Anhang zu den AGB: Auftragsbearbeitung (AVV)

nach Art. 9 des Bundesgesetzes über den Datenschutz (DSG, revidierte Fassung vom 1. September 2023)

Version 1.0, 28. September 2026. Anhang zu den Allgemeinen Geschäftsbedingungen von Kantello (AGB) derselben Version.

Parteien: die Auftraggeberin gemäss Auftrag (die «Verantwortliche», in den AGB «die Auftraggeberin») und die Samsa Labs AG, Pilatusstrasse 18, 6003 Luzern, Schweiz, UID CHE-143.735.292, Marke Kantello (die «Auftragsbearbeiterin», in den AGB «die Auftragnehmerin»). Dieser Anhang gilt mit der Unterzeichnung des Auftrags, der auf die AGB und diesen Anhang verweist.

1. Gegenstand und Dauer

1.1 Die Auftragsbearbeiterin bearbeitet für die Verantwortliche Personendaten, um die Leistungen aus dem Auftrag und den AGB zu erbringen: den Bau, den Betrieb und die Pflege der Website der Verantwortlichen gemäss Auftrag, den Betrieb des KI-Agenten der Verantwortlichen und seines Servers, und die damit verbundenen Berichte und Entwürfe.

1.2 Dieser Anhang gilt, solange der Vertrag aus Auftrag und AGB gilt, und darüber hinaus, bis die Auftragsbearbeiterin alle Personendaten nach Ziffer 10 übergeben, gelöscht oder zurückgegeben hat.

1.3 Dieser Anhang geht dem Auftrag und den AGB in Datenschutzfragen vor. Soweit die Datenschutz-Grundverordnung der EU (DSGVO) auf eine Bearbeitung anwendbar ist (Art. 3 Abs. 2 DSGVO), gilt dieser Anhang zugleich als Vertrag nach Art. 28 Abs. 3 DSGVO; die Begriffe «Verantwortliche» und «Auftragsbearbeiterin» entsprechen dann «Verantwortlicher» und «Auftragsverarbeiter».

2. Rollen

2.1 Die Verantwortliche entscheidet über Zweck und Mittel der Bearbeitung. Ihr gehören ihre Inhalte, ihr Code, ihre Domain und alle ihre Daten (AGB Ziffer 7), auch dort, wo sie in einem Konto der Auftragsbearbeiterin liegen.

2.2 Die Auftragsbearbeiterin bearbeitet Personendaten nur im Auftrag und nach den Weisungen der Verantwortlichen und nur, soweit es für die vereinbarten Leistungen nötig ist. Sie nutzt die Daten nicht für eigene Zwecke.

2.3 Es gibt zwei Arten von Konten:

- **Konten der Verantwortlichen:** OpenAI (das Sprachmodell ihres Agenten), Google (Search Console, Google Analytics 4, Google Tag Manager, Google Ads, Google-Cloud-Projekt), Cloudflare (Website, Zone, Web-Zugang zum Agenten (Cloudflare Tunnel und Cloudflare Access)) und der Mail-Anbieter für das Formular. Die Verantwortliche hält diese Konten und den Vertrag mit dem Anbieter selbst und akzeptiert dessen Datenverarbeitungsbedingungen selbst. Diese Anbieter sind ihre eigenen Auftragsbearbeiter, **nicht Unterauftragsbearbeiter der Auftragsbearbeiterin**. Die Auftragsbearbeiterin arbeitet dort nur mit

Kantello
Samsa Labs AG
Pilatusstrasse 18
6003 Luzern

Kontakt
kantello.com
hi@kantello.com
+41 41 505 00 14

den Rollen, die die Verantwortliche ihr gibt; im Cloudflare-Konto als Mitglied mit der Rolle Super Administrator.
- **Konten der Auftragsbearbeiterin:** Hetzner (Server des Agenten und Sicherungen), GitHub (Repository), Tailscale (privates Netz für die Verwaltung des Servers) und die Werkzeuge, mit denen die Auftragsbearbeiterin die Website baut und prüft. Sie hält diese Konten, bezahlt sie und schliesst die Verträge selbst; die Anbieter sind ihre Unterauftragsbearbeiter nach Ziffer 7 und Anhang 2.

2.4 Eigene Bearbeitung der Auftragsbearbeiterin: Geschäftskontaktdaten der Verantwortlichen (Namen, Funktionen, E-Mail-Adressen, Termine, Rechnungsdaten) bearbeitet die Auftragsbearbeiterin als eigene Verantwortliche für die Abwicklung des Vertrags; das fällt nicht unter diesen Anhang. E-Mails der Verantwortlichen an hi@kantello.com liest und beantwortet der Agent der Auftragsbearbeiterin mit Sprachmodellen von OpenAI über das OpenAI-Konto der Samsa Labs AG; seine Antworten tragen die Zeile «Diese Nachricht wurde mit KI-Unterstützung verfasst.» Dieser Agent hält kein Konto der Verantwortlichen.

