ORIENTIERUNGSHILFE

KI in der Steuerberatung

Berufsrecht, Strafrecht, Datenschutz und EU AI Act

Einordnung und Praxishilfe für einen kontrollierten KI-Einsatz in Steuerkanzleien

Redaktionelle Informationshandreichung für das kammerübergreifende KI-Forum

Rechts- und Informationsstand: 28. Juli 2026

ZIELGRUPPE	FOKUS	FORMAT
Steuerberaterinnen, Steuerberater, Kanzleiteams	Mandatsdaten, Geheimnisschutz, Governance	Orientierung - keine verbindliche Rechtsauffassung

Wichtiger Hinweis

Dieses Dokument ist weder amtliche Verlautbarung noch Beschluss oder verbindliche Rechtsauffassung der Steuerberaterkammer Niedersachsen oder einer anderen beteiligten Kammer. Es dient ausschließlich der allgemeinen Information und ersetzt weder die Prüfung des konkreten Einzelfalls noch eine rechtliche, berufsrechtliche oder datenschutzrechtliche Beratung.

0 Das Wichtigste auf vier Seiten

AKTUALISIERUNG 28.07.2026 AI-Act-Fristen kurzfristig geändert

Die BStBK-FAQ „KI im steuerberatenden Berufsstand“ ist eine wertvolle Orientierung, basiert aber ausdrücklich auf dem Rechtsstand Juli 2025. Am 27. Juli 2026 ist die Verordnung (EU) 2026/1744 („Digital Omnibus on AI“) in Kraft getreten. Sie hat unter anderem die Hochrisiko-Fristen und Art. 4 KI-VO geändert. Diese Handreichung bildet den Stand nach dieser Änderung ab. [S8] [S14] [S15]

Zwölf Kernaussagen

1

KI ist nicht generell verboten.

Steuerberaterinnen und Steuerberater dürfen KI als Arbeitsmittel einsetzen. Entscheidend sind der konkrete Anwendungsfall, die Daten, die Produktvariante, die Vertragslage und die menschliche Kontrolle.

2

Nicht der Markenname entscheidet.

Ein Consumer-Account, ein Business-Tarif, eine API, eine Kanzleisoftware-Integration und eine lokal betriebene Lösung desselben Herstellers können rechtlich völlig unterschiedlich zu bewerten sein.

3

Mandatsgeheimnisse brauchen eine kontrollierte Umgebung.

Identifizierbare Mandatsdaten gehören nicht in private, kostenlose oder sonst nicht freigegebene KI-Zugänge. Eine „Enterprise“-Bezeichnung allein genügt allerdings ebenfalls nicht.

4

§ 62a StBerG ist die zentrale berufsrechtliche Dienstleister-Norm.

Er verlangt insbesondere Erforderlichkeit, sorgfältige Auswahl, Textform, Geheimhaltungs- und Need-to-know-Regeln, Subdienstleisterkontrolle und gegebenenfalls vergleichbaren Geheimnisschutz im Ausland. [S3]

5

Einwilligung ist nicht immer nötig - aber manchmal.

§ 62a Abs. 5 StBerG verlangt sie, wenn die externe Dienstleistung unmittelbar einem einzelnen Mandat dient. Ob und wann ein generatives KI-Tool darunter fällt, ist noch nicht abschließend geklärt. [S3] [S6] [S8]

6

Einwilligung und Verzicht sind zwei verschiedene Dinge.

Die Einwilligung nach § 62a Abs. 5 erlaubt die mandatsbezogene Einschaltung. Ein ausdrücklicher Verzicht nach Abs. 6 kann Anforderungen aus Abs. 2 und 3 abbedingen. Ein solcher Verzicht ist eng, konkret und informiert zu gestalten - nicht pauschal.

7

Der Mandant kann nicht „die DSGVO wegverzichten“.

Berufsrechtliche Einwilligung oder Entbindung, strafrechtliche Befugnis und datenschutzrechtliche Rechtsgrundlage sind getrennt zu prüfen. Ein Mandant kann außerdem nicht ohne Weiteres über Geheimnisse oder personenbezogene Daten Dritter disponieren.

8

§ 203 StGB gilt neben dem Berufsrecht.

Die zulässige Einbindung mitwirkender Personen ist möglich. Unbefugtes Offenbaren und unzureichende Verpflichtung weiterer Mitwirkender können aber strafrechtliche Risiken auslösen. Nicht jeder Berufsrechtsverstoß ist automatisch eine Straftat - beide Ebenen laufen nebeneinander. [S4] [S7]

9

Pseudonymisierung ist keine Anonymisierung.

Pseudonymisierte Daten bleiben regelmäßig personenbezogen und meistens auch berufsrechtlich geheim. Nur eine belastbare Anonymisierung kann den Personenbezug und gegebenenfalls die Mandatszuordnung entfallen lassen.

10

Die fachliche Verantwortung bleibt beim Berufsträger.

KI ist kein „zweiter Berufsträger“. Rechtsstand, Sachverhalt, Fundstellen, Berechnungen, Fristen und Schlussfolgerungen müssen mit der dem Risiko entsprechenden Tiefe geprüft werden. [S1] [S5] [S8]

11

Der AI Act verlangt heute vor allem Governance.

Für typische Text-, Recherche- und Dokumentenassistenz stehen Art. 4 KI-Kompetenz sowie ab 2. August 2026 die spezifischen Transparenzregeln des Art. 50 im Vordergrund. Klassische Kanzleiassistenz ist nicht allein wegen des KI-Einsatzes ein Hochrisiko-System. [S13]-[S16]

12

Kontrolliert starten ist besser als Schatten-IT.

Kanzleien brauchen eine Positivliste, ein KI-Register, Datenklassen, Freigabeprozesse, Schulung, technische Kontrollen und dokumentierte fachliche Prüfregeln. Das DStV-Muster kann hierfür eine Ausgangsbasis sein. [S17]

Schnellprüfung: Darf dieser KI-Anwendungsfall starten?

Die folgende Prüfung ist bewusst konservativ. Ein „Ja“ bei einer Stufe ersetzt nicht die nächsten Stufen. Die Entscheidung sollte bei mandatsnahen oder datenintensiven Anwendungen in einem kurzen Prüfvermerk dokumentiert werden.

1 Zweck festlegen
Welche konkrete Aufgabe soll die KI erledigen? Entwurf, Recherche, Dokumentenanalyse, Buchungsvorschlag, Transkription, Personalentscheidung oder autonome Aktion?

2 Daten klassifizieren
Enthält die Eingabe Berufsgeheimnisse, personenbezogene Daten, besondere Kategorien, Zugangsdaten oder nur öffentliche bzw. belastbar anonymisierte Informationen?

3 Produktvariante identifizieren
Welcher Anbieter, welche juristische Vertragspartnerin, welcher Tarif, welche Region, welche Einstellungen, welche Connectoren und welche Subdienstleister werden tatsächlich verwendet?

4 § 62a prüfen
Ist der Zugriff für die Leistung erforderlich? Sind Auswahl, Textform, Verschwiegenheit, Need-to-know, Subdienstleister und Auslandsbezug geregelt? Dient die Leistung unmittelbar einem einzelnen Mandat?

5 § 203 prüfen
Ist die Offenbarung befugt und auf das Erforderliche beschränkt? Sind alle mitwirkenden Personen und weiteren Mitwirkenden wirksam in den Geheimnisschutz einbezogen?

6 DSGVO prüfen
Rollen, Rechtsgrundlage, Art. 28, Transparenz, Speicherfristen, Training, Sicherheit, Drittlandtransfer und gegebenenfalls DSFA klären.

7 AI Act prüfen
Rolle als Betreiber/Anbieter, verbotene Praktik, Hochrisiko-Kontext, Art. 4 KI-Kompetenz und Art. 50 Transparenz einordnen.

8 Menschliche Kontrolle festlegen
Wer prüft welche Aspekte? Was darf die KI vorbereiten, was niemals final entscheiden oder versenden?

9 Technische Leitplanken aktivieren
MFA, Rollen, Training aus, Retention minimieren, Connectoren begrenzen, DLP/Logging, keine privaten Accounts.

10 Freigeben und überwachen
Pilot mit Testdaten, dokumentierte Freigabe, Mitarbeiterschulung, Qualitätsmessung und turnusmäßige Neubewertung.

MERKREGEL Vier Tore statt „DSGVO-konform“-Label
Ein belastbarer Einsatz muss vier Tore passieren: (1) Berufsgeheimnis, (2) Strafrecht, (3) Datenschutz, (4) AI Act und fachliche Verantwortung. Ein Anbieterhinweis „DSGVO-konform“, EU-Hosting oder „kein Training“ beantwortet jeweils nur einen Teil der Prüfung.

