AGENTENKOLLEGE · DAVID KOGAN

Vertrag zur Auftragsverarbeitung (AVV)

nach Art. 28 DSGVO · Stand: Mai 2026 · agentenkollege.de

Entwurf zur Prüfung. Diese Vorlage wurde sorgfältig erstellt, ist jedoch vor dem Einsatz mit Kunden anwaltlich bzw. datenschutzrechtlich zu prüfen. Verbindlich wird das Dokument erst mit beidseitiger Unterzeichnung.

Präambel und Parteien

Dieser Vertrag zur Auftragsverarbeitung (nachfolgend **„AVV"**) wird geschlossen zwischen:

Verantwortlicher (Auftraggeber):
[Firmenname]
[Rechtsform]
[Anschrift: Straße, PLZ, Ort, Land]
vertreten durch **[Vertretungsberechtigte Person / Funktion]**
(nachfolgend **„Verantwortlicher"**)

und

Auftragsverarbeiter (Auftragnehmer):
David Kogan, Einzelunternehmen, Geschäftsbezeichnung **Agentenkollege**
Engernweg 79, 33100 Paderborn, Deutschland
Telefon: +49 176 56967667 · E-Mail: kontakt@agentenkollege.de
Datenschutz: datenschutz@agentenkollege.de · Web: agentenkollege.de
(nachfolgend **„Auftragsverarbeiter"**)

Verantwortlicher und Auftragsverarbeiter werden nachfolgend gemeinsam auch als **„Parteien"** bezeichnet.

Dieser AVV ist Bestandteil des zwischen den Parteien abgeschlossenen Hauptvertrags über die Bereitstellung von Managed-KI-Agenten (nachfolgend **„Hauptvertrag"**) und konkretisiert die datenschutzrechtlichen Pflichten gemäß Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, **DSGVO**). Im Verhältnis zum Hauptvertrag hat dieser AVV Vorrang, soweit datenschutzrechtliche Belange betroffen sind.

§ 1 Gegenstand, Art und Dauer der Verarbeitung

1.1 Gegenstand

Der Auftragsverarbeiter erbringt für den Verantwortlichen den im Hauptvertrag näher beschriebenen Dienst: Betrieb von vollständig konfigurierten, managed KI-Agenten (nachfolgend **„Agenten"**), die im Auftrag des Verantwortlichen autonome oder semi-autonome Aufgaben ausführen. Jeder Agent läuft auf einer dedizierten Ubuntu-Linux-VM bei Hetzner Cloud in Deutschland (Rechenzentren Nürnberg oder Falkenstein). Im Zuge dieser Tätigkeit verarbeitet der Auftragsverarbeiter personenbezogene Daten ausschließlich nach Weisung des Verantwortlichen.

1.2 Art der Verarbeitung

Die Verarbeitung umfasst insbesondere das Erheben, Speichern, Lesen, Abfragen, Weiterleiten, Verwenden, Kombinieren und Löschen personenbezogener Daten, soweit diese Vorgänge für den Betrieb der Agenten erforderlich sind (z. B. Abruf von E-Mails, Zugriff auf CRM-Einträge, Erstellung und Versand von Nachrichten, Ablage in dem git-versionierten Wissensspeicher des Agenten).

1.3 Dauer

Die Verarbeitung beginnt mit Inkrafttreten dieses AVV und endet mit der Beendigung des Hauptvertrags oder, sofern früher, mit schriftlicher Weisung des Verantwortlichen, die Verarbeitung einzustellen. Die Pflichten aus diesem AVV bleiben bis zur vollständigen Löschung bzw. Rückgabe der Daten nach § 10 bestehen.