3. Art und Zweck der Bearbeitung, Datenkategorien, betroffene Personen

3.1 Die Bearbeitung ist in Anhang 3 im Einzelnen beschrieben. Zusammengefasst:

Bereich	Zweck	Datenkategorien	Betroffene Personen
Website (Hosting, Auslieferung)	Auslieferung der Seiten, Schutz vor Missbrauch	IP-Adresse, Browser, aufgerufene Seite, Zeitpunkt (Server-Logs des Hosters); Cookie-Wahl	Besucherinnen und Besucher der Website der Verantwortlichen
Kontaktformular	Zustellung von Anfragen an die Verantwortliche, Spam-Schutz, Conversion-Messung	Vorname, Nachname, E-Mail-Adresse, Mitteilung; weitere Angaben eines Formulars nach dem Umfang, der beim Intake festgelegt wird; IP-Adresse und Zeit beim Absenden (Spam-Schutz); Ereignis «Formular zugestellt» ohne Inhalt	Personen, die eine Anfrage senden (Interessentinnen, Interessenten, Kundinnen, Kunden)
Messung (Google Tag Manager, Google Analytics 4, Google Ads)	Nutzung der Website verstehen; Anfragen aus Anzeigen zählen	Nach Zustimmung: Cookies, Gerätetyp, ungefähre Region, Seitenaufrufe, Ereignisse; ohne Zustimmung nur Pings ohne Cookies und Kennung (Consent Mode v2, erweitert)	Besucherinnen und Besucher
KI-Agent (Website-Änderungen, Berichte, Entwürfe)	Website pflegen und ändern; Wochenbericht; Entwürfe für Beiträge, Anzeigen und E-Mails	Chat-Nachrichten und Sitzungen der Mitarbeitenden mit Zugang; Inhalte der Website (Team-Namen, Fotos); Kennzahlen aus Google Analytics 4, Search Console und Google Ads (aggregiert, Suchanfragen); Bestellzahlen eines Shops über dessen Schnittstelle (Anzahl, Umsatz), wenn angeschlossen; in E-Mail-Entwürfen: Name, E-Mail-Adresse und Anliegen der Empfängerin oder des Empfängers, soweit das Team sie dem Agenten gibt	Mitarbeitende der Verantwortlichen; Kundinnen, Kunden und Interessenten (nur in Entwürfen auf Anweisung); Besucherinnen und Besucher (aggregiert); Kundinnen und Kunden eines Shops (nur Zahlen, keine Namen, sofern nicht beim Intake anders festgelegt)

Bereich	Zweck	Datenkategorien	Betroffene Personen
Web-Zugang zum Agenten (agent.‹Domain der Verantwortlichen›)	Anmeldung der Mitarbeitenden, Schutz des Zugangs	E-Mail-Adresse, Zeitpunkt, IP-Adresse, Land und Browser der Anmeldung (Cloudflare Access im Konto der Verantwortlichen); Kennung des gekoppelten Browsers (mit Zuordnung zur Person auf dem Server)	Mitarbeitende der Verantwortlichen
Freigaben	Aufzeichnung jedes Ja und Nein zu einer Handlung nach aussen und jedes Ein- und Ausschaltens von Full Access und Autopilot (AGB Ziffer 9.7)	Name der freigebenden Person, Kennung ihres gekoppelten Browsers, Entscheid, Datum, Vorlage; beim Ein- und Ausschalten Modus und Bereich	Personen der Verantwortlichen mit Zugang zum Agenten
Repository und Bau der Website	Code und Inhalte verwalten, bauen, prüfen, veröffentlichen	Inhalte der Website: Namen und Fotos des Teams, Firmenangaben, Rechtstexte; keine Besucher- oder Formulardaten	Mitarbeitende der Verantwortlichen
Intake, Prüfberichte, Support	Bestandesaufnahme, Baseline, Bau und Prüfung der Website, Support	Exporte aus Search Console, Google Analytics 4, Google Ads (aggregiert); Bildschirmfotos der Website; Notizen zu Gesprächen	Mitarbeitende der Verantwortlichen; Besucherinnen und Besucher (aggregiert)

Kommt ein weiterer Chat-Kanal zum Agenten dazu (zum Beispiel Microsoft Teams), sobald er eingerichtet und freigegeben ist, wird die Bearbeitung dann in dieser Tabelle und in Anhang 2 und 3 ergänzt (Ziffer 7.2).

3.2 Besonders schützenswerte Personendaten (Art. 5 lit. c DSG) sind nicht Gegenstand der Bearbeitung. Trifft die Auftragsbearbeiterin dennoch auf solche Daten (zum Beispiel in einer Formularanfrage), bearbeitet sie diese nur zur Zustellung an die Verantwortliche.

4. Weisungen

4.1 Weisungen erteilt die Verantwortliche schriftlich (E-Mail genügt) oder im Chat mit dem Agenten; sie werden im Entscheidungsprotokoll des Repositories festgehalten. Der Auftrag, die AGB, der nach dem Intake bestätigte Umfang und dieser Anhang gelten als erste Weisungen.

4.2 Hält die Auftragsbearbeiterin eine Weisung für rechtswidrig, teilt sie das der Verantwortlichen unverzüglich mit und darf die Ausführung aussetzen, bis die Verantwortliche die Weisung bestätigt oder ändert.

4.3 Weisungsberechtigt gegenüber der Auftragsbearbeiterin sind die Personen, die der Auftrag nennt (Unterzeichnende und Ansprechperson), und weitere Personen, die die Verantwortliche schriftlich benennt. Aufträge an den Agenten erteilen die Personen, denen die Verantwortliche Zugang zum Agenten gibt. Dasselbe gilt für das Einschalten von Full Access und Autopilot (AGB Ziffer 9.7): es ist eine Weisung der Verantwortlichen für den Bereich und die Dauer des Modus und wird im Freigabe-Register festgehalten. Handlungen nach aussen geben nur Personen mit Zugang zum Agenten frei (AGB Ziffer 9.2), einzeln oder mit einem Autopiloten.

5. Pflichten der Auftragsbearbeiterin

5.1 **Vertraulichkeit.** Die Auftragsbearbeiterin behandelt alle Personendaten vertraulich. Personen, die Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet. Heute (Stand dieser Version) ist das Niklas Jung; kommt eine weitere Person dazu (zum Beispiel eine Freelancerin oder ein Freelancer), teilt die Auftragsbearbeiterin das vorher mit und verpflichtet die Person schriftlich.

5.2 **Datensicherheit.** Die Auftragsbearbeiterin trifft die technischen und organisatorischen Massnahmen in Anhang 1 (Art. 8 DSG). Sie passt sie dem Stand der Technik an und verringert das Schutzniveau nicht ohne Zustimmung der Verantwortlichen. Schaltet eine Person mit Zugang Full Access oder einen Autopiloten ein (AGB Ziffer 9.7), ist das die Zustimmung der Verantwortlichen, soweit der Modus eine Massnahme nach Anhang 1 lockert; die Massnahmen, die AGB Ziffer 9.9 nennt, gelten in jedem Modus.

