

§203-StGB-Checkliste für KI-Tools in der Steuerkanzlei

Mandantendaten und Steuer-IDs im Prompt – diese Punkte vor dem KI-Einsatz klären

Hinweis: Diese Checkliste ist eine allgemeine Orientierung und keine Rechtsberatung. Sie ersetzt keine individuelle rechtliche Prüfung im Einzelfall.

Schnelltest: Braucht diese Aufgabe eine §203-Absicherung?

AUFGABE	JA	NEIN
Enthält der Prompt Mandantennamen, Steuer-IDs oder erkennbare Fallangaben?	☐	☐
Geht es um Mandantenschreiben, Belege oder Diktate mit Mandantenbezug?	☐	☐
Wird ein kostenloser Tarif ohne AVV für Kanzleiarbeit genutzt?	☐	☐

Mindestens einmal "Ja"? Dann greift §203 StGB – weiter zur Checkliste unten. Nur interne Recherche ohne Mandantenbezug (z. B. öffentliche Fachartikel zusammenfassen)? Meist unproblematisch.

Die 8-Punkte-Checkliste vor dem KI-Einsatz mit Mandantendaten

- 1 AVV nach Art. 28 DSGVO vorhanden?** Bei Consumer-Tarifen (z. B. ChatGPT Plus) oft nur in Business-/Enterprise-Tarifen enthalten – für den konkret gebuchten Tarif prüfen.
- 2 Reicht ein AVV allein, oder ist zusätzlich §203 StGB relevant?** Sobald Mandantendaten, Namen oder Steuer-IDs im Prompt landen, genügt ein AVV allein regelmäßig nicht – zusätzliche vertragliche Vereinbarung im Einzelfall prüfen.
- 3 Serverstandort und Mutterkonzern getrennt bewertet?** Cloud-Act-Risiko hat zwei Dimensionen: direkter Zugriff bei US-Serverstandort und mittelbarer Zugriff über einen US-Mutterkonzern, selbst bei EU-Servern.
- 4 DATEV-eigene KI-Funktion geprüft, statt automatisch externes Tool?** DATEV integriert KI direkt in die Kanzleisoftware – Mandantendaten verlassen dabei das vertraglich bereits geregelte Umfeld nicht.
- 5 Europäischer Anbieter mit EU-Sitz und EU-Server als erster Filter geprüft?** Schließt beide Cloud-Act-Risikodimensionen weitgehend aus (z. B. Taxy.io, Neuroflash, Open Telekom Cloud).
- 6 KI-Training-Opt-out aktiv gesetzt?** Bei kostenlosen Tarifen häufig nicht standardmäßig aktiv – muss aktiv gesetzt werden und wird leicht übersehen.
- 7 Automatisierungs-Workflows (z. B. Belegvorsortierung) auf Auftragsverarbeitung und Datenregion geprüft?** Gilt auch für Tools, die nur im Hintergrund Belege vorsortieren.
- 8 Bei besonders hohem Schutzbedarf: lokale/On-Premise-Alternative geprüft?** Mandantendaten verlassen dabei die eigene Infrastruktur nicht – erfordert aber spürbaren technischen Aufwand.

Auf einen Blick

Unproblematisch: interne Recherche ohne Mandantenbezug (ChatGPT Plus, Claude, Gemini).

Geringeres Zusatzrisiko: Mandantenschreiben mit Namen/Steuer-ID über ein EU-Tool mit AVV (z. B. Taxy.io). **Nur nach Prüfung:** Diktate mit Mandantenbezug – vorab Auftragsverarbeitung und Datenregion klären.