§ 2 Art der Daten und Kategorien betroffener Personen

2.1 Kategorien betroffener Personen

Die Verarbeitung kann folgende Kategorien betroffener Personen betreffen (Angaben beispielhaft; die konkrete Festlegung obliegt dem Verantwortlichen):

- Beschäftigte des Verantwortlichen (Mitarbeiterinnen und Mitarbeiter, freie Mitarbeitende)
- Kundinnen und Kunden des Verantwortlichen sowie deren Ansprechpersonen
- Interessenten und Leads (Vertriebskontakte)
- Lieferanten und Dienstleister des Verantwortlichen sowie deren Ansprechpersonen
- Bewerberinnen und Bewerber (sofern ein Recruiting-Agent eingesetzt wird)
- **[weitere Kategorien nach Weisung des Verantwortlichen]**

2.2 Kategorien personenbezogener Daten

Die Verarbeitung kann folgende Datenkategorien umfassen (Angaben beispielhaft; konkrete Festlegung durch den Verantwortlichen):

- Stamm- und Kontaktdaten (Name, Vorname, Berufsbezeichnung, E-Mail-Adresse, Telefonnummer, Postanschrift)
- Kommunikationsdaten (E-Mails, Chat-Nachrichten, Gesprächsnotizen)
- Vertragsdaten (Angebote, Aufträge, Rechnungen, Zahlungsinformationen)
- CRM-Daten (Kundenhistorie, Aktivitäten, Leads, Opportunity-Daten)
- Kalender- und Terminplanungsdaten
- Dokumente und Dateien (soweit vom Verantwortlichen in den Agenten-Kontext übergeben)
- Bewerberdaten (soweit ein Recruiting-Agent beauftragt ist)
- **[weitere Datenkategorien nach Weisung des Verantwortlichen]**

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sowie Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO dürfen ohne ausdrückliche schriftliche Weisung des Verantwortlichen und ohne gesonderte Rechtfertigung **nicht** verarbeitet werden. Sollte der Verantwortlicher beabsichtigen, derartige Daten durch den Agenten verarbeiten zu lassen, ist dies vorab schriftlich mit dem Auftragsverarbeiter zu vereinbaren.

§ 3 Weisungsrecht des Verantwortlichen

3.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Der Hauptvertrag sowie dieser AVV gelten als initiale Weisung. Weitere Weisungen können schriftlich (E-Mail genügt) erteilt werden.

3.2 Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

3.3 Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die DSGVO oder sonstige datenschutzrechtliche Bestimmungen der EU oder eines Mitgliedstaats verstößt, so informiert er den Verantwortlichen unverzüglich. Der Auftragsverarbeiter ist berechtigt, die Ausführung einer solchen Weisung bis zu einer Klärung auszusetzen; er haftet nicht für Schäden, die daraus entstehen, dass er eine datenschutzwidrige Weisung nicht ausgeführt hat.

3.4 Weisungen, die über den vereinbarten Leistungsumfang hinausgehen und zusätzlichen Aufwand verursachen, können nach beidseitiger Vereinbarung gesondert vergütet werden.

§ 4 Pflichten des Auftragsverarbeiters

4.1 Vertraulichkeit und Verpflichtung von Beschäftigten

Der Auftragsverarbeiter gewährleistet, dass alle Personen, die mit der Verarbeitung der Daten des Verantwortlichen betraut sind, der Vertraulichkeit verpflichtet werden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Hinweis: Agentenkollege ist derzeit ein Einzelunternehmen ohne angestellte Beschäftigte. Sollten künftig Mitarbeitende oder Subunternehmer hinzugezogen werden, die Zugang zu personenbezogenen Daten des Verantwortlichen erhalten, werden diese vor Tätigkeitsbeginn auf Vertraulichkeit verpflichtet; der Verantwortliche wird hierüber gemäß § 5 informiert.

4.2 Technische und organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die konkret implementierten Maßnahmen sind in **Anlage 2** dieses AVV dokumentiert. Der Auftragsverarbeiter überprüft und aktualisiert die TOM regelmäßig.