Die vier rechtlichen Ebenen im Überblick

Ebene	Zentrale Normen	Leitfrage	Typische Folge bei Fehlern
Berufsrecht	§ 57, § 62, § 62a StBerG; § 5 BOStB	Darf ein externer Dienstleister Zugang zu Berufsgeheimnissen erhalten und unter welchen organisatorischen Bedingungen?	Berufsaufsichtliche Maßnahmen; Haftungs- und Vertrauensrisiken
Strafrecht	§ 203 StGB	Ist die Offenbarung an mitwirkende Personen befugt und sind weitere Mitwirkende wirksam zur Geheimhaltung verpflichtet?	Persönliche strafrechtliche Risiken bei erfülltem Tatbestand
Datenschutz	DSGVO, BDSG	Gibt es personenbezogene Daten, eine Rechtsgrundlage, korrekte Rollen, Art.-28-Vertrag, Sicherheit, Transparenz und zulässige Transfers?	Aufsichtsmaßnahmen, Bußgelder, Schadenersatz, Betroffenenrechte
KI-Regulierung	Verordnung (EU) 2024/1689 i. d. F. der VO (EU) 2026/1744	Welche Rolle und Risikoklasse liegt vor? Gelten KI-Kompetenz-, Transparenz- oder Hochrisikopflichten?	Marktaufsicht, Sanktionen, organisatorische Pflichten
Fachverantwortung	§ 57 StBerG; Mandatsvertrag; allgemeines Haftungsrecht	Ist das Ergebnis fachlich nachvollziehbar, aktuell, vollständig und freigegeben?	Falschberatung, Frist- und Vermögensschäden, Deckungsfragen

Ampel für den ersten Kanzleialltag

Stufe	Beispiele	Praxisregel
GRÜN	Öffentliche Gesetze, fiktive Fälle, allgemeine Formulierungen, belastbar anonymisierte Daten; freigegebenes Tool; Ergebnis wird geprüft.	Typischerweise niedriges Geheimnis- und Datenschutzrisiko. Qualitätskontrolle bleibt erforderlich.
GELB	Identifizierbare Mandatsdaten in einer geprüften Business-/Enterprise-Umgebung; Dokumentenanalyse; Transkription; Connectoren; Agenten; ausländische Supportzugriffe.	Nur nach dokumentierter §-62a-/DSGVO-Prüfung, technischen Kontrollen und gegebenenfalls Einwilligung.
ROT	Mandatsdaten in privaten oder nicht freigegebenen Accounts; Training mit Eingaben aktiviert; unkontrollierte Plugins; Passwörter/ELSTER-Zugänge; ungeprüfte finale Beratung oder autonomer Versand.	Nicht einsetzen. Erst Architektur, Vertrag und Prozess ändern.

STAND DER RECHTSPRECHUNG **Keine speziell einschlägige veröffentlichte Entscheidung identifiziert**

In öffentlich zugänglichen Quellen wurde zum Stichtag keine Entscheidung gefunden, die den Einsatz generativer KI durch Steuerberaterinnen oder Steuerberater konkret an § 62a StBerG und § 203 StGB misst. Das schließt nicht aus, dass unveröffentlichte oder nur in Datenbanken vorhandene Entscheidungen existieren. Die Einordnung stützt sich daher vor allem auf Gesetz, Gesetzesmaterialien und berufsständische bzw. aufsichtsbehördliche Orientierung.

Inhalt Aufbau der Handreichung

LESELOGIK Drei Kennzeichnungen im Text

„Gesetzlich klar“ bezeichnet eine unmittelbar aus Normtext oder gefestigter Grundstruktur ableitbare Aussage. „Vertretbare Einordnung“ markiert eine begründete Anwendung auf KI-Sachverhalte. „Offene Frage / konservative Praxis“ weist auf fehlende Rechtsprechung, Produktabhängigkeit oder Auslegungsunsicherheit hin.

1 Ausgangspunkt, Reichweite und Begriffe

Der Einsatz künstlicher Intelligenz ist für Steuerkanzleien kein einheitlicher Rechtsfall. Ein Sprachmodell, eine OCR-Funktion, ein Fachdatenbank-Assistent, ein Meeting-Bot, ein E-Mail-Copilot und ein autonomer Agent unterscheiden sich technisch und rechtlich. Ebenso relevant ist, ob ein Tool lokal, in einer EU-Cloud, über eine API oder in einem Consumer-Webkonto genutzt wird.

Diese Handreichung setzt deshalb nicht bei Produktnamen an. Sie betrachtet die konkrete Verarbeitungskette: Wer ist Vertragspartner? Welche Daten werden eingegeben oder automatisch abgerufen? Wo werden sie gespeichert und verarbeitet? Werden sie für Training oder Produktverbesserung genutzt? Welche Subdienstleister, Supportzugriffe, Suchfunktionen oder Connectoren sind beteiligt?

1.1 Adressaten und Anwendungsbereich

Adressaten sind Steuerberaterinnen und Steuerberater, steuerberatende Berufsausübungsgesellschaften sowie Kanzleimitarbeitende, die KI-Systeme auswählen, freigeben oder nutzen. Die berufsrechtliche Letztverantwortung liegt bei den Berufsträgern und - je nach Organisationsform - bei der Kanzleileitung.

Erfasst sind sowohl generative KI-Systeme als auch nicht-generative Systeme, wenn sie Daten analysieren, klassifizieren, prognostizieren oder Entscheidungen vorbereiten. Viele praktische Pflichten gelten außerdem unabhängig davon, ob ein Produkt rechtstechnisch als KI-System im Sinne der KI-Verordnung einzustufen ist: Berufsverschwiegenheit, DSGVO, IT-Sicherheit und fachliche Sorgfalt bleiben anwendbar.

1.2 Wichtige Begriffe

Begriff	Praxisbedeutung
Berufsgeheimnis / fremdes Geheimnis	Nicht öffentlich bekannte Information, an deren Geheimhaltung ein sachlich begründetes Interesse besteht und die im beruflichen Zusammenhang bekannt wurde. Erfasst sind nicht nur personenbezogene Daten, sondern etwa auch Unternehmens-, Vertrags-, Steuer- und Mandatsinformationen.
Personenbezogene Daten	Informationen über identifizierte oder identifizierbare natürliche Personen. Daten juristischer Personen sind nicht als solche von der DSGVO geschützt, können aber Berufs- und Geschäftsgeheimnisse sein.
Anonymisierung	Veränderung, nach der eine Person unter Berücksichtigung aller vernünftigerweise einsetzbaren Mittel nicht mehr identifizierbar ist. Das Entfernen von Name und Steuernummer genügt häufig nicht.
Pseudonymisierung	Ersetzung direkter Kennzeichen durch Codes. Die Zuordnung bleibt mit Zusatzwissen möglich. Die Daten bleiben personenbezogen und regelmäßig auch mandatsbezogen geheim.
Dienstleister nach § 62a StBerG	Andere Person oder Stelle, die im Rahmen der Berufsausübung mit einer Dienstleistung beauftragt wird. Bei KI ist regelmäßig die juristische Anbieterin bzw. die gesamte relevante Leistungskette zu betrachten - nicht das mathematische Modell als solches.
Auftragsverarbeiter	Stelle, die personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Verantwortlichen verarbeitet. Eigene Zwecke, etwa Training oder Produktverbesserung mit Kanzleidaten, können diese Einordnung verändern.
Betreiber nach KI-VO	Eine natürliche oder juristische Person, Behörde oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet. Eine Kanzlei ist bei typischer Nutzung fremder KI-Produkte regelmäßig Betreiberin.
Anbieter nach KI-VO	Akteur, der ein KI-System oder Modell entwickelt bzw. entwickeln lässt und unter eigenem Namen oder eigener Marke in Verkehr bringt oder in Betrieb nimmt. Eigene Kanzlei-Tools können im Einzelfall einen Rollenwechsel auslösen.

VERTRETBARE EINORDNUNG **Technischer Zugriff ist nicht auf menschliches Mitlesen beschränkt**

Bei gewöhnlicher Cloud-Inferenz werden Eingaben systemseitig verarbeitet. Berufs- und datenschutzrechtlich sollte deshalb nicht darauf abgestellt werden, ob ein Beschäftigter des Anbieters die Eingabe tatsächlich liest. Maßgeblich sind Zugangs- und Verarbeitungsmöglichkeiten, Weisungsbindung, technische Schutzmaßnahmen und die gesamte Dienstleisterkette. Bei wirksamer Ende-zu-Ende-Verschlüsselung ohne Entschlüsselungsmöglichkeit des Dienstleisters kann die Bewertung anders ausfallen.

1.3 Was dieses Dokument nicht ersetzt

die Prüfung eines konkreten Vertrags, Data Processing Addendum, Subprozessorenverzeichnisses und Transfermechanismus;

die berufsrechtliche Einzelfallauskunft der zuständigen Steuerberaterkammer;

die Beratung durch Datenschutzbeauftragte oder spezialisierte Rechtsberatung bei komplexen oder hochriskanten Einsatzfällen;

eine technische Sicherheitsprüfung, insbesondere bei Agenten, Connectoren, Browser-Erweiterungen oder selbst entwickelten Anwendungen;

die fachliche Prüfung des konkreten Arbeitsergebnisses.