5.3 **Unterstützung bei Rechten der betroffenen Personen.** Verlangt eine Person Auskunft, Berichtigung, Löschung, Herausgabe oder Datenübertragung (Art. 25 ff. DSG), unterstützt die Auftragsbearbeiterin die Verantwortliche innert 5 Arbeitstagen mit den nötigen Informationen und Handlungen. Anfragen, die bei der Auftragsbearbeiterin eingehen, leitet sie unverzüglich an die Verantwortliche weiter und beantwortet sie nicht selbst. Anfragen an die Auftragsbearbeiterin gehen an dpa@samsalabs.com.

5.4 **Meldung von Verletzungen der Datensicherheit.** Die Auftragsbearbeiterin meldet der Verantwortlichen so rasch als möglich, spätestens innert 72 Stunden nach Kenntnis, jede Verletzung der Datensicherheit (Art. 24 Abs. 3 DSG): was geschehen ist, welche Daten und Personen betroffen sind, welche Folgen zu erwarten sind, was sie getan hat und was sie vorschlägt. Die Meldung an den EDÖB und an die betroffenen Personen bleibt Sache der Verantwortlichen; die Auftragsbearbeiterin unterstützt sie dabei. Als Verletzung gilt auch, wenn die Sicherheitsprüfung des Agenten-Servers (Anhang 1, Ziffer 6) ein Geheimnis dort findet, wo der Agent es lesen könnte.

5.5 **Verzeichnis und Nachweis.** Die Auftragsbearbeiterin führt ein Verzeichnis ihrer Bearbeitungen für die Verantwortliche, soweit Art. 12 DSG es verlangt, und hält die Nachweise nach Ziffer 9 bereit.

5.6 **Datenschutz-Folgenabschätzung.** Muss die Verantwortliche eine Datenschutz-Folgenabschätzung durchführen (Art. 22 DSG), unterstützt die Auftragsbearbeiterin sie mit den Informationen, die nur sie hat.

5.7 **Keine Rechtstexte.** Die Auftragsbearbeiterin schreibt keine Datenschutzerklärung und keine Cookie-Richtlinie für die Verantwortliche. Sie nennt ihr, was die Website technisch tut (welche Dienste laden, wann, mit welchen Cookies), damit die Verantwortliche oder ihre Rechtsberatung die Texte schreiben kann.

6. Technische und organisatorische Massnahmen

Die Massnahmen stehen in Anhang 1. Sie folgen dem Grundsatz: die Konten der Auftragsbearbeiterin sind pro Kundin getrennt, und ihre Zugangsschlüssel liegen nur beim Tool-Broker; die Auftragsbearbeiterin und der Agent erhalten in den Konten der Verantwortlichen nur die Rolle, die nötig ist; kein Geheimnis liegt dort, wo der Agent es lesen kann; der Server nimmt keine Verbindung aus dem Internet an; keine Handlung nach aussen ohne ein aufgezeichnetes, einmaliges Ja oder einen aufgezeichneten Autopiloten, den eine Person mit Zugang eingeschaltet hat (AGB Ziffer 9.7).

7. Unterauftragsbearbeiter

7.1 Die Verantwortliche stimmt den Unterauftragsbearbeitern in Anhang 2, Teil A zu. Die Anbieter in Anhang 2, Teil B sind keine Unterauftragsbearbeiter: die Verantwortliche hält diese Konten selbst (Ziffer 2.3); der Vertrag besteht direkt zwischen ihr und dem Anbieter.

7.2 Will die Auftragsbearbeiterin einen weiteren Unterauftragsbearbeiter beiziehen oder einen ersetzen, teilt sie das der Verantwortlichen mindestens 30 Tage vorher schriftlich mit. Die Verantwortliche kann innert dieser Frist aus sachlichen Gründen widersprechen. Einigen sich die Parteien nicht, kann die Verantwortliche den Vertrag für die betroffene Leistung kündigen.

7.3 Die Auftragsbearbeiterin schliesst mit ihren Unterauftragsbearbeitern (Anhang 2, Teil A) Datenverarbeitungsbedingungen ab, die den Pflichten dieses Anhangs entsprechen; bei diesen Anbietern sind das deren Standardbedingungen, die die Auftragsbearbeiterin vor dem Beizug prüft.

8. Bekanntgabe ins Ausland

8.1 Personendaten werden in die Länder in Anhang 2 bekanntgegeben. Für Staaten mit angemessenem Datenschutz nach Anhang 1 der Datenschutzverordnung (unter anderem die Mitgliedstaaten der EU, darunter Deutschland, Irland und Frankreich) braucht es keine zusätzliche Garantie.

8.2 Für die USA stützt sich die Bekanntgabe auf die Zertifizierung des Anbieters unter dem Swiss-U.S. Data Privacy Framework, soweit der Anbieter zertifiziert ist, und sonst auf die Standardvertragsklauseln des Anbieters mit den vom EDÖB anerkannten Anpassungen für die Schweiz. Anhang 2 nennt die Grundlage pro Anbieter mit dem Datum der Prüfung; die Auftragsbearbeiterin prüft die Zertifizierungen vor dem Go-live der Website der Verantwortlichen erneut.

8.3 Für andere Staaten ohne angemessenen Datenschutz stützt sich die Bekanntgabe auf die Garantie, die Anhang 2 pro Anbieter nennt. Fehlt dort eine Garantie, gibt die Auftragsbearbeiterin keine Personendaten der Verantwortlichen in diesen Staat bekannt.

9. Kontrollrechte

9.1 Die Auftragsbearbeiterin weist der Verantwortlichen auf Verlangen nach, dass sie diesen Anhang einhält: mit dem Zugangsregister im Repository (`docs/ACCESS.md`), den Berichten der Sicherheitsprüfung des Agenten-Servers (Anhang 1, Ziffer 6), dem Register der Freigaben und dem Protokoll der Sicherungen.

9.2 Reicht das nicht, kann die Verantwortliche oder eine von ihr beauftragte, zur Vertraulichkeit verpflichtete Person die Bearbeitung prüfen: einmal pro Vertragsjahr, mit 30 Tagen Ankündigung, während der Geschäftszeiten, auf Kosten der Verantwortlichen, ausser die Prüfung deckt einen wesentlichen Verstoss auf. Die Auftragsbearbeiterin gewährt Zugang zu den Nachweisen, nicht zu Geheimnissen anderer Kundinnen und Kunden.