4.3 Unterstützung bei Betroffenenrechten

Der Auftragsverarbeiter unterstützt den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung seiner Pflicht, Anträge auf Wahrnehmung von Betroffenenrechten (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) zu beantworten. Der Auftragsverarbeiter leitet eingehende Betroffenenanfragen, die sich auf den Verarbeitungsbereich des Verantwortlichen beziehen, unverzüglich an diesen weiter.

4.4 Unterstützung gemäß Art. 32–36 DSGVO

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

4.5 Meldung von Datenschutzverletzungen

Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten, die den Verarbeitungsbereich dieses AVV betreffen, **unverzüglich** und ohne unangemessene Verzögerung, spätestens jedoch innerhalb von **24 Stunden** nach Bekanntwerden. Die Meldung erfolgt schriftlich (E-Mail genügt) an die vom Verantwortlichen benannte Adresse und enthält die in Art. 33 Abs. 3 DSGVO genannten Mindestangaben, soweit diese zum Zeitpunkt der Erstmeldung bereits verfügbar sind. Weitere Details werden unverzüglich nachgereicht. Das Nähere regelt § 8.

4.6 Nachweis der Compliance

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel genannten Pflichten zur Verfügung und ermöglicht Überprüfungen und Inspektionen gemäß § 7.

§ 5 Unterauftragsverhältnisse

5.1 Der Auftragsverarbeiter ist berechtigt, die in **Anlage 1** dieses AVV aufgeführten Unterauftragsverarbeiter einzusetzen. Der Verantwortliche erteilt hiermit seine **allgemeine Genehmigung** gemäß Art. 28 Abs. 2 DSGVO für die in Anlage 1 gelisteten Unterauftragsverarbeiter.

5.2 **Ankündigungspflicht bei Änderungen:** Beabsichtigt der Auftragsverarbeiter, einen neuen Unterauftragsverarbeiter einzusetzen oder einen bestehenden auszutauschen, kündigt er dies dem Verantwortlichen schriftlich mit einer Frist von mindestens **30 Kalendertagen** an. Der Verantwortliche hat das Recht, einer solchen Änderung aus sachlichem Datenschutzgrund innerhalb dieser Frist schriftlich zu widersprechen. Kommt keine Einigung zustande, haben beide Parteien das Recht, den Hauptvertrag außerordentlich zu kündigen.

5.3 **Weitergabepflichten:** Setzt der Auftragsverarbeiter Unterauftragsverarbeiter ein, so hat er ihnen die Datenschutzpflichten aus diesem AVV im Wesentlichen aufzuerlegen. Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen vollumfänglich für die Erfüllung der Pflichten durch den Unterauftragsverarbeiter verantwortlich.

5.4 Die interne Inanspruchnahme von Nebenleistungen (z. B. Telekommunikation, Wartung, Hosting-Infrastruktur, die bereits in Anlage 1 erfasst sind) gilt nicht als Unterauftragsverhältnis im Sinne dieses Paragraphen.

§ 6 Technische und organisatorische Maßnahmen

Die zum Zeitpunkt des Vertragsschlusses geltenden technischen und organisatorischen Maßnahmen (TOM) nach Art. 32 DSGVO sind in **Anlage 2** dieses AVV dokumentiert.

Der Auftragsverarbeiter ist berechtigt und verpflichtet, die TOM im Laufe der Zeit anzupassen und weiterzuentwickeln, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen, die das Schutzniveau der Daten des Verantwortlichen erheblich verändern, werden dem Verantwortlichen vorab mitgeteilt.

§ 7 Kontroll- und Auditrechte des Verantwortlichen

7.1 Der Verantwortliche ist berechtigt, die Einhaltung der Datenschutzvorschriften und der Verpflichtungen aus diesem AVV beim Auftragsverarbeiter zu überprüfen. Er kann dies in angemessenem Umfang durch Anforderung von Nachweisen und Dokumentationen, durch Fragebögen oder durch Vor-Ort-Inspektionen (auch durch beauftragte Dritte) vornehmen.