2 Prüfmodell: Daten - Tool - Anwendungsfall - Kontrolle

Eine KI-Freigabe sollte niemals nur lauten „ChatGPT erlaubt“ oder „Copilot verboten“. Rechtssicherer und praktikabler ist ein Vier-Faktoren-Modell. Es verbindet die DStV-Logik „Tool - Anwendungsfall - Daten - Risiko“ mit der spezifischen Verantwortung des steuerberatenden Berufsstands. [S17]

2.1 Faktor 1: Welche Daten?

Datenklasse	Beispiele	Konsequenz
A - öffentlich / neutral	Gesetze, Verwaltungsanweisungen, allgemein zugängliche Texte, fiktive Fälle	Kein Mandatsgeheimnis; gegebenenfalls Urheberrecht und Qualität prüfen.
B - intern, nicht mandatsbezogen	Kanzleiprozesse, eigene Vorlagen, interne Strategie, Mitarbeiterinformationen	Geschäftsgeheimnis, Beschäftigtendatenschutz und IT-Sicherheit beachten.
C - pseudonymisiert	Name ersetzt, Zuordnungsschlüssel vorhanden oder Re-Identifikation aus Kontext möglich	Weiterhin personenbezogen und regelmäßig Berufsgeheimnis.
D - identifizierbare Mandatsdaten	Steuererklärungen, Bescheide, Verträge, Bilanzen, Lohnunterlagen, E-Mails	Höchste berufs- und datenschutzrechtliche Prüfungstiefe.
E - besondere Schutzdaten	Gesundheit, Religion, Gewerkschaft, Strafdaten, Zugangsdaten, Passwörter, Authentisierungstoken	Zusätzliche Rechtsgrundlage und Sicherheitsmaßnahmen; Zugangsdaten gehören grundsätzlich nicht in KI-Eingaben.

2.2 Faktor 2: Welches Tool - in welcher Variante?

Die Prüfung muss mindestens die konkrete juristische Anbieterin, den Tarif, die Nutzerverwaltung, die Datenregion, den Inferenzort, die Speicherfristen, die Trainingsnutzung, Supportzugriffe, Subdienstleister, Websuche, Plugins, Connectoren und Export-/Löschmöglichkeiten erfassen. Produktbedingungen können sich ändern; Freigaben sind deshalb zu befristen und bei wesentlichen Änderungen zu erneuern.

> GESETZLICH KLAR **Ein Vertrag muss die tatsächliche Verarbeitung abbilden**
> Ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO und die Vereinbarung nach § 62a Abs. 3 StBerG dürfen keine bloßen Papierübungen sein. Sie müssen zur tatsächlich aktivierten Produktfunktion, Region und Dienstleisterkette passen. [S3] [S9] [S10]

2.3 Faktor 3: Welcher Anwendungsfall?

Anwendungsfall	Typische Daten	Risikotendenz	Zentrale Kontrolle
Sprachliche Überarbeitung	öffentlich oder intern	meist niedrig	Kein sensibler Sachverhalt, klare Kennzeichnung als Entwurf.
Fachrecherche mit Fachdatenbank-KI	fachliche Frage, ggf. ohne Mandatsdaten	niedrig bis mittel	Quellen, Aktualität und Fundstellen kontrollieren.
Analyse eines konkreten Steuerbescheids	identifizierbare Mandatsdaten	hoch	§ 62a, § 203, DSGVO, ggf. Einwilligung; dokumentierte Fachprüfung.
Beleg-OCR / Buchungsvorschlag	Mandats- und Rechnungsdaten	hoch, aber oft standardisierbar	Vertikale Fachlösung, klare Verträge, Stichproben und Fehlerkontrollen.
Meeting-Transkription	Stimmen, Inhalte, ggf. Geheimnisse	hoch	Vorherige Information/Einwilligung zur Aufnahme, Speicher- und Löschkonzept.
E-Mail-Entwurf mit Mandatsbezug	Mandatsdaten	hoch	freigegebene Umgebung; kein autonomer Versand; fachliche Freigabe.
Recruiting / CV-Sortierung	Bewerberdaten	hoch / AI-Act-Relevanz	Beschäftigtendatenschutz, Mitbestimmung, potenziell Hochrisiko-KI.

Anwendungsfall	Typische Daten	Risikotendenz	Zentrale Kontrolle
Website-Chatbot	Besucherfragen	mittel	Art.-50-Information über KI-Interaktion, Datenschutz, keine unkontrollierte Mandatsannahme.
Agent mit DATEV-/DMS-/E-Mail-Connector	breiter Daten- und Aktionszugriff	sehr hoch	Least privilege, Freigabeschritte, Logs, technische Tests, Exit- und Incident-Prozess.

2.4 Faktor 4: Welche Kontrolle?

Die erforderliche menschliche Prüfung richtet sich nach Schadenspotenzial, fachlicher Komplexität, Datenmenge und Automatisierungsgrad. Eine bloße formale Durchsicht ist keine wirksame Kontrolle, wenn der Prüfer die sachliche Richtigkeit nicht beurteilen kann. Für steuerliche Aussagen müssen mindestens Sachverhalt, Rechtsstand, Primärquellen, Berechnung und Ergebnislogik nachvollzogen werden.

Kontrollstufe	Beispiele	Mindeststandard
Stufe 1 - sprachlich	Rechtschreibung, Ton, Struktur	Stichprobe und Sichtprüfung; keine Mandatsentscheidung.
Stufe 2 - fachlicher Entwurf	Mandantenbrief, Recherche-Zusammenfassung	Quellenprüfung, Sachverhaltsabgleich, Freigabe durch fachkundige Person.
Stufe 3 - entscheidungsnah	Einspruch, Gestaltung, Frist, Steuerberechnung	vollständige fachliche Prüfung, dokumentierte Freigabe, gegebenenfalls Vier-Augen-Prinzip.
Stufe 4 - agentisch / ausführend	Versand, Buchung, Datenänderung, Portalaktion	vorherige Genehmigung kritischer Aktionen, technische Limits, Protokollierung, Rollback und laufende Überwachung.

3 Berufsrecht und § 62a StBerG

§ 57 Abs. 1 StBerG verpflichtet zur unabhängigen, eigenverantwortlichen, gewissenhaften und verschwiegenen Berufsausübung. § 5 BOStB konkretisiert die Verschwiegenheit: Geschützt ist grundsätzlich alles, was in Ausübung des Berufs bekannt geworden ist; die Pflicht besteht über das Mandat hinaus fort. [S1] [S5]

KI-Nutzung berührt sämtliche Grundpflichten zugleich. Die Verschwiegenheit betrifft die Datenweitergabe. Eigenverantwortlichkeit und Unabhängigkeit verlangen, dass die Kanzlei die Entscheidungshoheit behält. Gewissenhaftigkeit verlangt Auswahl-, Kontroll- und Fortbildungsmaßnahmen.

3.1 Beschäftigte und externe Dienstleister unterscheiden

Für Beschäftigte und sonstige in der Kanzlei tätige Personen ist § 62 StBerG zentral: Sie sind in Textform zur Verschwiegenheit zu verpflichten, über strafrechtliche Folgen zu belehren und in der Einhaltung zu unterstützen. Für externe Dienstleister gilt § 62a StBerG. [S2] [S3]

> **PRAXIS Browser-Plugin, Meeting-Bot und KI-Connector sind ebenfalls Dienstleisterfragen**
> Die rechtliche Prüfung darf nicht beim Haupt-Chatbot enden. Ein Browser-Plugin, ein Transkriptionsdienst, eine Suchfunktion, ein Datei-Parser oder ein Connector kann eine eigene Stelle mit eigenen Subdienstleistern und Datenflüssen sein.

3.2 § 62a StBerG Absatz für Absatz

Normteil	Bedeutung für KI
Abs. 1 - Zugang und Erforderlichkeit	Dienstleister dürfen Zugang zu verschwiegenheitsgeschützten Tatsachen nur erhalten, soweit dies für die Dienstleistung erforderlich ist. Datenminimierung ist daher auch berufsrechtlich geboten.
Abs. 2 - Auswahl und Beendigung	Dienstleister sorgfältig auswählen; Zusammenarbeit unverzüglich beenden, wenn die Einhaltung der vertraglichen Vorgaben nicht gewährleistet ist. Anbieterprüfung ist kein einmaliger Akt.
Abs. 3 - Vertrag in Textform	Dienstleister unter Belehrung über strafrechtliche Folgen zur Verschwiegenheit verpflichten; Kenntnisnahme auf Erforderliches begrenzen; weitere Dienstleister nur mit Ermächtigung und entsprechender Verpflichtung.
Abs. 4 - Ausland	Bei im Ausland erbrachten Leistungen muss der dortige Geheimnisschutz grundsätzlich vergleichbar sein, sofern der Geheimnisschutz dies im Einzelfall gebietet. Berufsrecht und DSGVO-Drittlandrecht sind getrennt zu prüfen.
Abs. 5 - einzelnes Mandat	Dient die Dienstleistung unmittelbar einem einzelnen Mandat, ist die Einwilligung des Mandanten erforderlich.
Abs. 6 - ausdrücklicher Verzicht	Auch bei Einwilligung gelten Auswahl- und Vertragsanforderungen grundsätzlich weiter. Der Mandant kann ausdrücklich auf Anforderungen der Absätze 2 und 3 verzichten.
Abs. 7 - gesetzliche Sonderfälle	Spezialgesetzliche Dienstleistungsfälle und bereits anderweitig gebundene Personen werden gesondert behandelt.
Abs. 8 - Datenschutz bleibt unberührt	Die berufsrechtliche Zulässigkeit ersetzt keine DSGVO-Prüfung.

