AGENTENKOLLEGE · DAVID KOGAN

Technische und organisatorische Maßnahmen

Anlage 2 zum AVV · nach Art. 32 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.

Die nachstehenden technischen und organisatorischen Maßnahmen (TOM) beschreiben den Stand der Sicherheitsvorkehrungen, die David Kogan (Einzelunternehmen, Geschäftsbezeichnung „Agentenkollege") als Auftragsverarbeiter gemäß Art. 32 DSGVO zum Schutz personenbezogener Daten implementiert hat. Sie beziehen sich konkret auf den Betrieb Managed-KI-Agenten, die im Auftrag von Kunden auf dedizierten virtuellen Maschinen bei Hetzner Cloud in Deutschland ausgeführt werden. Die Maßnahmen gelten ergänzend zu den Regelungen im Hauptvertrag und im Auftragsverarbeitungsvertrag (AVV).

1. Vertraulichkeit

1.1 Zutrittskontrolle (physische Sicherheit)

Die physische Infrastruktur wird vollständig durch den Hosting-Sub-Auftragsverarbeiter Hetzner Online GmbH betrieben. Hetzner betreibt seine Rechenzentren in Nürnberg und Falkenstein (Deutschland) nach ISO/IEC 27001 und gewährleistet:

- Gesicherter Zutritt zu Rechenzentrumsgebäuden (Zutrittskontrollsysteme, Videoüberwachung, Sicherheitspersonal);
- Trennung von Serverhallen und allgemein zugänglichen Bereichen;
- Protokollierung aller Zutrittsereignisse.

Agentenkollege selbst unterhält keine eigenen Serverräume. Nachweise zur physischen Sicherheit von Hetzner sind auf Anfrage erhältlich (ISO-Zertifikat, Hetzner-Datenschutzdokumentation).

1.2 Zugangskontrolle (logischer Zugang zur Infrastruktur)

- **SSH-Key-Only-Authentifizierung:** Der administrative Zugriff auf alle virtuellen Maschinen erfolgt ausschließlich per SSH mit asymmetrischem Schlüsselpaar (Ed25519 oder RSA ≥ 4096 Bit). Passwort-Authentifizierung ist systemseitig deaktiviert.
- **Keine exponierten Admin-Ports:** Verwaltungsports (SSH, Administrationsdienste) sind nicht öffentlich erreichbar; der Zugang erfolgt über restriktive Firewall-Regeln (Hetzner Cloud Firewall + UFW auf VM-Ebene). Admin-Zugriff ist auf bekannte IP-Adressen beschränkt.
- **TLS-Verschlüsselung aller Endpunkte:** Alle nach außen exponierten Dienste laufen hinter einem Caddy Reverse Proxy mit automatisch erneuertem TLS-Zertifikat (Let's Encrypt). Unverschlüsseltes HTTP wird systemseitig auf HTTPS umgeleitet.
- **Keine Root-Logins:** Der direkte SSH-Login als root ist deaktiviert; administrative Operationen erfolgen per sudo mit dediziertem Service-Account.

1.3 Zugriffskontrolle (Berechtigungen im laufenden Betrieb)

- **Prinzip der minimalen Rechtevergabe:** Jeder KI-Agent verfügt nur über die Systemrechte und API-Berechtigungen, die zur Erfüllung seiner konkreten Aufgabe erforderlich sind. Nicht benötigte Dienste, Ports und Dateisystempfade sind gesperrt.
- **Kundenseitig freigegebene Zugänge:** Der Agent greift auf externe SaaS-Systeme (CRM, ERP, E-Mail etc.) ausschließlich über Zugangsdaten an, die der Auftraggeber explizit für diesen Zweck bereitgestellt und freigegeben hat. Agentenkollege erhebt keine Zugangsdaten zu Systemen, für die keine ausdrückliche Freigabe vorliegt.
- **Isolierte Laufzeitumgebung:** Jeder Agent läuft in einem eigenen Docker-Container innerhalb seiner dedizierten VM. Container haben keinen Zugriff auf das Host-Filesystem außerhalb definierter Bind-Mounts.
- **Tool-Berechtigungen über Composio:** Die Anbindung von SaaS-Integrationen erfolgt über Composio; OAuth-Scopes und API-Schlüssel werden auf das für den jeweiligen Use-Case nötige Minimum begrenzt.