7.2 Auditankündigungen sind mit einer Vorlaufzeit von mindestens **10 Werktagen** schriftlich anzukündigen, sofern keine konkreten Anhaltspunkte für einen schwerwiegenden Verstoß vorliegen. Audits finden zu üblichen Geschäftszeiten und in einer Weise statt, die den laufenden Betrieb nicht unverhältnismäßig beeinträchtigt.

7.3 Der Auftragsverarbeiter kann als Nachweis der Compliance auch Zertifizierungen anerkannter Stellen (z. B. ISO 27001) oder Testate eines unabhängigen Prüfers vorlegen, die den Prüfumfang des Verantwortlichen abdecken.

7.4 Kosten für Audits trägt grundsätzlich der Verantwortliche; dies gilt nicht bei festgestellten wesentlichen Pflichtverletzungen des Auftragsverarbeiters.

§ 8 Benachrichtigung bei Datenschutzverletzungen

8.1 Der Auftragsverarbeiter benennt als Ansprechstelle für Datenschutzvorfälle: datenschutz@agentenkollege.de.

8.2 Bei einer Verletzung des Schutzes personenbezogener Daten, die die Daten des Verantwortlichen betrifft, benachrichtigt der Auftragsverarbeiter den Verantwortlichen **unverzüglich**, spätestens innerhalb von **24 Stunden** nach Bekanntwerden. Die Erstmeldung enthält mindestens:

- eine Beschreibung der Art der Verletzung, soweit bekannt einschließlich der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der betroffenen Datensätze;
- Name und Kontaktdaten des Ansprechpartners;
- eine Beschreibung der wahrscheinlichen Folgen;
- eine Beschreibung der bereits ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und ggf. zur Abmilderung ihrer nachteiligen Auswirkungen.

8.3 Sollten zum Zeitpunkt der Erstmeldung nicht alle Informationen vorliegen, werden diese unverzüglich in weiteren Meldungen nachgereicht.

8.4 Der Verantwortliche ist für die Beurteilung, ob eine Meldepflicht gegenüber der zuständigen Aufsichtsbehörde (Art. 33 DSGVO) oder eine Benachrichtigungspflicht gegenüber betroffenen Personen (Art. 34 DSGVO) besteht, selbst verantwortlich.

§ 9 Drittlandübermittlung

9.1 Die primäre Hosting-Infrastruktur (VM-Betrieb) erfolgt ausschließlich in Deutschland (Hetzner Cloud, Rechenzentren Nürnberg/Falkenstein). Es findet insoweit **kein Transfer in Drittstaaten** statt; ein Standard-AVV mit Hetzner genügt.

9.2 Mehrere der in Anlage 1 aufgeführten Unterauftragsverarbeiter haben ihren Sitz oder verarbeiten Daten in Drittstaaten außerhalb der EU/des EWR (insbesondere USA: OpenAI, Anthropic, Composio,

AgentMail; Irland im EWR: Stripe). Für diese Übermittlungen stützt sich der Auftragsverarbeiter auf geeignete Garantien gemäß Art. 46 DSGVO, insbesondere auf die von der Europäischen Kommission erlassenen **Standardvertragsklauseln (SCC)** in der aktuell gültigen Fassung (Durchführungsbeschluss 2021/914/EU).

9.3 Modelle aus der Volksrepublik China (insbesondere Moonshot AI / Kimi) werden vom Auftragsverarbeiter **nicht eingesetzt**. Eine entsprechende Drittstaaten-Übermittlung nach China findet daher nicht statt. Auf Wunsch des Verantwortlichen steht eine reine EU-Modell-Variante (Z.AI/GLM mit EU-Hosting oder Mistral Large EU) zur Verfügung, die keinen Drittstaaten-Transfer für die LLM-Inferenz auslöst.

9.4 Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage die abgeschlossenen SCC-Dokumente sowie etwaige Transfer Impact Assessments zur Verfügung. Anlage 1 enthält eine Übersicht aller Drittland-Übermittlungen und der jeweiligen Rechtsgrundlage.