3.3 Was muss in die Vertragskette?

Ein gewöhnlicher Art.-28-Vertrag kann viele Anforderungen bereits enthalten. Er deckt § 62a Abs. 3 aber nicht zwingend vollständig ab. Umgekehrt ersetzt eine Berufsgeheimnisvereinbarung nicht die Pflichtinhalte des Art. 28 DSGVO. BStBK und DStV stellen in ihren Datenschutz-Hinweisen einen Zusatz zum Auftragsverarbeitungsvertrag bereit. [S9]

Mindestfragen für § 62a Abs. 2 und 3	
☐	konkrete Dienstleistung, Zweck und Datenkategorien;
☐	Verpflichtung der Anbieterin und der tatsächlich mitwirkenden natürlichen Personen zur Verschwiegenheit;
☐	Belehrung über die strafrechtlichen Folgen nach §§ 203, 204 StGB;
☐	Need-to-know-Prinzip und technische Zugriffsbeschränkung;
☐	Ermächtigung und Verfahren für Subdienstleister einschließlich Vorabinformation und Widerspruchsmöglichkeit;
☐	Weitergabe der Geheimhaltungs- und Sicherheitspflichten an die gesamte Unterauftragnehmerkette;
☐	Verbot der Nutzung von Eingaben, Dateien und Ausgaben zu eigenen Trainings-, Werbe- oder Produktverbesserungszwecken;
☐	Datenregion, Fernzugriffe, Support, Logs, Backups und Löschfristen;
☐	Meldepflichten bei Sicherheitsvorfällen, behördlichen Zugriffen und Vertragsänderungen;
☐	Prüf-, Auskunfts- und Exit-Rechte sowie unverzügliche Beendigungsmöglichkeit.

GESETZLICH KLAR **„Kein Training“ ist wichtig, aber nicht ausreichend**

Selbst wenn ein Anbieter Eingaben nicht zum Modelltraining verwendet, bleiben Erforderlichkeit, Geheimhaltung, Unterauftragnehmer, Speicherfristen, Supportzugriffe, Auslandsverarbeitung und Sicherheit zu prüfen.

3.4 Wann dient die Dienstleistung unmittelbar einem einzelnen Mandat?

Die Gesetzesbegründung nennt als klassische Beispiele Sachverständige, Detektive, Stenografen bzw. Schreibkräfte und Übersetzer. Entscheidend ist nicht die Vertragsform oder Vergütung, sondern ob ein besonderer Bedarf gerade in einem einzelnen Mandat besteht. Allgemeine Infrastruktur- oder Kanzleidienstleistungen sollen demgegenüber ohne Einwilligung möglich sein, sofern die übrigen Voraussetzungen erfüllt sind. [S6]

Bei generativer KI ist die Grenzziehung noch nicht höchstrichterlich geklärt. Ein zentral beschaffter, mandatsübergreifend genutzter Kanzleiassistent spricht eher für ein allgemeines Arbeitsmittel. Wird dagegen für einen einzelnen komplexen Fall gezielt ein externer Spezialdienst oder ein nur hierfür konfigurierter Analyse-Service eingeschaltet, spricht mehr für Abs. 5.

Indiz	Beispiele
Eher allgemeines Arbeitsmittel	zentrale Kanzleilizenz; Nutzung für viele Mandate; standardisierte Sicherheits- und Vertragsarchitektur; kein besonderer externer Facheinsatz nur für einen Fall
Eher unmittelbar einzelmandatsbezogen	nur für ein konkretes Mandat beschaffter Spezialdienst; externer KI-Analyst/Sachverständiger; individuelle Modell- oder Datenaufbereitung ausschließlich für einen Fall
Grenzfall	allgemeiner Chat-Assistent, in den im konkreten Mandat umfangreiche identifizierbare Unterlagen geladen und fallbezogen analysiert werden

OFFENE FRAGE / KONSERVATIVE PRAXIS **Bei sensibler fallbezogener KI-Analyse Einwilligung erwägen**

Die BStBK weist auf die Auslegungsunsicherheit hin und empfiehlt bei sensiblen mandantenbezogenen Daten eine vorherige Einwilligung. Diese konservative Vorgehensweise schafft zusätzliche Transparenz, ersetzt aber weder § 62a Abs. 2 bis 4 noch die DSGVO. [S8]

3.5 Einwilligung, Entbindung und Verzicht sauber trennen

Instrument	Funktion	Grenzen
Einwilligung nach § 62a Abs. 5	Erlaubt die Einschaltung eines Dienstleisters, der unmittelbar einem einzelnen Mandat dient.	konkreter Dienstleister, Zweck, Daten, Umfang, Risiken und Alternativen erläutern
Entbindung / Offenbarungsbefugnis	Nimmt der Offenbarung gegenüber den benannten Empfängern im vereinbarten Umfang das „Unbefugte“.	nur durch verfügungsberechtigte Geheimnisträger; Drittgeheimnisse gesondert beachten
Ausdrücklicher Verzicht nach § 62a Abs. 6	Kann Anforderungen aus Abs. 2 und 3 abbedingen.	nur eng, einzeln bezeichnet, informiert und nach Risikoabwägung; kein pauschaler Blankoverzicht
Datenschutzrechtliche Einwilligung	Kann eine Rechtsgrundlage für bestimmte personenbezogene Datenverarbeitungen sein.	freiwillig, informiert, spezifisch, widerruflich; oft nicht die einzig mögliche oder stabilste Grundlage
AVV nach Art. 28 DSGVO	Regelt Auftragsverarbeitung bei Weisungsbindung.	ersetzt weder Mandanteneinwilligung nach Abs. 5 noch §-62a-Geheimnisschutz vollständig

WARNUNG **Kein pauschaler „Verzicht auf § 62a und Verschwiegenheit“**
Ein pauschaler AGB-Satz, wonach der Mandant jede KI-Nutzung und sämtliche Datenweitergaben gestattet, ist wegen fehlender Bestimmtheit, Transparenz, Drittgeheimnissen und fortbestehender gesetzlicher Pflichten kein belastbarer Standard. Der sicherere Weg ist ein geeignetes Tool mit vollständiger Vertrags- und Schutzarchitektur; Einwilligung und Teilverzicht bleiben Ausnahmeinstrumente.

3.6 Dienstleistungen im Ausland

„Ausland“ in § 62a Abs. 4 ist nicht deckungsgleich mit „Drittland“ nach der DSGVO. Auch eine Leistung innerhalb der EU kann im berufsrechtlichen Sinn im Ausland erbracht werden; umgekehrt löst eine bloße EU-Datenregion nicht alle Fragen, wenn Support, Administration, Logs oder Subdienstleister außerhalb der Region liegen.

Der Ausschussbericht zur Reform 2017 stellt klar, dass eine übliche informierte Einwilligung für die Offenbarung bei fehlendem vergleichbaren ausländischen Geheimnisschutz genügen kann; ein zusätzlicher ausdrücklicher Verzicht nach Abs. 6 ist für Abs. 4 nicht vorgesehen. Die Einwilligung muss aber die konkrete Auslandsverarbeitung und deren Risiken erfassen. [S7]

Auslandsprüfung - zwei Rechtsregime, eine Datenflusskarte	
☐	Wo erfolgen Speicherung, Inferenz, Protokollierung, Backup und Support?
☐	Können Beschäftigte oder Behörden außerhalb Deutschlands/EU auf Klartext zugreifen?
☐	Welche Subdienstleister in welchen Staaten sind beteiligt?
☐	Welche rechtlichen Schutzpflichten und Durchsetzungsmöglichkeiten bestehen dort?
☐	Ist eine mandatsbezogene Einwilligung oder Entbindung wirksam und ausreichend konkret?
☐	Unabhängig davon: Ist der Transfer nach Kapitel V DSGVO zulässig?
☐	Gibt es eine gleichwertige Alternative ohne Auslandszugriff?