1.4 Trennungskontrolle

Dies ist die zentrale Datenisolations-Architekturentscheidung von Agentenkollege:

- **Dedizierte VM pro Agent und Kunde:** Jeder Managed-Agent läuft auf einer eigenen, ausschließlich für diesen Kunden und diesen Agenten reservierten virtuellen Maschine bei Hetzner Cloud. Es findet kein Mischbetrieb statt. Kundendaten verschiedener Auftraggeber sind nicht nur logisch, sondern auf Betriebssystemebene vollständig getrennt.
- **Isolierter Wissensspeicher:** Der Obsidian-Vault (git-versionierter Wissensspeicher des Agenten) ist agent-spezifisch und auf das Dateisystem der jeweiligen VM beschränkt. Es gibt kein gemeinsames Wissens-Repository über Kundengrenzen hinweg.
- **Isolierte Mailbox:** Jeder Agent verfügt über eine dedizierte Mailbox (AgentMail), die ausschließlich dem jeweiligen Agenten und Kunden zugeordnet ist.
- **Netzwerktrennung:** VMs verschiedener Kunden kommunizieren nicht miteinander; interne Kommunikation wird durch Hetzner-Netzwerkisolation und VM-seitige Firewall-Regeln unterbunden.

1.5 Pseudonymisierung und Verschlüsselung

- **Verschlüsselung in Transit:** Alle Datenübertragungen zwischen Agent und externen Diensten sowie zwischen Kunden und der Admin-Oberfläche erfolgen TLS-verschlüsselt (mindestens TLS 1.2, präferiert TLS 1.3).
- **Hetzner-seitige Verschlüsselung:** Hetzner Cloud Volumes unterstützen Verschlüsselung; diese wird für Backup-Volumes genutzt.
- **Vault-Daten:** Der git-versionierte Obsidian-Vault wird täglich verschlüsselt in EU-Storage gesichert (siehe Abschnitt 3).
- **Keine unnötige Klartext-Persistenz:** API-Schlüssel und Zugangsdaten werden als Umgebungsvariablen oder in einem Secret-Store übergeben, nicht im Quellcode oder in Konfigurationsdateien im Klartext abgelegt.

2. Integrität

2.1 Weitergabekontrolle

- **TLS für alle Übertragungen:** Personenbezogene Daten werden ausschließlich TLS-verschlüsselt übertragen. Unverschlüsselte Übertragungswege sind technisch unterbunden (HTTPS-Redirect, HSTS-Header).
- **Kein ungesicherter E-Mail-Versand sensibler Inhalte:** Soweit der Agent E-Mails verarbeitet oder versendet, geschieht dies über SMTP mit STARTTLS/TLS-Erzwingung über den AgentMail-Dienst.
- **Protokollierung von Datenweitergaben:** Abrufe externer APIs und Datenübermittlungen werden in den Aktionsprotokollen des Agents festgehalten (siehe 2.2).

