

AlLoopwise — Wir implementieren Claude in Ihrem Unternehmen

20 Fragen an Ihren KI-Anbieter — bevor Mandantendaten fließen

Ein Fragenkatalog für Steuerkanzleien: Verschwiegenheit und Vertrag (§62a StBerG, §203 StGB), Architektur und Isolation — und die Inferenz-Frage, die kaum jemand stellt. Zu jeder Frage: das Warnsignal in der Antwort.

Kostenlose Arbeitshilfe — zum Weitergeben an Kollegen und Anbieter. Keine Anmeldung nötig.

ailoopwise.com · Pro Kunde isolierte Systeme, Datenbank und Dokumente auf deutschen Servern.
Diese Arbeitshilfe stellt Rechtsfragen allgemein dar und ersetzt keine rechtliche Prüfung Ihres Einzelfalls.

A — Verschwiegenheit & Vertrag

Die DSGVO ist nicht die einzige Messlatte. Für Berufsgeheimnisträger gelten §62a StBerG und §203 StGB — und die erste Aufgabe eines Anbieters ist, diesen Unterschied zu kennen, bevor Sie ihn erklären müssen.

- 1 Sind Sie bereit, sich vor Vertragsbeginn in Textform zur Verschwiegenheit verpflichten zu lassen (§203 Abs. 4 StGB)?**
Warnsignal: „Unsere AVV deckt das ab.“ — Eine Auftragsverarbeitungsvereinbarung ist Datenschutzrecht. Die berufsrechtliche Verpflichtung ist ein eigenes Dokument.
- 2 Kennen Sie §62a StBerG — und können Sie zeigen, wo Ihr Standardvertrag dessen Anforderungen abbildet?**
Warnsignal: Die Antwort beginnt mit „Wir sind DSGVO-konform“. Das war nicht die Frage.
- 3 Welche Personen bei Ihnen haben technisch Zugriff auf Klardaten — und sind genau diese Personen schriftlich verpflichtet?**
Warnsignal: „Unsere Mitarbeiter sind alle geschult.“ Geschult ist nicht verpflichtet.
- 4 Setzen Sie Subunternehmer oder Sub-Dienste ein? Gelten die Verpflichtungen nachweisbar auch für diese?**
Warnsignal: Eine Liste der Sub-Dienste existiert nicht oder ist „auf Anfrage“ — dann kennt der Anbieter seine eigene Kette nicht auswendig.
- 5 Was passiert bei Vertragsende — Rückgabe, Löschung, Löschnachweis, und in welcher Frist?**
Warnsignal: „Das regeln wir dann.“ Das Ende eines Vertrags ist der Moment, in dem Sie am wenigsten Verhandlungsmacht haben.

B — Architektur & Isolation

- 6 Läuft unsere Umgebung getrennt von anderen Kunden — eigene Instanz, eigene Datenbank? Oder teilen wir uns ein System, getrennt nur durch Berechtigungen?**
Warnsignal: „Wir sind mandantenfähig.“ Mandantenfähig heißt: geteiltes System. Das kann in Ordnung sein — aber es ist das Gegenteil von Isolation, und Sie sollten wissen, welches von beiden Sie kaufen.
- 7 Wo liegen unsere Daten physisch — Land, Rechenzentrum, Betreiber?**
Warnsignal: „In der EU“ ohne Namen. Ein Anbieter, der weiß, wo Ihre Daten liegen, kann das Rechenzentrum benennen.
- 8 Wer verwaltet die Verschlüsselung und die Schlüssel — Sie, wir, oder ein Dritter?**
Warnsignal: Verschlüsselung wird bejaht, die Schlüsselfrage bleibt unbeantwortet.
- 9 Können Sie einzelne Mandate oder Datensätze gezielt und nachweisbar löschen?**
Warnsignal: Löschung nur „zum Vertragsende insgesamt“ — ein Mandatswechsel kommt aber vorher.
- 10 Gibt es ein Audit-Log über Zugriffe und Verarbeitungen — und können wir es selbst einsehen?**
Warnsignal: Das Log existiert, aber nur der Anbieter kann hineinsehen. Ein Nachweis, den Sie nicht prüfen können, ist keiner.