4 Strafrechtlicher Geheimnisschutz nach § 203 StGB

Steuerberaterinnen und Steuerberater gehören zu den in § 203 Abs. 1 StGB genannten Berufsgeheimnisträgern. Geschützt sind fremde Geheimnisse, die ihnen anvertraut oder sonst bekannt geworden sind. Die Norm erfasst damit auch Geheimnisse juristischer Personen und Informationen ohne Personenbezug. [S4]

4.1 Mitwirkende Personen dürfen eingebunden werden

§ 203 Abs. 3 StGB erlaubt die Offenbarung gegenüber sonstigen mitwirkenden Personen, soweit dies für deren Tätigkeit erforderlich ist. Das war das strafrechtliche Gegenstück zur berufsrechtlichen Dienstleisterreform 2017. Die Zulässigkeit verlangt eine funktionale Mitwirkung und eine Begrenzung auf das Erforderliche.

Eine KI-Anbieterin kann als mitwirkende Stelle in Betracht kommen, wenn sie die technische Dienstleistung für die Kanzlei erbringt. Entscheidend ist wiederum die Organisation hinter dem System. Die maschinelle Verarbeitung macht die Offenbarung nicht automatisch irrelevant.

4.2 Weitere Mitwirkende und Unterauftragnehmer

§ 203 Abs. 4 StGB erstreckt den strafrechtlichen Geheimnisschutz auf mitwirkende Personen. Zugleich kann für den Berufsgeheimnisträger ein Risiko entstehen, wenn er nicht dafür Sorge getragen hat, dass weitere mitwirkende Personen zur Geheimhaltung verpflichtet werden und es anschließend zu einer unbefugten Offenbarung kommt. Deshalb sind Subprozessoren, Supportpartner und technische Unterauftragnehmer nicht nur eine DSGVO-Frage.

4.3 Berufsrecht und Strafrecht laufen nebeneinander

Der Ausschussbericht betont: Ein berufsrechtlich erlaubtes Offenbaren ist nicht „unbefugt“ im Sinne des § 203 StGB. Umgekehrt ist nicht jeder berufsrechtliche Organisationsfehler automatisch eine vollendete Straftat; die konkreten Tatbestandsvoraussetzungen des § 203 StGB müssen erfüllt sein. [S7]

> **VERTRETBARE EINORDNUNG** **Keine Gleichsetzung - aber auch keine Entwarnung**
> Ein fehlender §-62a-Zusatzvertrag kann berufsrechtlich problematisch sein, ohne dass bereits allein dadurch eine Straftat vollendet ist. Kommt es jedoch zu einer unbefugten Offenbarung oder wurde die Verpflichtung weiterer Mitwirkender pflichtwidrig nicht sichergestellt, kann die strafrechtliche Lage deutlich verschärft sein.

4.4 Einwilligung und Verfügungsbefugnis

Eine wirksame, informierte Entbindung oder Einwilligung des Geheimnisträgers kann eine Offenbarungsbefugnis schaffen. Sie wirkt jedoch nur in ihrem konkreten Umfang. Der Unterzeichner muss über das Geheimnis verfügen dürfen. In Mandatsunterlagen können zugleich Geheimnisse von Geschäftsführern, Mitarbeitenden, Angehörigen, Vertragspartnern oder Gesellschaften enthalten sein.

Bei einer juristischen Person ist zu prüfen, wer sie wirksam vertritt und ob zusätzlich Individualgeheimnisse natürlicher Personen betroffen sind. Eine allgemeine Unterschrift des Mandanten macht die Offenbarung solcher Drittgeheimnisse nicht automatisch zulässig.

4.5 Praktischer §-203-Prüfpfad

Prüffragen vor der Verarbeitung von Mandatsgeheimnissen	
☐	Liegt ein fremdes Geheimnis vor?
☐	Wem steht die Verfügungsbefugnis über dieses Geheimnis zu?
☐	Ist die externe Stelle funktional an der beruflichen Tätigkeit beteiligt?
☐	Ist der Zugang für die konkrete Tätigkeit erforderlich und minimiert?

Prüffragen vor der Verarbeitung von Mandatsgeheimnissen	
☐	Besteht eine gesetzliche oder wirksame rechtsgeschäftliche Offenbarungsbefugnis?
☐	Sind Anbieterin, natürliche Mitwirkende und Unterauftragnehmer in den Geheimnisschutz einbezogen?
☐	Sind technische und organisatorische Maßnahmen gegen unbefugte Offenbarung angemessen?
☐	Ist dokumentiert, warum die Kanzlei von einer befugten Einbindung ausgeht?

DOKUMENTATIONSREGEL **Befugnis, Erforderlichkeit und Dienstleisterkette gemeinsam festhalten**

Ein belastbarer Kurzvermerk benennt das betroffene Geheimnis bzw. die Datenklasse, den konkreten Zweck, die Offenbarungsbefugnis, die erforderlichen Empfänger einschließlich Unterauftragnehmern, die technischen Schutzmaßnahmen und die verantwortliche Freigabe. Eine bloße Ablage der Anbieter-AGB genügt dafür nicht.

5 Datenschutzrecht: DSGVO und BDSG

§ 62a Abs. 8 StBerG stellt ausdrücklich klar, dass Datenschutzrecht unberührt bleibt. Berufsgeheimnis und personenbezogene Daten überschneiden sich häufig, sind aber nicht identisch. Eine Bilanz einer GmbH kann berufsrechtlich geheim sein, ohne vollständig personenbezogen zu sein; umgekehrt können Beschäftigtendaten datenschutzrechtlich relevant sein, auch wenn sie nicht aus einem Mandat stammen. [S3]

5.1 Zweck und Datenbezug vorab bestimmen

Die Datenschutzkonferenz empfiehlt, Einsatzfelder und Zwecke vor der Einführung ausdrücklich festzulegen. Erst dann lässt sich prüfen, ob personenbezogene Daten erforderlich sind und welche Rechtsgrundlage greift. Das bloße Entfernen von Namen genügt nicht, wenn Identifikation über Kontext, seltene Merkmale, Dokumentstruktur oder Zusatzwissen möglich bleibt. [S10]

5.2 Rollen: Verantwortlicher, Auftragsverarbeiter oder eigener Zweck?

Für die steuerberatende Fachleistung ist die Kanzlei grundsätzlich selbst datenschutzrechtlich verantwortlich. Nutzt sie einen externen KI-Cloudanbieter ausschließlich nach Weisung, liegt häufig Auftragsverarbeitung nach Art. 28 DSGVO vor. Verwendet der Anbieter Eingaben dagegen für eigene Modelltrainings-, Analyse-, Werbe- oder Produktverbesserungszwecke, kann er insoweit eigener oder gemeinsam Verantwortlicher sein. Eine solche Eigenzwecknutzung ist bei Mandatsdaten regelmäßig nicht der vorzugswürdige Einsatzmodus. [S9] [S10]

Rolle	Indizien	Konsequenz
Reiner Auftragsverarbeiter	verarbeitet nur dokumentierte Weisungen; kein eigenes Training; klare Löschung; Subprozessorenkette	Art.-28-Vertrag plus §-62a-Zusatz, Kontrollen und Transferprüfung
Eigener Verantwortlicher	nutzt Daten für eigene Zwecke, z. B. allgemeine Produktverbesserung oder Profilbildung	eigene Rechtsgrundlage und Transparenz nötig; für Mandatsdaten meist ungeeignet
Gemeinsame Verantwortlichkeit	Kanzlei und Anbieter bestimmen Zwecke/Mittel in untrennbarer Weise gemeinsam	Art.-26-Regelung plus eigene Rechtsgrundlagen; erhöht Komplexität
Unklarer Status	Anbieterunterlagen widersprüchlich oder technisch unvollständig	keine Freigabe für personenbezogene oder geheime Daten bis Klärung

5.3 Rechtsgrundlage für jeden Verarbeitungsschritt

Für Erhebung, Übermittlung an den Anbieter, Speicherung, Auswertung, Rückgabe, Protokollierung und gegebenenfalls weitere Nutzung muss eine passende Rechtsgrundlage bestehen. Welche Grundlage einschlägig ist, hängt vom Zweck, Mandatsverhältnis, Dateninhalt und Betroffenenkreis ab. Besondere Kategorien personenbezogener Daten benötigen zusätzlich eine Grundlage nach Art. 9 DSGVO.

> **GESETZLICH KLAR** **Berufsrechtliche Einwilligung ist keine Universal-DSGVO-Einwilligung**
> Die Zustimmung des Mandanten zur Einschaltung eines KI-Dienstleisters kann Transparenz und Offenbarungsbefugnis schaffen. Sie ersetzt jedoch nicht automatisch die Rechtsgrundlage für sämtliche personenbezogenen Daten von Beschäftigten, Angehörigen, Geschäftspartnern oder sonstigen Dritten.

5.4 Art. 28, Subprozessoren und Vertragspraxis

Bei Auftragsverarbeitung ist ein Vertrag nach Art. 28 Abs. 3 DSGVO erforderlich. Er muss Gegenstand, Dauer, Art, Zweck, Datenarten, Betroffenenkategorien, Weisungen, Vertraulichkeit, Sicherheit, Subprozessoren, Unterstützung, Löschung und Nachweise regeln. Bei Mandatsgeheimnissen ist er um § 62a StBerG und §§ 203, 204 StGB zu ergänzen. [S9]

Eine allgemeine Genehmigung von Subprozessoren kann zulässig sein, wenn die Kanzlei über Änderungen informiert wird und eine realistische Widerspruchsmöglichkeit hat. Für KI-Dienste ist außerdem zu prüfen, ob Modelle, Suchdienste, Speicher-, Moderations-, Support- oder Telemetriedienste als weitere Auftragsverarbeiter beteiligt sind.