2.2 Eingabekontrolle

- **Aktionsprotokolle:** Jede Aktion, die der Agent durchführt (API-Aufruf, Dateiänderung, E-Mail-Versand, Tool-Nutzung), wird mit Zeitstempel, Aktion und Ergebnis protokolliert. Protokolle werden auf der jeweiligen VM vorgehalten und sind für den Kunden auf Anfrage einsehbar.
- **Human-in-the-Loop-Modus (erste 30 Tage):** In den ersten 30 Betriebstagen jedes neu eingesetzten Agenten wird jede Aktion vor der Ausführung einem menschlichen Reviewer (Agentenkollege und/oder Kundenseitig) zur Freigabe vorgelegt. Erst nach expliziter Bestätigung wird die Aktion ausgeführt. Dieser Modus stellt sicher, dass Datenverarbeitungen in der Einführungsphase nachvollziehbar und kontrollierbar bleiben.
- **Versionierung des Wissensspeichers:** Alle Änderungen am Obsidian-Vault des Agenten sind git-versioniert. Änderungen sind jederzeit nachvollziehbar, rücksetzbar und auditierbar.
- **Keine unkontrollierte autonome Datenweitergabe:** Der Agent darf Daten nur an Dienste und Endpunkte übermitteln, die im Scope des jeweiligen Agenten explizit konfiguriert sind.

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

- **Echtzeit-Monitoring:** Alle Agenten-VMs und exponierten Endpunkte werden durch Uptime Kuma kontinuierlich überwacht. Bei Ausfall erfolgt eine automatische Alarmierung.
- **Redundante Rechenzentrumsstandorte:** Die Infrastruktur ist so ausgelegt, dass VMs auf zwei Hetzner-Standorte in Deutschland (Nürnberg und Falkenstein) verteilt werden können, um Standortausfälle aufzufangen.
- **Recovery Point Objective (RPO): 24 Stunden.** Tägliche Backups gewährleisten, dass im Fehlerfall maximal der Datenverlust eines Tages entstehen kann.
- **Recovery Time Objective (RTO): 4 Stunden.** Im Wiederherstellungsfall wird angestrebt, den Betrieb innerhalb von 4 Stunden wieder aufzunehmen.

3.2 Datensicherung und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- **Tägliche Backups:** VM-Snapshots und der git-versionierte Vault werden täglich gesichert. Backup-Ziel ist EU-Storage (ausschließlich Standorte innerhalb der Europäischen Union).
- **Verschlüsselte Backup-Übertragung und -Speicherung:** Backup-Daten werden vor der Übertragung in den EU-Storage-Bucket verschlüsselt.

- **Wiederherstellbarkeit:** Backups werden regelmäßig auf Vollständigkeit und Wiederherstellbarkeit geprüft. Testwiederherstellungen werden dokumentiert.
- **Caddy und Konfigurationsmanagement:** Alle Konfigurationsdateien (Caddy, Docker-Compose, Agent-Konfigurationen) sind versioniert und ermöglichen eine schnelle Neuprovisioning der gesamten Agent-Umgebung aus dem Backup.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Auftragskontrolle

- **AVV mit allen Sub-Auftragsverarbeitern:** Mit jedem Dienstleister, der im Rahmen des Betriebs personenbezogene Daten verarbeitet, besteht ein gültiger Auftragsverarbeitungsvertrag. Dies umfasst insbesondere:

Sub-Auftragsverarbeiter	Funktion	Sitz / Datenstandort	Drittland-Absicherung
Hetzner Online GmbH	VM-Hosting, Speicher	Deutschland (NUE/FSN)	Kein Drittstaattransfer; Standard-AVV
Composio Inc.	SaaS-Tool-Integrationen	USA	SCC + TIA erforderlich
AgentMail	Agent-Mailboxen	USA	SCC + TIA erforderlich
LLM-Anbieter (je nach Agent: Anthropic, OpenAI, Mistral, Z.AI / GLM)	KI-Inferenz	USA / EU	USA: SCC + TIA erforderlich; EU-Anbieter ohne Drittland-Transfer. Modelle aus China (Moonshot/Kimi) werden nicht eingesetzt.

- **Aktuelle AVV-Liste:** Agentenkollege führt eine interne Liste aller aktiven Sub-Auftragsverarbeiter mit AVV-Status, Datenstandort und ggf. Drittland-Absicherung. Diese ist auf begründete Anfrage des Auftraggebers einsehbar.

