

8 Fragen, die Sie Ihrem KI-Anbieter stellen müssen

— bevor Mandantendaten in die Cloud gehen. Ein Kurz-Check für Kanzleien, Treuhänder, Wirtschaftsprüfer und Steuerberater.

Künstliche Intelligenz spart in Kanzleien Stunden — bei Recherche, Entwürfen, Auswertungen. Doch sobald Mandantendaten in eine Cloud-KI fließen, steht Ihr Berufsgeheimnis auf dem Spiel (Art. 321 StGB, Art. 13 BGFA, revidiertes DSG). Diese acht Fragen trennen einen sicheren Anbieter von einem Risiko.

- 1 Verlassen identifizierende Mandantendaten überhaupt mein Haus?**
Der beste Schutz: Namen, Adressen, AHV-Nummern, IBAN & Co. werden **anonymisiert**, **bevor** ein Text an ein Cloud-Modell geht — nicht erst «in der Cloud» verarbeitet.
- 2 Wer hält den Schlüssel zur Rück-Zuordnung?**
Bleibt die Zuordnungstabelle (Klartext ↔ Platzhalter) **bei Ihnen in der Kanzlei** — oder beim Anbieter? Nur wenn Sie den Schlüssel halten, behalten Sie die Kontrolle.
- 3 Kann eine US-Behörde auf den Anbieter Druck ausüben — unabhängig vom Server-Standort?**
Der Standort allein schützt nicht. Entscheidend ist der **US-Bezug**: Ein Schweizer Ableger eines US-Konzerns (z.B. Microsoft Schweiz, 100 % US-Mutter) unterliegt trotz Schweizer Rechenzentrum dem Zugriff via CLOUD Act, FISA §702 und Executive Order 12333. Fragen Sie: Ist der Anbieter **eigentümer- und betriebsseitig** von US-Strukturen getrennt — Schweizer Firma, Schweizer Systeme, physisch entkoppelt?
- 4 Werden meine Daten zum Training des Modells verwendet?**
Ein «Nein, niemals» muss **vertraglich** zugesichert sein — nicht nur in den AGB versteckt. Sonst werden Mandatsinhalte Teil eines fremden Modells.
- 5 Kann ich belegen, was geschützt wurde?**
Für Aufsicht und Haftung zählt Nachweisbarkeit. Gibt es ein Protokoll, das zeigt, welche Daten anonymisiert wurden und was das Modell tatsächlich gesehen hat?
- 6 Rechnet das System — oder rät es?**
Bei Zahlen (Abschlüsse, Fristen, Beträge) darf KI nicht «halluzinieren». Seriöse Anbieter lassen **Code deterministisch rechnen** und die KI nur interpretieren — auditierbar, kein Ratespiel auf Geld-Pfaden.
- 7 Was passiert im Ernstfall — und beim Ausstieg?**
Wie schnell werden Daten auf Verlangen gelöscht? Bekomme ich meine Inhalte beim Anbieterwechsel vollständig zurück? Ein sauberer Exit gehört zur Datenhoheit.
- 8 Kann fremdes Recht die Löschung meiner Daten verhindern?**
Selbst eine Lösch-Zusage kann ausgehebelt werden: In den USA entsteht eine **Aufbewahrungs-Pflicht automatisch mit Klageerhebung** (bzw. bei absehbarem Verfahren) — ganz ohne expliziten Beschluss. Sie sollte typischerweise Trainingsdaten, relevante Modell-Outputs und interne Kommunikation umfassen. Fragen Sie: Kann eine fremde Justiz Ihre Datenhoheit überschreiben?*

Zögern Sie bei einer dieser Fragen?

Praevana wurde genau dafür gebaut: KI-Produktivität wie die grossen Kanzleien — aber Personendaten werden anonymisiert, **bevor** sie die Cloud erreichen, und der Schlüssel bleibt bei Ihnen. Fragen zu einem der acht Punkte? Antworten Sie einfach direkt auf unsere Mail — wir helfen unverbindlich weiter.

* Illustratives Beispiel (NYT Co. v. Microsoft/OpenAI, 23-cv-11195, SDNY, 2023) — keine Rechtsberatung. Sachverhalte und Rechtslage können sich ändern; im Einzelfall fachkundig prüfen lassen.