10. Übergabe, Löschung und Rückgabe

10.1 Nach dem Ende des Vertrags übergibt die Auftragsbearbeiterin der Verantwortlichen die Daten in ihren Konten nach AGB Ziffer 8: das Repository und den Zustand des Agenten (auf einem neuen Server im Hetzner-Konto der Verantwortlichen). Den alten Server, seine Snapshots und Sicherungen löscht sie, nachdem die Verantwortliche die Übergabe bestätigt hat.

10.2 Alle übrigen Personendaten der Verantwortlichen, die die Auftragsbearbeiterin auf eigenen Systemen hält (Prüfberichte, Exporte, Notizen), löscht sie innert 30 Tagen nach der Übergabe und bestätigt die Löschung schriftlich.

10.3 Daten in den Konten der Verantwortlichen bleiben bei der Verantwortlichen. Die Auftragsbearbeiterin gibt ihre Rollen und Mitgliedschaften zurück, widerruft ihre Zugangsschlüssel und dokumentiert die Rotation (AGB Ziffer 8.3).

10.4 Gesetzliche Aufbewahrungspflichten (zum Beispiel für Rechnungen) bleiben vorbehalten; solche Daten werden gesperrt und nur dafür aufbewahrt.

11. Haftung

Die Haftung richtet sich nach den AGB (Ziffer 15) und nach Gesetz. Für Verstösse gegen zwingendes Datenschutzrecht gilt die gesetzliche Haftung.

12. Schlussbestimmungen

12.1 Änderungen dieses Anhangs brauchen die Schriftform (E-Mail genügt); für eine neue Version gilt AGB Ziffer 18. Änderungen von Anhang 2 folgen Ziffer 7.2.

12.2 Dieser Anhang untersteht schweizerischem Recht. Gerichtsstand ist Luzern; zwingende Gerichtsstände bleiben vorbehalten.

Anhang 1: Technische und organisatorische Massnahmen

Die Massnahmen beschreiben, was die Kantello-Plattform tut (Stand dieser Version, 28. September 2026). Sie gelten für die Website der Verantwortlichen und den Server ihres Agenten.

1. Konten und Zugänge

- Die Konten der Auftragsbearbeiterin sind pro Kundin getrennt: ein Hetzner-Projekt, ein GitHub-Repository und ein eigenes Kennzeichen (Tag) im privaten Tailscale-Netz nur für die Verantwortliche. Jeder Zugangsschlüssel für die Einrichtung gilt nur für die Verantwortliche und liegt nur beim Tool-Broker (Ziffer 3). Einen Server oder eine andere kostenpflichtige Ressource legt die Auftragsbearbeiterin nur mit dem einmaligen Ja ihrer Geschäftsführung an.
- In den Konten der Verantwortlichen erhalten die Auftragsbearbeiterin und der Agent nur die Rolle, die nötig ist (Google Ads, wenn das Abo den Kanal umfasst und die Verantwortliche die Rolle vergibt: Schreibzugriff nur innerhalb der Ausgabenobergrenzen, die die Verantwortliche im Konto setzt, AGB Ziffer 10.4). Im Cloudflare-Konto ist die Auftragsbearbeiterin Mitglied mit der Rolle Super Administrator, weil nur diese Rolle kontoeigene Zugangsschlüssel anlegen kann; die Verantwortliche bleibt selbst Super Administrator.
- Jeder Zugang steht mit Inhaberin, Umfang und Datum im Zugangsregister im Repository (`docs/ACCESS.md`).
- Logins und Zwei-Faktor-Schutz für die Konten der Verantwortlichen richtet die Verantwortliche selbst ein, im eigenen Browser. Zugangsdaten werden über die Einladung des Anbieters übergeben, nie per E-Mail, Chat oder Ticket.
- Geheimnisse stehen nie im Repository, in Protokollen, in Tickets oder auf Befehlszeilen. Build-Werte liegen als Geheimnisse der GitHub-Deployment-Umgebungen; Laufzeit-Geheimnisse des Formulars als Cloudflare-Pages-Variablen. Ein Build-Protokoll zeigt nur «vorhanden» oder «fehlt», nie einen Wert.

2. Website

- Statische Website ohne Datenbank und ohne Kundendaten; ein Shop der Verantwortlichen ist ein getrenntes System und wird nicht angefasst.
- Cookie-Banner mit gleichwertigem Akzeptieren und Ablehnen; ausser dem Google-Tag ohne Cookies und Kennung (Consent Mode v2, erweitert) lädt kein Drittinhalt vor der Zustimmung; der Spam-Schutz des Formulars (Cloudflare Turnstile) lädt erst, wenn jemand das Formular benutzt.

- Formularanfragen werden nicht auf der Website gespeichert, sondern über den Mail-Anbieter der Verantwortlichen an deren Postfach zugestellt; Spam-Schutz durch Turnstile, Mindest-Ausfüllzeit und Begrenzung der Anfragen pro Adresse.
- Sicherheits-Header (unter anderem Content-Security-Policy, HSTS, Referrer-Policy), HTTPS, Vorschau nur hinter Cloudflare Access und ohne Indexierung; die Vorschau sendet keine Conversion.
- Jede Änderung geht über einen Pull Request und die automatischen Prüfungen des Repositories; die Produktion wird nur nach dem Ja einer Freigabeperson (AGB Ziffer 9.2) oder im Autopiloten (AGB Ziffer 9.7) veröffentlicht; Rückzug jederzeit.