§ 10 Löschung und Rückgabe nach Vertragsende

10.1 Nach Beendigung des Hauptvertrags oder auf gesonderte Weisung des Verantwortlichen stellt der Auftragsverarbeiter dem Verantwortlichen sämtliche personenbezogenen Daten in einem gängigen, maschinenlesbaren Format zur Verfügung (**vollständiger Datenexport**). Dies umfasst insbesondere den Inhalt des Agenten-Wissensspeichers (Obsidian-Vault, Git-Repository), gespeicherte E-Mails der Agenten-Mailbox sowie sonstige im Rahmen der Auftragsverarbeitung gespeicherte Daten des Verantwortlichen.

10.2 Nach Bestätigung des erfolgreichen Exports durch den Verantwortlichen, spätestens jedoch nach Ablauf von **30 Kalendertagen** nach Vertragsende löscht der Auftragsverarbeiter alle personenbezogenen Daten des Verantwortlichen vollständig und unwiederbringlich, einschließlich sämtlicher Sicherungskopien. Dies schließt die Deprovisionierung der dedizierten VM ein.

10.3 Der Auftragsverarbeiter bestätigt die vollständige Löschung dem Verantwortlichen schriftlich.

10.4 Gesetzlich vorgeschriebene Aufbewahrungsfristen, die dem Auftragsverarbeiter selbst obliegen (z. B. steuerrechtliche Aufbewahrungspflichten für Rechnungsdaten nach § 147 AO), bleiben unberührt. In diesem Fall ist die weitere Verarbeitung auf den gesetzlich erforderlichen Umfang zu beschränken.

§ 11 Haftung

11.1 Die Haftung der Parteien gegenüber betroffenen Personen richtet sich nach Art. 82 DSGVO.

11.2 Im Innenverhältnis zwischen den Parteien gilt: Hat eine Partei einen Schaden verursacht, für den sie nach Art. 82 DSGVO gesamtschuldnerisch haftet, so kann sie bei der anderen Partei Regress nehmen, soweit deren Verschulden an dem Schaden nachgewiesen ist, Art. 82 Abs. 5 DSGVO.

11.3 Die Haftung des Auftragsverarbeiters gegenüber dem Verantwortlichen für Verletzungen dieses AVV richtet sich nach den Haftungsbestimmungen des Hauptvertrags. Soweit der Hauptvertrag keine abweichenden Regelungen enthält, haftet der Auftragsverarbeiter für Schäden aus schuldhafter Verletzung dieses AVV nach den allgemeinen gesetzlichen Vorschriften. Die Haftung für leichte Fahrlässigkeit ist, soweit gesetzlich zulässig, auf vorhersehbare, vertragstypische Schäden begrenzt.

11.4 Für Schäden, die daraus entstehen, dass der Verantwortliche fehlerhafte oder rechtswidrige Weisungen erteilt hat, haftet ausschließlich der Verantwortliche.

§ 12 Schlussbestimmungen

12.1 **Schriftformerfordernis:** Änderungen und Ergänzungen dieses AVV bedürfen der Textform (E-Mail genügt). Mündliche Nebenabreden bestehen nicht.

12.2 **Vorrang:** Dieser AVV hat Vorrang vor etwaigen abweichenden oder widersprüchlichen Datenschutzbestimmungen im Hauptvertrag, soweit datenschutzrechtliche Belange betroffen sind.

12.3 **Salvatorische Klausel:** Sollten einzelne Bestimmungen dieses AVV unwirksam oder undurchführbar sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Parteien verpflichten sich, die unwirksame oder undurchführbare Bestimmung durch eine wirksame Regelung zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung möglichst nahekommt.

12.4 **Anwendbares Recht:** Dieser AVV unterliegt ausschließlich dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (CISG).

12.5 **Gerichtsstand:** Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist, soweit gesetzlich zulässig, **Paderborn, Deutschland**.

