

Bevor Mandantendaten eine KI erreichen

Für Kanzleien, Steuerberater und Arztpraxen in Deutschland. Geprüft am 15. Oktober 2026. Keine Rechtsberatung.

1. Der Vertrag mit dem Anbieter (§ 43e BRAO, § 62a StBerG)

1. Textform, keine bloß angeklickte Richtlinie
2. Verschwiegenheitsverpflichtung mit Belehrung über strafrechtliche Folgen (§ 203 StGB)
3. Zugang nur soweit für den Dienst erforderlich
4. Unterauftragnehmer nur, wenn erlaubt, und in Textform verpflichtet
5. Anbieter im Ausland: vergleichbarer Schutz; Server in der EU bevorzugen (BRAK, Dez. 2024)
6. Zusätzlich Auftragsverarbeitungsvertrag (Art. 28 DSGVO); Gesundheitsdaten: Art. 9

2. Einwilligung und Anonymisierung

1. Mandatsbezogener Einsatz: Einwilligung des Mandanten (§ 43e Abs. 5 BRAO, § 62a Abs. 5 StBerG); die BStBK (27. Jan. 2026) nennt den ChatGPT-Fall nicht zweifelsfrei
2. Ohne Verschwiegenheitsvereinbarung oder Einwilligung: nur abstrakte Anfragen
3. Namen entfernen reicht oft nicht (BRAK): Details verallgemeinern, jede Seite auf Name, Adresse, Steuernummer prüfen
4. Braucht die Aufgabe die echten Akte, braucht sie einen verpflichteten Anbieter oder eine Einwilligung

3. Kanzlei-Richtlinie

1. Werkzeuge und Kontoart je Werkzeug freigeben
2. Auftragsverarbeitungsvertrag und Verschwiegenheitsverpflichtung je Werkzeug ablegen
3. Festlegen, was eingegeben werden darf
4. Festlegen, wann um Einwilligung gebeten wird; Vorlage bereithalten
5. Ein Berufsträger prüft jedes KI-Ergebnis in der Mandatsarbeit; Mitarbeitende schulen

Kostenlose Konten trainieren oft mit Eingaben; bei Business-Konten lässt sich das vertraglich ausschließen (BStBK-FAQ, 27. Jan. 2026). Beides ersetzt die Verschwiegenheitsverpflichtung nicht.