3. Server des Agenten

- Eigener Server nur für die Verantwortliche bei Hetzner in Deutschland, im Konto der Auftragsbearbeiterin. Die Hetzner-Firewall hat keine eingehende Regel; die Firewall des Servers lässt nur Verbindungen über das private Tailscale-Netz zu; OpenSSH ist nach der Einrichtung abgeschaltet; Gateway und Bedienoberfläche hören nur auf dem Server selbst (localhost). Kein öffentlicher Port. Verwaltet wird der Server nur über Tailscale SSH, im Notfall über die Konsole von Hetzner.
- Der Web-Zugang ist agent.‹Domain der Verantwortlichen›, über Cloudflare Tunnel und Cloudflare Access im Cloudflare-Konto der Verantwortlichen. Der Server baut die Verbindung zu Cloudflare selbst auf (nur ausgehend) und öffnet keinen Port; Cloudflare leitet nur Anfragen weiter, die Cloudflare Access einer freigegebenen Person zugeordnet hat. Die Bedienoberfläche verlangt zusätzlich einen einmal gekoppelten Browser; ein gemeinsames Geheimnis erhält keine Person. Freigaben gibt eine Person in der Bedienoberfläche; es zählt nur ein Ja aus einem gekoppelten Browser einer Person mit Zugang. Dasselbe gilt für das Einschalten von Full Access und Autopilot. Die Verbindungen sind verschlüsselt; Cloudflare entschlüsselt sie in seinem Netz. Verlässt eine Person mit Zugang das Team, werden ihre Anmeldung und die Kopplung ihrer Browser entzogen und jedes gemeinsame Geheimnis des Zugangs erneuert. Der Web-Zugang wird erst freigeschaltet, wenn die Abnahmeprüfung zeigt, dass die Bedienoberfläche keine Freigabe über AGB Ziffer 9 hinaus erweitern und keinen Zugangsschlüssel erreichen kann.
- Getrennte Benutzer: ein Administrator (Anmeldung nur über Tailscale SSH, sudo); der Agent ohne sudo, ohne Login und ohne Schreibrecht auf seinen eigenen Code, seine Konfiguration und seine Regeln; eigene Dienstbenutzer für den Tool-Broker und den Freigabe-Dienst.
- SSH nur mit Schlüssel, kein Root-Login, kein Passwort; automatische Sicherheitsupdates; fail2ban.
- Der Agent hält kein Geheimnis, mit dem er senden, bezahlen, veröffentlichen oder Geld ausgeben könnte, und keinen GitHub-Schlüssel. Solche Geheimnisse liegen beim Tool-Broker in Dateien, die nur root und der Broker lesen. Der Agent erreicht die Hosts dieser Anbieter nicht direkt (Egress-Regeln der Firewall).
- Code und Inhalte, die der Agent ändert, baut und testet der Server nie als Benutzer des Agenten: das geschieht als eigener Benutzer ohne Login und ohne Zugangsschlüssel, in kurzlebigen, abgeschotteten Umgebungen; beim Installieren der Pakete sind lokale, interne und Tailscale-Adressen gesperrt, und die Bildschirmfotos entstehen ohne Netz. Veröffentlicht wird nur, was diese Prüfung bestanden hat. Das gilt in jedem Modus: auch mit Full Access oder im Autopiloten (AGB Ziffer 9.7) wird nur veröffentlicht, was in dieser Umgebung gebaut wurde und die Prüfung bestanden hat; was der Agent mit Full Access selbst ausführt, läuft als sein Benutzer, ohne Zugangsschlüssel.
- Das Bearbeitungswerkzeug des Agenten (Codex) arbeitet nur mit Dateiwerkzeugen in einem eigenen Ordner, ohne Befehlszeile, ohne Web und ohne Zugangsschlüssel; eine Sitzung wird nach 900 Sekunden abgebrochen.
- Jede Handlung nach aussen braucht ein einmaliges, an die genaue Anfrage gebundenes Freigabe-Token. Es entsteht nur, wenn eine Person mit Zugang über den Freigabe-Link der Anfrage aus ihrem gekoppelten Browser zustimmt, oder in einem Bereich, den eine Person mit Zugang auf Autopilot gestellt hat (AGB Ziffer 9.7): dann stellt es der Freigabe-Dienst selbst aus, und das Register vermerkt «Autopilot» mit Person und Zeitpunkt des Einschaltens. Eine unbeantwortete Anfrage verfällt nach 10 Minuten.

Ausserhalb eines Autopiloten gibt es für Handlungen nach aussen kein «Immer erlauben»: die Anfrage bietet nur «einmal erlauben» und «ablehnen» an, und ein anderes Ja wird nicht angenommen. Jedes Ja wird mit Person, gekoppeltem Browser und Zeitpunkt aufgezeichnet, jedes Nein mit Zeitpunkt.

- Befehle, die der Agent auf seinem eigenen Server ausführen will und die nicht auf seiner festen Liste stehen, fragt er ebenfalls in der Bedienoberfläche an. Eine Person mit Zugang kann einen solchen Befehl einmal oder dauerhaft erlauben. Hat eine Person mit Zugang Full Access eingeschaltet (AGB Ziffer 9.7), fragt der Agent nicht; jeder solche Befehl gilt dann als von ihr erlaubt, auch wenn er eine Verbindung ins Internet aufbaut, soweit die Netzregeln des Servers (Egress-Regeln) es zulassen; mit Full Access lassen sie nur Ziele zu, in die eine Bekanntgabe nach Ziffer 8 (Bekanntgabe ins Ausland) erlaubt ist. Eine dauerhafte Erlaubnis ist ein bewusster Entscheid dieser Person; sie wird mit Person und Zeitpunkt aufgezeichnet, steht im Nachweis nach Ziffer 9 und kann von der Auftragsbearbeiterin wieder entfernt werden. Der Agent kann sich keine dauerhafte Erlaubnis erteilen und Full Access nicht selbst einschalten. Eine Befehlserlaubnis und Full Access geben nie eine Handlung nach aussen frei: jede Handlung nach aussen braucht weiterhin ihr eigenes, einmaliges Ja, ausser in einem Autopiloten.
- Der Agent teilt kein Geheimnis mit dem Agenten der Auftragsbearbeiterin und hält kein Token zum Veröffentlichen auf Meta oder LinkedIn.