5.5 Training, Historie und Speicherfristen

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen verlangt, Eingabetraining, Chat-Historie, öffentliche Linkfreigaben und unnötige Langzeitspeicherung soweit möglich zu deaktivieren. Die DSK nennt ausdrücklich Einstellungen, bei denen Eingaben nicht für Training verwendet und Historien nicht länger als nötig gespeichert werden. [S10]

Datenschutzfreundliche Grundkonfiguration	
☐	Training / Modellverbesserung mit Kanzleidaten deaktiviert und vertraglich ausgeschlossen;
☐	Chat- und Dateihistorie auf das notwendige Minimum begrenzt;
☐	klare Löschung von Chats, Dateien, Logs und Backups;
☐	keine öffentliche Freigabe von Chats oder Dokumentenlinks;
☐	keine automatischen Connector-Synchronisationen ohne Daten- und Rechteprüfung;
☐	Telemetrie, Feedback und Supportzugriffe transparent geregelt;
☐	Export- und Löschmöglichkeiten getestet.

5.6 Internationale Datenübermittlung

Eine Speicherung oder Verarbeitung außerhalb des EWR sowie Remote-Zugriff aus Drittländern erfordert eine Grundlage nach Kapitel V DSGVO, etwa Angemessenheitsbeschluss oder geeignete Garantien. Zusätzlich ist eine Transfer-Risikoprüfung erforderlich, soweit kein Angemessenheitsbeschluss greift. Diese Prüfung ist unabhängig vom berufsrechtlichen Geheimnisschutz nach § 62a Abs. 4.

PRAXIS „EU Data Residency“ ist eine wichtige, aber unvollständige Aussage

Zu prüfen sind auch Inferenz, Logs, Missbrauchserkennung, Support, Administratorzugriff, Backups, Connectoren, Websuche und Subdienstleister. Eine EU-Speicherzusage kann einzelne Datenarten oder Funktionen ausnehmen.

5.7 Transparenz, Verzeichnis und Betroffenenrechte

Datenschutzhinweise und Verzeichnis von Verarbeitungstätigkeiten sind anzupassen, wenn KI-Einsatz neue Zwecke, Empfänger, Datenkategorien, Drittlandtransfers oder Speicherfristen mit sich bringt. Nicht jede einzelne Textassistenz muss werblich hervorgehoben werden; die gesetzlich erforderlichen Informationen müssen aber transparent und zutreffend sein.

Die Kanzlei muss außerdem Auskunft, Berichtigung, Löschung, Einschränkung und Widerspruch praktisch erfüllen können. Der Anbieter muss die hierfür notwendigen Informationen und Funktionen bereitstellen.

5.8 Datenschutz-Folgenabschätzung und Datenschutzbeauftragter

Eine DSFA ist nicht allein deshalb automatisch erforderlich, weil ein KI-Tool verwendet wird. Sie ist erforderlich, wenn die konkrete Verarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen zur Folge hat. Die DSK betont eine Vorab-Risikoprüfung und weist darauf hin, dass dies bei KI-Anwendungen vielfach der Fall sein kann. [S10]

Risikotreiber sind etwa umfangreiche oder hochsensible Daten, systematische Bewertung, neue Technologien, große Personengruppen, Zusammenführung von Datenbeständen, Überwachung oder entscheidungsnahe Automatisierung. Ist eine DSFA erforderlich, kann nach § 38 BDSG unabhängig von der Beschäftigtenzahl eine Pflicht zur Benennung eines Datenschutzbeauftragten bestehen. [S12]

5.9 Automatisierte Entscheidungen und menschliche Prüfung

Art. 22 DSGVO kann einschlägig sein, wenn eine ausschließlich automatisierte Entscheidung rechtliche Wirkung entfaltet oder Betroffene ähnlich erheblich beeinträchtigt. Eine bloße pro forma-Bestätigung durch einen Menschen genügt nicht. Die prüfende Person muss tatsächlich verstehen, eingreifen und die Entscheidung ändern können.

5.10 Datenschutz-Checkliste

DSGVO-Mindestprüfung für KI-Tools	
☐	Zweck und notwendige Daten festgelegt;
☐	Personenbezug und besondere Kategorien geprüft;
☐	Verantwortlicher / Auftragsverarbeiter / gemeinsame Verantwortlichkeit geklärt;
☐	Rechtsgrundlage für jeden Verarbeitungsschritt dokumentiert;
☐	Art.-28-Vertrag vollständig und mit §-62a-/§-203-Zusatz versehen;
☐	Subprozessoren und Änderungsverfahren geprüft;
☐	Training, Historie, Retention und Löschung konfiguriert;
☐	TOMs, Verschlüsselung, MFA, Rollen und Logging bewertet;
☐	Kapitel-V-Transferprüfung abgeschlossen;
☐	Datenschutzhinweise und Verzeichnis aktualisiert;
☐	DSFA-Vorabprüfung durchgeführt;
☐	Betroffenenrechte und Incident-Prozess praktisch getestet.

6 EU AI Act nach dem Digital Omnibus 2026

Die KI-Verordnung folgt einem risikobasierten Ansatz. Die meisten in Kanzleien eingesetzten Assistenzsysteme fallen in die Kategorie minimaler oder begrenzter Risiken. Zusätzliche Pflichten entstehen aber durch die konkrete Rolle, den Einsatzkontext und die Funktion - insbesondere bei Personalentscheidungen, biometrischen/emotionalen Auswertungen, öffentlich interagierenden Chatbots oder KI-generierten öffentlichen Inhalten. [S13]-[S16]

6.1 Aktueller Zeitplan zum 28. Juli 2026

Datum	Bedeutung
1. August 2024	KI-Verordnung tritt in Kraft.
2. Februar 2025	Verbote bestimmter KI-Praktiken und Art. 4 KI-Kompetenz werden anwendbar.
2. August 2025	Governance- und GPAI-Pflichten werden weitgehend anwendbar.
27. Juli 2026	Verordnung (EU) 2026/1744 („Digital Omnibus on AI“) tritt in Kraft; Art. 4 und Zeitplan werden geändert.
2. August 2026	Großer Teil der übrigen Regeln, Durchsetzung und Art. 50 Transparenzpflichten werden anwendbar.
2. Dezember 2027	Hochrisiko-Regeln für die in Anhang III genannten sensiblen Einsatzbereiche, u. a. Beschäftigung, werden anwendbar.
2. August 2028	Hochrisiko-Regeln für KI als Sicherheitskomponente bestimmter regulierter Produkte nach Anhang I werden anwendbar.

KORREKTUR ZUR BSTBK-FAQ **Frühere August-2026-Aussage ist überholt**

Die BStBK-FAQ spricht auf Rechtsstand Juli 2025 noch davon, dass umfassende Hochrisikopflichten „vermutlich ab August 2026“ gelten. Nach der inzwischen in Kraft getretenen Änderungsverordnung gelten für Anhang-III-Hochrisikofälle der 2. Dezember 2027 und für Anhang-I-Produkte der 2. August 2028. [S8] [S14]

6.2 Art. 4 KI-Kompetenz - was Kanzleien tatsächlich tun müssen

Art. 4 Abs. 1 verlangt nach der Änderung, dass Anbieter und Betreiber Maßnahmen ergreifen, um die Entwicklung der KI-Kompetenz ihres Personals und anderer in ihrem Auftrag mit Betrieb und Nutzung befasster Personen zu unterstützen. Zu berücksichtigen sind technische Kenntnisse, Erfahrung, Ausbildung, Schulung, Nutzungskontext und betroffene Personengruppen. Ein bestimmtes oder „ausreichendes“ individuelles Kompetenzniveau muss nicht garantiert werden. [S15]

Die Pflicht bleibt damit eine risikobasierte Organisationspflicht. Ein einmaliger allgemeiner Vortrag kann für risikoarme Textassistenz genügen, nicht aber für Mitarbeitende, die sensible Dokumente analysieren, Agenten freigeben oder Personalentscheidungen vorbereiten. Die Kommission hält es in vielen Fällen für unzureichend, nur die Bedienungsanleitung lesen zu lassen.

