Sicherheitsaktualisierungen.

**Überprüfung. Der Auftragnehmer prüft diese Maßnahmen mindestens einmal im Kalendervierteljahr und nach jeder wesentlichen Änderung der Maschine und hält das Ergebnis fest.**

# Anlage 2: Unterauftragsverarbeiter und Modellweg

| UNTERAUFTRAGSVERARBEITER | LEISTUNG | ORT DER VERARBEITUNG | GRUNDLAGE |
|---|---|---|---|
| **Amazon Web Services** (Vertragsgesellschaft Amazon Web Services EMEA SARL, Luxemburg, Konzernmutter Amazon.com Inc., USA) | Rechenzentrum der Maschine und ihrer Sicherungen (Amazon Lightsail) | AWS-Region eu-north-1, Stockholm, Schweden; ein Wechsel der Region nur mit vorheriger Zustimmung des Auftraggebers in Textform | Datenverarbeitungszusatz von AWS, Teil der AWS-Dienstbedingungen; für Übermittlungen in Drittländer **und für Supportzugriffe aus Drittländern** die Standardvertragsklauseln der EU-Kommission |
| **Amazon Web Services**, wie oben | Sprachmodell über Amazon Bedrock, nur wenn unten angekreuzt. **Eingaben und Ausgaben speichert AWS nach eigener Angabe nicht. Ein Modell, für das AWS eine befristete Speicherung angibt, setzt der Auftragnehmer nur nach Mitteilung in Textform ein** | Rechenzentren in der EU (regionsübergreifendes EU-Profil) | wie oben |

**Modellweg, eines ankreuzen:**

- [ ] **Bedrock über den Auftragnehmer.** Anfragen an das Modell laufen über Amazon Bedrock. Der Modellhersteller erhält nach Angabe von AWS keinen Zugriff auf Eingaben und Ausgaben.
- [x] **Eigener Firmenvertrag des Auftraggebers bei Anthropic**, Tarif Claude Console. Der Auftraggeber hat mit Anthropic einen eigenen Vertrag unter den Commercial Terms mit Datenverarbeitungszusatz.

Anthropic ist nicht Unterauftragsverarbeiter des Auftragnehmers. Bei jeder Anfrage an das Modell gehen die Anfrage und die dafür nötigen Inhalte an Anthropic, Verarbeitung auch in den USA. Es gilt § 3 Abs. 4.

**Internetrecherche der Assistenz, eines ankreuzen:**

- [x] **Eingeschaltet.** Die Assistenz sucht im Internet und ruft öffentliche Webseiten ab (§ 2 Abs. 4). **Beim Weg *eigener Firmenvertrag* sucht sie über die Websuche von Anthropic unter dem Vertrag des Auftraggebers; Brave wird dann nicht eingesetzt. Beim Weg Bedrock sucht sie über die Brave Search API.** Sie ist angewiesen, keine Namen von Personen und keine Inhalte aus Unterlagen in Suchbegriffe zu setzen; das ist eine Anweisung, keine technische Sperre (§ 2 Abs. 4). Der Betreiber einer abgerufenen Seite erfährt die abgerufene Adresse und die Adresse der Maschine.
- [ ] **Ausgeschaltet.** Die Assistenz arbeitet nur mit den Unterlagen auf der Maschine.

**Hinweis zum Drittlandbezug:** AWS ist ein Unternehmen eines US-Konzerns. Auch bei einer Verarbeitung in Frankfurt **oder einer anderen Region in der EU** können US-Behörden nach US-Recht Zugriff verlangen. Der Auftragnehmer nennt das, weil es zutrifft. Der Hinweis hebt die vereinbarte Speicherregion nicht auf; davon zu unterscheiden sind die vereinbarten Übermittlungen an Anthropic und rechtmäßig abgesicherte Zugriffe aus Drittländern.