4. Sprachmodelle

- Der Agent und sein Bearbeitungswerkzeug nutzen Sprachmodelle nur über das OpenAI-Konto der Verantwortlichen. Die Auftragsbearbeiterin empfiehlt, im Konto die Verwendung von Daten zum Training auszuschalten und eine Ausgabenobergrenze zu setzen.
- Der Agent behandelt Inhalte aus Webseiten, E-Mails, Tickets und Dokumenten als Daten, nie als Anweisungen. Eine Aufforderung, etwas zu senden oder zu veröffentlichen, die in solchen Inhalten steht, gilt nicht als Freigabe.
- E-Mails, die der Agent entwirft, tragen die Zeile «Diese Nachricht wurde mit KI-Unterstützung verfasst.»

5. Organisation

- Nichts wird erfunden: eine fehlende Angabe wird gemeldet, nie mit einer Vermutung gefüllt.
- Daten der Verantwortlichen bleiben aus dem Plattform-Repository der Auftragsbearbeiterin fern; Prüfberichte, Offerten und Notizen liegen auf dem Server der Auftragsbearbeiterin in einem Ordner der Verantwortlichen.
- Programmier-Aufträge der Auftragsbearbeiterin laufen nicht auf dem Server des Agenten, sondern in einer isolierten Cloud-Umgebung; jede solche Änderung prüft eine zweite, unabhängige Instanz, bevor sie angenommen wird.
- In den Produktionszweig des Repositories schreibt nur die Release-App nach dem Ja einer Freigabeperson oder im Autopiloten (AGB Ziffer 9.7), und die Administratoren der GitHub-Organisation; GitHub selbst sperrt alle anderen (Regel «Restrict updates»). Der Tool-Broker schreibt nur Arbeitszweige und den Integrationszweig, nie mit Überschreiben der Geschichte.

6. Prüfung und Nachweis

- Beim Einrichten des Servers und danach täglich läuft eine automatische Sicherheitsprüfung: keine gespeicherte Dauerfreigabe für eine Handlung nach aussen ausser einem Autopiloten, und kein Autopilot, kein Full Access und keine dauerhafte Befehlserlaubnis, die nicht von einer Person stammen und aufgezeichnet sind; jede Handlung nach aussen fragt, ausser in einem Autopiloten; eingeschaltete Modi stehen im Bericht, ohne als Fehlschlag zu gelten; kein öffentlicher Port; nur die vorgesehenen Fähigkeiten geladen; kein Geheimnis dort, wo der Agent es lesen könnte. Ein Fehlschlag stoppt den Agenten und meldet sich bei der Auftragsbearbeiterin. Ein Geheimnis, das der Agent lesen konnte, gilt als verbrannt: der Agent bleibt gestoppt, bis es ersetzt ist. Die Berichte sind der Nachweis nach Ziffer 9; der bestandene Bericht der ersten Prüfung ist Bedingung für die Inbetriebnahme. Jede neue Sicherheitsabnahme des

Servers durch die Auftragsbearbeiterin (zum Beispiel nach einem Update) setzt Full Access zurück; die Auftragsbearbeiterin teilt das der Verantwortlichen mit (AGB Ziffer 9.10).
- Ein Integritätsprüfer stellt sicher, dass Code, Konfiguration und Regeln des Agenten unverändert sind.

7. Sicherung und Wiederherstellung

- Nächtliche, verschlüsselte Sicherung (restic) des Zustands des Agenten (Erinnerungen, Sitzungen, Konfiguration, Anmeldungen, Arbeitsordner, Freigabe-Register) auf einen Sicherungsspeicher bei Hetzner in Deutschland; Aufbewahrung 14 tägliche und 8 wöchentliche Sicherungen, danach automatische Löschung; der Schlüssel liegt nur im Passwort-Manager der Auftragsbearbeiterin und auf dem Server in einer Datei, die nur root liest.
- Der Code der Website liegt im Repository mit vollständiger Geschichte; die bisherige Website bleibt nach dem Go-live als Sicherung bestehen, bis die Verantwortliche ihre Löschung verlangt.
- Google Tag Manager führt eine Versionsgeschichte; jede veröffentlichte Container-Version wird ins Repository exportiert.

8. Beendigung

- Übergabe nach AGB Ziffer 8 (Repository übertragen, Server im Konto der Verantwortlichen neu aufgebaut und Daten zurückgespielt, Mitgliedschaft im Cloudflare-Konto und Rollen bei Google und OpenAI entfernt), Widerruf jedes Zugangsschlüssels mit Protokoll, Löschung nach Ziffer 10; die Übergabe-Anleitung liegt seit dem Go-live im Repository.

Anhang 2: Anbieter und Unterauftragsbearbeiter

Nur Anbieter, die unter dem vereinbarten Betriebsmodell tatsächlich Daten der Verantwortlichen bearbeiten. Grundlage für die USA: Zertifizierung unter dem Swiss-U.S. Data Privacy Framework (DPF), geprüft am 23. September 2026 für Cloudflare und Google; für GitHub, Tailscale, OpenAI und Anthropic Standardvertragsklauseln (SCC).

Teil A: Unterauftragsbearbeiter der Auftragsbearbeiterin (Konten der Samsa Labs AG)

Anbieter	Leistung	Daten	Land	Grundlage Ausland
Hetzner Online GmbH, Gunzenhausen	Server des Agenten (ein Projekt nur für die Verantwortliche) und verschlüsselter Sicherungsspeicher; ausserdem der Server der Auftragsbearbeiterin, auf dem Prüfberichte und Notizen zur Verantwortlichen liegen	Chat-Nachrichten, Berichte, Entwürfe, Freigabe-Register, Anmeldung des Agenten beim Modell-Konto, Sicherungen; Prüfberichte und Notizen	Deutschland (Falkenstein oder Nürnberg)	angemessen (EU)
GitHub, Inc., San Francisco (Microsoft)	Repository der Website in der Organisation Kantello, automatische Prüfungen und Veröffentlichung (Actions), Deployment-Geheimnisse	Inhalte des Repositories (Code, Texte, Team-Namen und Fotos, Freigaben im Entscheidungsprotokoll); Build-Werte als Geheimnisse	USA	SCC