12.6 **Dokumentenbestandteile:** Dieser AVV besteht aus dem vorstehenden Vertragstext sowie den folgenden Anlagen, die integraler Bestandteil dieses Vertrags sind:

- Anlage 1: Verzeichnis der Unterauftragsverarbeiter
- Anlage 2: Technische und organisatorische Maßnahmen (TOM)

Verantwortlicher	**Auftragsverarbeiter**
Ort, Datum: _____	Ort, Datum: Paderborn, _____
Firmenstempel / Unterschrift	Unterschrift
[Name, Funktion]	David Kogan
[Firmenname]	Agentenkollege

Anlage 1: Verzeichnis der genehmigten Unterauftragsverarbeiter

Stand: Mai 2026. Änderungen werden gemäß § 5 Abs. 2 mit 30 Tagen Vorlaufzeit angekündigt.

Unternehmen	Sitz / Land	Zweck / Funktion	Drittlandtransfer / Rechtsgrundlage
Hetzner Online GmbH	Gunzenhausen, Deutschland	VM-Hosting, Rechenzentrum Nürnberg / Falkenstein (eine dedizierte VM pro Agent)	Kein Drittlandtransfer; dt. AVV
Cloudflare Germany GmbH / Cloudflare Inc.	München, Deutschland (Billing-Entität)	DNS-Verwaltung, Security-Proxy, DDoS-Schutz, TLS-Terminierung	Möglicher USA-Transfer; SCC (2021/914/EU)
OpenAI, LLC	San Francisco, USA	Large Language Model (LLM), Sprachverarbeitung und Textgenerierung	USA; SCC + TIA
Anthropic, PBC	San Francisco, USA	Large Language Model (LLM), Sprachverarbeitung und Textgenerierung (insb. komplexe Analyse-Tasks)	USA; SCC + TIA
Z.AI / Zhipu AI (GLM)	EU-Hosting-Variante	Large Language Model (LLM), datenschutzfreundliche EU-Alternative	Kein Drittlandtransfer bei EU-Hosting-Variante
Composio, Inc.	USA	Tool-Anbindung / SaaS-Integrationen (CRM, Kalender, E-Mail, Dokumente u. a.)	USA; SCC + TIA
AgentMail	USA	Dedizierte Mailbox pro Agent (Empfang und Versand von E-Mails im Kundenauftrag)	USA; SCC + TIA
Stripe Payments Europe, Ltd.	Dublin, Irland (EU/EWR)	Zahlungsabwicklung (Abrechnungsdaten des Verantwortlichen)	EWR; kein Drittlandtransfer (Irland)

Hinweis: Modelle aus der Volksrepublik China (insbesondere Moonshot AI / Kimi) werden vom Auftragsverarbeiter nicht eingesetzt und sind ausdrücklich nicht Bestandteil dieses Vertrags.

Anlage 2: Technische und organisatorische Maßnahmen (TOM)

Die nachfolgenden TOM werden vom Auftragsverarbeiter zum Schutz personenbezogener Daten des Verantwortlichen implementiert und laufend gepflegt (Art. 32 DSGVO).

1. Zutrittskontrolle (Physische Sicherheit)

- Verarbeitung ausschließlich in Hetzner-Rechenzentren in Deutschland mit zertifizierter Zutrittssteuerung (ISO 27001, SOC 2).
- Kein eigenes Rechenzentrum; physische Zutrittskontrolle obliegt Hetzner Online GmbH.
- Administrative Tätigkeiten des Auftragsverarbeiters erfolgen ausschließlich remote über verschlüsselte Verbindungen.

2. Zugangskontrolle (Systemzugang)

- Authentifizierung ausschließlich per SSH-Schlüssel (Passwort-Login deaktiviert); SSH-Port nicht standardmäßig (Non-default Port oder VPN-Zugangsbeschränkung).
- Zwei-Faktor-Authentifizierung für alle administrativen Accounts und Cloud-Management-Portale.
- Automatische Sicherheitsupdates (unattended-upgrades) auf allen VMs aktiv.