C — Die Inferenz-Frage, die kaum jemand stellt

Fast jede Compliance-Checkliste fragt, wo Daten *gespeichert* werden. Fast keine fragt, wo das Sprachmodell *rechnet* — dabei ist genau das der Moment, in dem Ihr Text im Klartext verarbeitet wird.

11 **Wo läuft die Modell-Inferenz physisch — im selben Rechenzentrum wie unsere Daten, in einer EU-Cloud-Region, oder bei einem Anbieter in den USA?**

Warnsignal: Die Antwort nennt nur den Speicherort. Speicherung und Inferenz sind zwei verschiedene Orte — wer den Unterschied nicht macht, kennt ihn nicht.

12 **Wer kann im Moment der Verarbeitung technisch Klartext lesen — welches Unternehmen, in welchem Land, unter welchem Recht?**

Warnsignal: „Niemand, alles ist verschlüsselt.“ Während der Inferenz liegt der Text für das verarbeitende System im Klartext vor — die ehrliche Antwort benennt, wer dieses System betreibt.

13 **Speichert der Modellanbieter unsere Eingaben — wie lange, und lässt sich das vertraglich oder technisch abstellen?**

Warnsignal: „Standardmäßig nein“ ohne Dokument. Aufbewahrungsregeln stehen bei seriösen Anbietern schriftlich in der Dokumentation — lassen Sie sich die Stelle zeigen.

14 **Werden unsere Daten für Modell-Training verwendet — und wo steht das schriftlich?**

Warnsignal: Ein mündliches „natürlich nicht“. Die Antwort hat eine Fundstelle oder sie zählt nicht.

15 **Wenn Sie mehrere Modelle einsetzen: Gelten Ihre Antworten auf 11-14 für jedes einzelne Modell — oder nur für das Standardmodell?**

Warnsignal: Die Antwort gilt „im Prinzip“ für alle. Modellwechsel ändern Datenwege — pro Modell, oder gar nicht.

D — Betrieb & Ehrlichkeit

16 **Was können Sie uns NICHT zusagen?**

Warnsignal: „Bei uns ist alles abgedeckt.“ Ein Anbieter, der keine Grenzen nennt, hat sie nicht durchdacht.

17 **Was passiert bei einem Ausfall — wer haftet wofür, und wo steht das im Vertrag?**

Warnsignal: Haftungsfragen werden aufs „partnerschaftliche Verhältnis“ verschoben.

18 **Wie erfahren wir von Änderungen — neue Sub-Dienstleister, Modellwechsel, neue Datenwege?**

Warnsignal: Gar nicht, oder „steht dann in den AGB“. Änderungen an Datenwegen verdienen eine aktive Mitteilung.

19 **Können wir mit einem kleinen, klar abgegrenzten Projekt starten, bevor wir uns binden?**

Warnsignal: Nur Jahresverträge, nur Komplettpakete. Wer von seiner Leistung überzeugt ist, kann klein anfangen.

20 **Dürfen wir mit einer Kanzlei sprechen, die Sie bereits betreuen?**

Warnsignal: Ausweichen. Die ehrliche Antwort eines jungen Anbieters lautet: „Noch nicht — deshalb zeigen wir Ihnen stattdessen das System selbst.“ Auch das ist ein Datenpunkt, und ein besserer als eine erfundene Referenz.

Wer diesen Katalog geschrieben hat — und unsere eigene Antwort auf Frage 20

AILoopwise implementiert Claude und KI-Workflows im Mittelstand: pro Kunde isolierte Systeme — eigene Umgebung, eigene Datenbank auf deutschen Servern — und die Modellwahl wird pro Kunde transparent benannt, Frage 11 bis 15 inklusive. Unsere ehrliche Antwort auf Frage 20 lautet heute: noch nicht. Fragen Sie uns trotzdem — wir zeigen Ihnen stattdessen das System, live, auf Dokumenten aus Ihrer Branche.

ailoopwise.com/de/use-cases/tax-advisory