4.2 Datenschutz-Management

- **Verarbeitungsverzeichnis:** Agentenkollege führt ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO.
- **Privacy by Design / Privacy by Default:** Neue Agenten-Deployments und technische Änderungen werden vor dem Rollout auf Datenschutzrelevanz geprüft. Standardmäßig werden nur die Daten verarbeitet, die für den jeweiligen Auftragsgegenstand zwingend erforderlich sind.
- **Datensparsamkeit:** Im Wissensspeicher (Obsidian-Vault) werden nur aufgabenrelevante Informationen abgelegt. Nicht mehr benötigte Daten werden auf Anweisung des Auftraggebers oder nach Vertragsende gelöscht bzw. zurückgegeben.

4.3 Incident-Response und Meldeprozess

- **Erkennung:** Sicherheitsrelevante Ereignisse (unberechtigte Zugriffe, ungewöhnliches Systemverhalten, Datenverluste) werden durch das Monitoring (Uptime Kuma, System-Logs) erkannt und lösen umgehend eine manuelle Prüfung aus.

- **Meldepflicht gegenüber dem Auftraggeber:** Wird eine Datenpanne festgestellt oder ist eine solche nicht auszuschließen, informiert Agentenkollege den Auftraggeber unverzüglich, spätestens innerhalb von **36 Stunden** nach Kenntnisnahme, um die Frist nach Art. 33 DSGVO (72 Stunden gegenüber der Aufsichtsbehörde) einhalten zu können. Die Meldung enthält Art, Umfang, wahrscheinliche Ursache und bereits eingeleitete Maßnahmen.
- **Dokumentation:** Sicherheitsvorfälle werden intern dokumentiert, einschließlich Zeitverlauf, Ursache, Auswirkung und getroffener Abhilfemaßnahmen.

4.4 Regelmäßige Überprüfung der Maßnahmen

- **Jährliche TOM-Überprüfung:** Die vorliegenden TOM werden mindestens einmal jährlich sowie anlässlich wesentlicher technischer oder organisatorischer Änderungen überprüft und ggf. aktualisiert.
- **Patch-Management:** Betriebssystem- und Software-Updates werden zeitnah eingespielt, sicherheitskritische Patches bevorzugt behandelt. Docker-Images werden regelmäßig auf aktualisierte Basis-Images umgestellt.
- **Überprüfung der Sub-Auftragsverarbeiter:** Die Datenschutz- und Sicherheitsstandards aller Sub-Auftragsverarbeiter werden in regelmäßigen Abständen und bei Vertragsänderungen neu bewertet (z. B. Prüfung aktueller Zertifikate, TIA-Aktualität).
- **Backup-Tests:** Die Wiederherstellbarkeit von Backups wird periodisch durch Testwiederherstellungen in isolierter Umgebung verifiziert und dokumentiert.

Hinweis zum aktuellen Entwicklungsstand

Agentenkollege ist derzeit ein Einzelunternehmen ohne angestellte Mitarbeiter. Die beschriebenen Maßnahmen sind auf diesen Betriebsmaßstab zugeschnitten: technische Kontrollen ersetzen weitgehend die organisatorischen Strukturen, die in größeren Unternehmen durch interne Abteilungen, dedizierte DSB-Rollen oder formalisierte Prozesse abgebildet werden. Mit dem Wachstum des Unternehmens, insbesondere bei Einstellung von Personal, Erweiterung des Kundenstamms oder Aufnahme besonders sensibler Verarbeitungskategorien, werden diese TOM entsprechend fortgeschrieben: formale Schulungskonzepte, eine Datenschutzbeauftragten-Rolle (sofern gesetzlich erforderlich), erweiterte Zugriffsverwaltung und tiefergehende Auditierbarkeit sind dann Teil der nächsten Ausbaustufe.

Ort, Datum	Ort, Datum
David Kogan Agentenkollege Auftragsverarbeiter	**[Name, Unternehmen]** Auftraggeber