- Zugriff auf Kundendaten ausschließlich durch den Auftragsverarbeiter selbst; keine weiteren Personen ohne gesonderte schriftliche Vereinbarung.

3. Zugriffskontrolle (Datenzugang / Berechtigungen)

- Strikte Mandantentrennung: eine dedizierte VM pro Agent, kein gemeinsamer Betrieb von Kundendaten verschiedener Auftraggeber auf einer VM.
- Docker-Container-Isolation für Agent-Prozesse; minimale Systemberechtigungen (Least Privilege).
- Git-Zugriff auf den Wissensspeicher (Obsidian-Vault) über SSH-Key; kein öffentlicher Zugriff.
- Caddy Reverse Proxy: TLS-Terminierung mit Let's Encrypt, automatische HTTPS-Weiterleitung, kein Klartextzugang.

4. Trennungskontrolle

- Vollständige logische und physische Trennung von Kundendaten verschiedener Auftraggeber durch dedizierte VMs.
- Separate Mailboxen pro Agent über AgentMail; kein gemeinsamer Posteingang über Kundengrenzen hinweg.
- Trennung von Produktions- und Testumgebungen.

5. Pseudonymisierung und Verschlüsselung

- Transportverschlüsselung: TLS 1.2 / 1.3 auf allen öffentlich erreichbaren Endpunkten (Caddy / Let's Encrypt).
- Verschlüsselung des SSH-Schlüsselpaars mit Passphrase.
- Verschlüsselung sensibler Konfigurationsdaten (API-Keys, Zugangsdaten) mittels Secrets-Management (Umgebungsvariablen, verschlüsselte Dateien, kein Klartext in Versionsverwaltung).

6. Verfügbarkeitskontrolle

- Regelmäßige Backups der VM-Snapshots bei Hetzner (automatisiert, tägliche inkrementelle Snapshots, 7 Tage Aufbewahrung).
- Monitoring der VM-Verfügbarkeit mit automatischer Benachrichtigung bei Ausfällen.
- Notfallwiederherstellungsverfahren dokumentiert; Wiederherstellungszeit (RTO) und Wiederherstellungspunkt (RPO) nach Hauptvertrag.

7. Integrität

- Git-Versionierung des Wissensspeichers sichert Nachvollziehbarkeit aller Datenänderungen.
- Systemprotokollierung (syslog / journald) auf allen VMs; Protokolle werden für mindestens 30 Tage aufbewahrt.
- Integritätsprüfungen durch Container-Image-Pinning (Digests) bei Docker-Updates.

8. Human-in-the-Loop (Erste 30 Tage)

- In den ersten 30 Tagen des Betriebs führt der Agent keine Aktion eigenständig aus; jede Aktion wird dem Verantwortlichen oder dessen Beauftragten zur Freigabe vorgelegt.
- Protokollierung aller freigegebenen und abgelehnten Aktionen.

9. Datenschutz durch Technik und Voreinstellung (Art. 25 DSGVO)

- Minimalprinzip: Agenten werden so konfiguriert, dass sie nur auf die Daten zugreifen, die zur Aufgabenerfüllung erforderlich sind.
- Keine dauerhafte Speicherung von Klartext-Nachrichten aus LLM-Interaktionen über das für den Wissensspeicher erforderliche Maß hinaus.

10. Organisatorische Maßnahmen

- Dokumentiertes Verfahren zur Behandlung von Datenschutzverletzungen (Incident Response).
- Laufende Überprüfung und Aktualisierung der Sicherheitsmaßnahmen.
- Schriftliche Vereinbarungen mit allen Unterauftragsverarbeitern (SCC, AVV).

Agentenkollege · David Kogan · Engernweg 79 · 33100 Paderborn · datenschutz@agentenkollege.de