Anbieter	Leistung	Daten	Land	Grundlage Ausland
Tailscale Inc., Toronto	Koordination des privaten Netzes, über das nur die Auftragsbearbeiterin den Server verwaltet; der Datenverkehr selbst ist Ende-zu-Ende verschlüsselt	Verbindungs-Metadaten (Geräte, Schlüssel, Zeiten), keine Inhalte	Kanada, USA	SCC
OpenAI Ireland Ltd, Dublin, und OpenAI, L.L.C., USA, über das Konto der Samsa Labs AG	Bau und Prüfung der Website: isolierte Cloud-Aufgaben, die Änderungen am Repository als Pull Request erstellen, und die Spezialisten, mit denen der Agent der Auftragsbearbeiterin den Neubau prüft	Inhalte des Repositories und der Vorschau (Code, Texte, Team-Namen und Fotos, Bildschirmfotos), Intake-Notizen; keine Besucher- oder Formulardaten	Irland, USA	SCC von OpenAI
Anthropic, PBC, San Francisco (Claude Code, Cloud-Sitzung)	Unabhängige Prüfung jeder Programmier-Änderung der Auftragsbearbeiterin vor der Annahme; liest die Änderung als Daten, führt nichts aus	Inhalte des Repositories wie oben	USA	SCC
Cloudflare, Inc., San Francisco, Konto der Auftragsbearbeiterin	Design-Vorschauen vor dem Go-live, bevor die Website im Konto der Verantwortlichen läuft	Inhalte der Website (Team-Namen und Fotos); keine Besucher- oder Formulardaten	USA, Rechenzentren weltweit	DPF und SCC

Teil B: Anbieter in den Konten der Verantwortlichen (keine Unterauftragsbearbeiter der Auftragsbearbeiterin)

Die Verantwortliche hält diese Konten und die Verträge selbst. Die Auftragsbearbeiterin arbeitet dort nur mit den Rollen, die die Verantwortliche ihr gibt.

Anbieter	Leistung	Daten	Land	Grundlage Ausland	Rolle der Auftragsbearbeiterin
Cloudflare, Inc., San Francisco	Hosting der Website (Pages, Vorschau und Produktion), Zone der Domain der Verantwortlichen, Formular-Funktion, Spam-Schutz (Turnstile), Cloudflare Access für die Vorschau und den Web-Zugang zum Agenten (Cloudflare Tunnel und Cloudflare Access für agent.‹Domain›)	Server-Logs (IP, Browser, Seite, Zeit), Formulardaten im Durchlauf, Turnstile-Prüfdaten, Anmeldungen an der Vorschau, Anmeldungen am Web-Zugang (E-Mail-Adresse, Zeitpunkt, IP-Adresse, Land, Browser), Verkehr zwischen Browser und Agent im Durchlauf (Chat-Nachrichten, Vorschauen, Freigabe-Anfragen mit Empfängern und Dokumenten)	USA, Rechenzentren weltweit	DPF und SCC	Mitglied mit der Rolle Super Administrator; richtet ein und betreibt
OpenAI Ireland Ltd, Dublin, und OpenAI, L.L.C., USA	Sprachmodell des Agenten der Verantwortlichen und seines Bearbeitungswerkzeugs	Chat-Nachrichten, Inhalte der Website, Kennzahlen, Entwürfe	Irland, USA	SCC von OpenAI	keine Rolle im Konto; der Agent meldet sich auf dem Server an (Training im Konto ausschalten)
Google Ireland Ltd, Dublin, und Google LLC, USA	Google Tag Manager, Google Analytics 4, Google Ads (Conversion und Kampagnen), Search Console, Google-Cloud-Projekt für die Schnittstellen	Messdaten nach Zustimmung; ohne Zustimmung Pings ohne Cookies; Kennzahlen und Suchanfragen für die Berichte; Kampagnenentwürfe	Irland, USA	DPF und SCC	die Rollen, die die Verantwortliche vergibt (Google Ads: Schreibzugriff nur innerhalb der Obergrenzen im Konto, AGB Ziffer 10.4)
Mail-Anbieter für das Formular: wird beim Intake festgelegt	Zustellung der Formularanfragen an das Postfach der Verantwortlichen	Formulardaten	wird beim Intake festgelegt	wird beim Intake festgelegt	Zugang nur für die Einrichtung

Chat und Freigaben laufen über den Web-Zugang (Cloudflare, Konto der Verantwortlichen, Teil B). Ein weiterer Chat-Kanal (zum Beispiel Microsoft Teams) erhält, sobald er eingerichtet und freigegeben ist, eine eigene Zeile in diesem Anhang (Ziffer 7.2).

Nicht in diesem Anhang, weil eigene Verantwortliche oder Vertragspartner der Verantwortlichen: das Postfach der Verantwortlichen, das die Formularanfragen empfängt (zum Beispiel Microsoft 365), eine allfällige Shop-Plattform der Verantwortlichen (getrenntes System), die Werbeplattformen von Google und Meta (Konten der Verantwortlichen; der Agent hält kein Token für Meta), die Registrierstelle der Domain. Werkzeuge der Auftragsbearbeiterin für die Vertragsabwicklung mit Geschäftskontaktdaten der

Verantwortlichen (Namen, Termine, Rechnungen), eigene Bearbeitung nach Ziffer 2.4: Google Workspace (hi@kantello.com; Google Cloud EMEA Ltd, Irland, und Google LLC, USA), Linear (Linear Orbit, Inc., USA; Tickets mit Namen und Terminen), Infinity (Buchhaltung, Rechnungen; NextBusiness AG, Zürich), Stripe (Zahlungslinks; Stripe Payments Europe Ltd, Irland, und Stripe, Inc., USA), Calendly (Terminbuchung für Gespräche; Calendly LLC, Buford, USA).