Zielgruppe	Mindestinhalte
Basisnutzer	Funktionsweise, Halluzinationen, Datenklassen, erlaubte Tools, sichere Prompts, Meldeweg
Fachnutzer	Quellenprüfung, Rechtsstand, Dokumenten- und Berechnungsprüfung, Mandatsfreigabe
Administratoren	Tarife, Rollen, Logging, Retention, Connectoren, Subprozessoren, Incident Response
Führung / Berufsträger	Risikoeinstufung, Freigaben, § 62a/§ 203, DSGVO, AI Act, Qualität und Haftung
Entwickler / Agentenbauer	Systemgrenzen, Zugriffskontrolle, Tests, Human-in-the-loop, Monitoring, Änderungsmanagement

DOKUMENTATION **Kein Zertifikat vorgeschrieben - Nachweis dennoch sinnvoll**

Die Kommission verlangt kein bestimmtes Zertifikat und keine festgelegte Governance-Struktur. Ein internes Schulungs- und Maßnahmenprotokoll, Rollenmatrix, Unterlagen und Aktualisierungsrhythmus sind als Nachweis und zur Kanzleiorganisation sinnvoll. [S15]

6.3 Art. 50 Transparenz ab 2. August 2026

Fall	Pflichtenkern
Direkte Interaktion mit Menschen	Anbieter müssen Systeme grundsätzlich so gestalten, dass Menschen erkennen, dass sie mit KI interagieren, sofern dies nicht offensichtlich ist. Kanzleien sollten bei Website- oder Mandantenchatbots die Umsetzung überprüfen.
Maschinenlesbare Markierung	Anbieter generativer Systeme müssen Ausgaben technisch markierbar und erkennbar machen, soweit technisch machbar. Dies betrifft primär Anbieter.
Deepfakes	Betreiber müssen künstlich erzeugte oder manipulierte Bild-, Audio- oder Videoinhalte, die authentisch erscheinen, grundsätzlich offenlegen.
Öffentliche Texte zu Themen öffentlichen Interesses	Betreiber müssen KI-generierte/manipulierte Texte kennzeichnen, wenn sie zur Information der Öffentlichkeit veröffentlicht werden. Ausnahme: substanzielle menschliche Prüfung bzw. redaktionelle Kontrolle und übernommene redaktionelle Verantwortung.

PRAXISANTWORT **Kein allgemeiner KI-Hinweis auf jedem Mandantenbrief**

Ein individuell an einen Mandanten gerichteter, fachlich geprüfter Brief ist regelmäßig keine Veröffentlichung zur Information der Öffentlichkeit über eine Angelegenheit öffentlichen Interesses. Selbst in öffentlichen Fachinformationen entfällt die Kennzeichnungspflicht für Text nach Art. 50 Abs. 4, wenn eine substanzielle menschliche Prüfung oder redaktionelle Kontrolle stattfindet und eine Person redaktionelle Verantwortung übernimmt. Oberflächliche Rechtschreibkontrolle genügt dafür nicht. [S16]

6.4 Verbotene Praktiken und rote Linien

Für Kanzleien besonders relevant ist das Verbot bestimmter Emotionserkennung am Arbeitsplatz. Tools, die aus Stimme, Gesicht oder Verhalten Emotionen von Beschäftigten ableiten, sind daher nicht als gewöhnliche Meeting- oder HR-Funktion zu behandeln. Weitere Verbote betreffen unter anderem manipulative, ausbeuterische oder bestimmte biometrische Praktiken. [S13]

6.5 Hochrisiko-Kontexte in Steuerkanzleien

Use Case	AI-Act-Einordnung	Praxis
Normale Text- und Rechercheassistenz	in der Regel nicht allein deshalb hochriskant	Qualität, Art. 4, gegebenenfalls Art. 50 und andere Rechtsgebiete beachten.
Bewerberauswahl / CV-Sortierung	kann Anhang-III-Hochrisiko sein	ab 2.12.2027 umfassende Betreiberpflichten; schon heute DSGVO, AGG, Mitbestimmung und Governance.
Leistungsüberwachung / Beförderung / Kündigung	kann Hochrisiko sein	keine intransparente automatisierte Bewertung; strenge Human-Oversight- und Datenregeln.
Emotionserkennung am Arbeitsplatz	grundsätzlich verbotene Praktik, enge Ausnahmen	nicht freigeben, nur spezialisierte rechtliche Prüfung.
Kredit- oder Zugangsbewertung für wesentliche Dienste	je nach Rolle und Zweck potenziell Hochrisiko	relevant, wenn Kanzlei selbst solche Entscheidungen unterstützt oder System für Mandanten betreibt.
Eigenes extern angebotenes KI-Steuerprodukt	möglicher Anbieterstatus	Produkt-, Markt- und Haftungspflichten gesondert prüfen.

6.6 Vom Betreiber zum Anbieter

Wer ein fremdes System lediglich nutzt, ist typischerweise Betreiber. Wer ein System unter eigenem Namen oder eigener Marke anbietet, dessen Zweck wesentlich verändert oder es erheblich modifiziert, kann Anbieterpflichten übernehmen. Das ist für Kanzleien relevant, die eigene Mandantenportale, KI-Assistenten oder White-Label-Produkte entwickeln und Dritten bereitstellen.

> OFFENE FRAGE / TECHNISCHE EINZELFALLPRÜFUNG **Eigene Apps und Agenten**
>
> Ob eine mit Codex, Claude Code oder anderen Entwicklungsassistenten erstellte Kanzlei-App selbst ein KI-System enthält, hängt von der fertigen Architektur ab. Eine mit KI programmierte, anschließend rein deterministische App ist nicht allein wegen ihrer Entstehung ein KI-System. Ruft sie im Betrieb ein Modell auf, verarbeitet sie Daten über diese Laufzeitkomponente und ist entsprechend zu prüfen.

6.7 Mindestprüfung einer selbst entwickelten Kanzlei-App

Prüfbereich	Kernfrage	Mindestnachweis
Laufzeitarchitektur	Arbeitet die fertige App rein lokal und deterministisch oder ruft sie Modelle, APIs, Cloudspeicher bzw. externe Dienste auf?	Architektur- und Datenflussdiagramm; dokumentierte Endpunkte
Datenabfluss	Welche Nutzdaten, Metadaten, Logs, Crash-Reports, Telemetrie und Backups verlassen das Kanzleinetz?	Netzwerk- und Protokolltest in einer Testumgebung
Abhängigkeiten	Welche Bibliotheken, Container, Plugins und Dienste werden eingesetzt; wie werden Schwachstellen und Updates beherrscht?	Software-Stückliste, Lizenz- und Schwachstellenscan
Identität und Geheimnisse	Wo liegen API-Schlüssel, Zertifikate und Zugangsdaten; gelten Least Privilege, Rotation und Trennung von Test/Produktion?	Secrets-Konzept, Rollenmatrix, MFA und Schlüsselrotation
Fehler und Änderungen	Was passiert bei Ausfall, Fehlantwort, Datenkorruption oder Modellwechsel; gibt es Rollback, Tests und Freigaben?	Abnahmetests, Change-Log, Backup-/Restore- und Rollback-Nachweis
Verantwortung	Wer wartet, überwacht und stoppt die Anwendung; wann wird neu geprüft?	Benannte Produktverantwortung, Incident- und Neubewertungsprozess

7 Fachliche Verantwortung, Qualität und Haftung

Die berufsrechtliche Eigenverantwortlichkeit endet nicht am Interface eines KI-Tools. Die BStBK betont, dass Entscheidungen und Verantwortung beim Menschen bleiben und KI-Ergebnisse stets fachkundig geprüft werden müssen. [S8]

7.1 KI ist kein zweiter Berufsträger

Ein Vier-Augen-Prinzip setzt zwei fachlich verantwortliche Prüfungen voraus. Ein Sprachmodell kann Gegenargumente oder Prüffragen liefern, ersetzt aber keine zweite qualifizierte Person. Ebenso darf eine Quellenangabe der KI nicht als Nachweis gelten, bevor die Originalquelle geöffnet und inhaltlich geprüft wurde.

7.2 Mindestprüfung steuerlicher KI-Ergebnisse

Fachliche Freigabe - steuerlicher Inhalt	
☐	Sachverhalt vollständig und richtig wiedergegeben?
☐	Rechtsstand und maßgeblicher Zeitraum korrekt?
☐	Gesetz, Richtlinie, BMF-Schreiben und Rechtsprechung im Original geprüft?
☐	Fundstellen real, einschlägig und nicht aus dem Zusammenhang gerissen?
☐	Berechnung reproduziert und mit Plausibilitätskontrolle versehen?
☐	Gegenansichten, Übergangsrecht und Verfahrensfragen berücksichtigt?
☐	Fristen, Zuständigkeit und Formanforderungen separat geprüft?
☐	Ergebnis in verständlicher Form mit Unsicherheiten und Annahmen dokumentiert?
☐	Bei hohem Schadenpotenzial Vier-Augen-Freigabe oder Spezialprüfung?
☐	Finale Fassung ohne verborgene Prompts, Kommentare oder Metadaten versandt?