Anhang 3: Beschreibung der Bearbeitung im Einzelnen

Nr.	Bearbeitung	Wo	Wer sieht die Daten	Aufbewahrung
1	Auslieferung der Website und Server-Logs	Cloudflare Pages (Konto der Verantwortlichen)	Cloudflare; die Auftragsbearbeiterin nur in aggregierten Statistiken	Logs bei Cloudflare nach dessen Regeln; keine eigene Speicherung
2	Cookie-Wahl (Cookie `kt_consent`) und Design-Wahl (lokaler Speicher)	Browser der Besucherin oder des Besuchers	niemand ausser dem Browser	Cookie: sechs Monate; lokaler Speicher: bis zur Löschung
3	Formularanfrage: Prüfung (Turnstile, Ausfüllzeit, Anfragen pro Adresse) und Zustellung per E-Mail	Cloudflare-Funktion, Mail-Anbieter, Postfach der Verantwortlichen	die Verantwortliche; der Mail-Anbieter im Durchlauf; die Auftragsbearbeiterin nicht (kein Zugang zum Postfach)	keine Speicherung auf der Website; beim Mail-Anbieter nach dessen Regeln; im Postfach nach den Regeln der Verantwortlichen
4	Ereignis «Formular zugestellt» als Conversion (ohne Inhalt der Anfrage)	Google Tag Manager, Google Ads, Google Analytics 4	Google; die Verantwortliche und der Agent in aggregierten Berichten	nach den Einstellungen der Verantwortlichen in Google Analytics 4 (Empfehlung: 14 Monate)
5	Messung nach Zustimmung (Seitenaufrufe, Klicks auf Telefon, E-Mail, Shop, Offerte)	Google Tag Manager, Google Analytics 4, Google Ads	wie 4	wie 4
6	Chat mit dem Agenten; Änderungen an der Website; Vorschau-Links	Server des Agenten (Hetzner, Konto der Auftragsbearbeiterin, Projekt nur für die Verantwortliche), OpenAI (Konto der Verantwortlichen), Cloudflare Tunnel und Cloudflare Access (Konto der Verantwortlichen), GitHub, Cloudflare-Vorschau	die Personen mit Zugang zum Agenten, der Agent; die Auftragsbearbeiterin als Betreiberin des Servers	Sitzungen und Erinnerungen des Agenten bis zur Löschung durch die Verantwortliche; Sicherungen 14 Tage täglich, 8 Wochen wöchentlich; Freigaben der Website dauerhaft im Repository
7	Wochenbericht: Lesen von Google Analytics 4, Search Console, Google Ads und, wenn angeschlossen, der Bestellzahlen eines Shops	Server des Agenten; Google; Schnittstelle (API) des Shops, lesend	wie 6	Berichte auf dem Server des Agenten bis zur Löschung durch die Verantwortliche

Nr.	Bearbeitung	Wo	Wer sieht die Daten	Aufbewahrung
8	Entwürfe für Beiträge, Anzeigen und E-Mails aus Inhalten der Website, eines Shops und der Nachrichten des Teams	Server des Agenten; OpenAI (Konto der Verantwortlichen)	wie 6	wie 7
9	Intake und Baseline: Exporte aus Search Console, Google Analytics 4, Google Ads; Bildschirmfotos; Prüfbericht der Website	Repository (Baseline- und Intake-Unterlagen); Server der Auftragsbearbeiterin (Ordner der Verantwortlichen)	die Auftragsbearbeiterin, die Verantwortliche, der Agent	im Repository dauerhaft (gehört der Verantwortlichen); auf dem Server der Auftragsbearbeiterin bis zur Löschung nach Ziffer 10
10	Bau und Prüfung der Website: Code-Änderungen durch Cloud-Aufgaben, unabhängige Prüfung, Prüfung des Neubaus durch Spezialisten des Agenten der Auftragsbearbeiterin	OpenAI (Konto der Samsa Labs AG), Anthropic Claude Code (Konto der Samsa Labs AG), Server der Auftragsbearbeiterin, GitHub	die Auftragsbearbeiterin	im Repository dauerhaft; Bildschirmfotos der Prüfung 14 Tage auf dem Server der Auftragsbearbeiterin; bei den Anbietern nach deren Regeln für Geschäftskunden
11	Anmeldung am Web-Zugang zum Agenten	Cloudflare Access (Konto der Verantwortlichen); Kopplungsverzeichnis auf dem Server des Agenten (Person und Kennung des gekoppelten Browsers)	die Verantwortliche, die Auftragsbearbeiterin als Mitglied des Cloudflare-Kontos und als Betreiberin des Servers; Cloudflare (nur die Anmeldungen)	Protokoll der Anmeldungen bei Cloudflare 24 Stunden im Free-Plan (30 Tage im Plan Standard); Kopplungsverzeichnis bis zum Entzug des Zugangs, längstens bis zur Übergabe; Freigabe-Register auf dem Server des Agenten für die Dauer des Vertrags; es gehört zum Zustand des Agenten und geht bei der Übergabe an die Verantwortliche (Ziffer 10.1); die Kopie auf dem alten Server wird mit ihm gelöscht; in den Sicherungen nach Anhang 1 Ziffer 7 (14 Tage täglich, 8 Wochen wöchentlich)

Nr.	Bearbeitung	Wo	Wer sieht die Daten	Aufbewahrung
12	Freigaben: Frage, Vorlage, Ja oder Nein; Ein- und Ausschalten von Full Access und Autopilot (AGB Ziffer 9.7)	Bedienoberfläche des Agenten (agent.‹Domain›, Cloudflare Access im Konto der Verantwortlichen), Server des Agenten (Freigabe-Register), Repository (Entscheidungsprotokoll für Veröffentlichungen der Website)	die Personen mit Zugang zum Agenten, die Auftragsbearbeiterin als Betreiberin	Freigabe-Register auf dem Server des Agenten für die Dauer des Vertrags; es gehört zum Zustand des Agenten und geht bei der Übergabe an die Verantwortliche (Ziffer 10.1); die Kopie auf dem alten Server wird mit ihm gelöscht; in den Sicherungen nach Anhang 1 Ziffer 7 (14 Tage täglich, 8 Wochen wöchentlich); Einträge im Entscheidungsprotokoll dauerhaft im Repository, das der Verantwortlichen gehört