7.3 Dokumentation nach Risiko

Dokustufe	Beispiel	Nachweis
Leicht	allgemeine Formulierung ohne Fach- oder Mandatsdaten	Tool und Zweck im KI-Register; normale Endkontrolle
Mittel	fachlicher Entwurf ohne Mandatsdaten	Prompt/Quelle bei Bedarf, Prüfer, fachliche Freigabe, Version
Hoch	Mandatsdaten, Berechnung, Einspruch, Gestaltung, Agentenaktion	Use-Case-Freigabe, Daten-/Vertragsprüfung, wesentliche Eingaben/Quellen, Prüfschritte, Verantwortlicher, finale Version

7.4 Haftung und Versicherung

Fehlerhafte KI-Ergebnisse werden im Mandatsverhältnis grundsätzlich nicht dadurch entschuldigt, dass sie technisch erzeugt wurden. Die Kanzlei muss Einsatzgrenzen, Prüfprozesse und Qualifikation so organisieren, dass vorhersehbare Fehler erkannt werden. Anbieterbedingungen enthalten häufig weitreichende Haftungsbegrenzungen; sie verlagern das Mandatsrisiko nicht automatisch auf den Anbieter.

Kanzleien sollten prüfen, ob ihre Berufshaftpflicht besondere Anzeige-, Dokumentations- oder Ausschlussregeln für KI, Softwareentwicklung, automatisierte Dienste oder eigene digitale Produkte enthält. Eine pauschale Aussage zur Deckung ist ohne konkreten Versicherungsvertrag nicht möglich.

7.5 Urheberrecht, Quellen und Geheimnisse

KI-Ausgaben können geschützte Inhalte, unklare Übernahmen oder erfundene Zitate enthalten. Für Veröffentlichungen, Schulungsunterlagen und Mandantendokumente sind Quellen, Nutzungsrechte und Eigenleistung zu prüfen. Vertrauliche Fachliteratur oder Datenbankinhalte dürfen nicht ohne Nutzungsrecht in offene Systeme hochgeladen werden.

Quellen- und Veröffentlichungscheck	
☐	Alle zitierten Fundstellen im Original geöffnet, gelesen und dem konkreten Aussagegehalt zugeordnet;
☐	wörtliche und sinngemäße Übernahmen kenntlich gemacht; Zitatumfang und Nutzungsrecht geprüft;
☐	keine lizenzierten Volltexte, Mandantenunterlagen oder internen Arbeitsergebnisse unbefugt in offene KI-Systeme geladen;
☐	Bild-, Tabellen-, Software- und Datenbankrechte sowie Anbieterbedingungen für die geplante Nutzung geprüft;
☐	KI-generierte Formulierungen auf auffällige Nähe zu fremden Texten und auf erfundene Quellen kontrolliert;
☐	finale Veröffentlichung bzw. Mandantenfassung einer verantwortlichen Person zugeordnet und versioniert.

8 Kanzleipraxis: Ampel, Anbieterprüfung und Einführung

8.1 Detaillierte Use-Case-Ampel

Anwendung	Ampel	Bedingung
Allgemeine E-Mail-Formulierung ohne Mandatsdaten	GRÜN	freigegebenes Tool, normale Sichtprüfung
Newsletter zu Gesetzesänderung aus öffentlichen Quellen	GRÜN/GELB	Primärquellen prüfen; Art. 50 nur bei öffentlichem Interesse ohne substanzielle menschliche Prüfung problematisch
Anonymisierte steuerliche Fallfrage	GRÜN/GELB	Anonymisierung belastbar prüfen; seltene Merkmale und Kontext beachten
Pseudonymisierter Fall in öffentlichem Chatbot	ROT	Pseudonymisierung entfernt Geheimnis-/Personenbezug nicht
Bescheid oder Vertrag in geprüftem Enterprise-Tool	GELB	§ 62a/§ 203/DSGVO und ggf. Einwilligung; Retention/Training/Region prüfen
Mandatsunterlage in privatem Plus-/Consumer-Konto	ROT	keine organisatorische Freigabe und regelmäßig unzureichende Vertrags-/Kontrolllage
Meeting-Bot in Mandantengespräch	GELB	vorherige Information/Einwilligung, § 201 StGB, § 62a, DSGVO, Löschung [S19]
Website-Chatbot für allgemeine Fragen	GELB	KI-Hinweis, Datenschutz, keine verbindliche Einzelfallberatung, Übergabe an Menschen
Agent darf E-Mails versenden oder Buchungen auslösen	GELB/ROT	Genehmigungsschritt, Least privilege, Logging, Limits, Test- und Rollback-Konzept
KI analysiert Bewerber und erstellt Ranking	ROT bis zur Spezialprüfung	Beschäftigtendatenschutz, AGG, Mitbestimmung, Hochrisiko-Perspektive

8.2 Anbieter-Due-Diligence

15-Punkte-Prüfung vor Freigabe eines KI-Tools	
☐	1. Juristische Vertragspartnerin, Produktname, Tarif und Versionsstand eindeutig festhalten.
☐	2. Verantwortungsrolle nach DSGVO und Vertragsarchitektur (Art. 28/26/eigene Zwecke) klären.
☐	3. Training, Feedback, Produktverbesserung und menschliche Inhaltsprüfung mit Kanzleidaten ausschließen.
☐	4. Speicher-, Inferenz-, Log-, Backup-, Moderations- und Supportorte kartieren.
☐	5. Vollständige Subprozessorenliste, Änderungsmitteilung und Widerspruchs-/Exit-Verfahren prüfen.
☐	6. §-62a-/§-203-Verpflichtung in Textform einschließlich strafrechtlicher Belehrung sicherstellen.
☐	7. Need-to-know, Rollen, privilegierte Zugriffe und Supportzugriffe vertraglich und technisch begrenzen.
☐	8. Löschfristen, Zero-Retention-Optionen, Export und nachweisbare Löschung testen.
☐	9. Verschlüsselung, MFA/SSO, RBAC, DLP, Audit-Logs, Zertifizierungen und Incident-Meldung bewerten.

15-Punkte-Prüfung vor Freigabe eines KI-Tools	
☐	10. Websuche, Connectoren, Apps, Plugins und Agentenaktionen separat prüfen.
☐	11. Drittlandtransfer und berufsrechtlichen Auslandsgeheimnisschutz getrennt dokumentieren.
☐	12. Modellwechsel, neue Funktionen, Preis-/Vertragsänderungen und Kündigungs-/Exit-Regeln regeln.
☐	13. Fachliche Eignung, Quellenfunktion, Fehlerbilder und Reproduzierbarkeit mit Testfällen evaluieren.
☐	14. Anbieterhaftung, Freistellungen, SLA und Support im Störungsfall prüfen.
☐	15. Freigabe befristen und mindestens jährlich bzw. anlassbezogen neu bewerten.

8.3 Technische Mindestkontrollen

Kontrollfeld	Mindestmaßnahme
Identität und Zugriff	betriebliche Einzelaccounts, MFA/SSO, Rollen, kein Account-Sharing, sofortiger Entzug bei Austritt
Datenbegrenzung	DLP, Upload-Limits, verbotene Datenklassen, keine Passwörter/Token, Least privilege bei Connectoren
Einstellungen	Training aus, Historie/Retention minimiert, öffentliche Links gesperrt, Apps/Plugins nur Positivliste
Agenten	kritische Aktionen genehmigungspflichtig, Sandbox/Test, Ausgaben- und Transaktionslimits, Rollback
Protokollierung	Admin- und Nutzungslogs, aber datenschutzkonforme Beschäftigtenkontrolle; Incident-Spuren
Sicherheit	Verschlüsselung, Geräteschutz, Patchmanagement, Browserkontrollen, Backup und Notfallplan

8.4 Einführung in zehn Schritten

1 KI-Inventar
Offizielle und inoffizielle Tools, Browser-Erweiterungen, Meetingbots und Fachsoftwarefunktionen erfassen.

2 Use Cases priorisieren
Drei risikoarme, messbare Fälle auswählen; keine vollautomatische Steuerentscheidung als Start.

3 Datenklassen definieren
Öffentlich, intern, pseudonymisiert, Mandatsdaten, besondere Schutzdaten.

4 Richtlinie beschließen
Positivliste, Verbote, Prüfstufen, Verantwortlichkeiten und Meldeweg.

5 Anbieter prüfen
Verträge, Datenflüsse, Sicherheit, § 62a, DSGVO, AI Act und Exit.

6 Technik konfigurieren
Accounts, MFA, Rollen, Retention, Training, Connectoren und Logging.

7 **Pilotieren**
Nur Test-/öffentliche Daten; Qualitäts- und Fehlerbilder dokumentieren.

8 **Schulen**
Rollen- und risikobasiert nach Art. 4; Teilnahme und Inhalte dokumentieren.

9 **Freigeben**
Use-Case-Prüfvermerk, gegebenenfalls Einwilligung, fachliche Kontrollmatrix.

10 **Überwachen**
Nutzung, Vorfälle, Anbieteränderungen und Nutzen regelmäßig evaluieren.

8.5 Mindestinhalt einer Kanzlei-KI-Richtlinie

Kernbausteine - an Kanzlei und Betriebsrat anpassen	
☐	Zweck und Geltungsbereich;
☐	freigegebene Tools, Tarife und Funktionen (Positivliste);
☐	verbotene private Accounts, Browser-Plugins und Datenarten;
☐	Datenklassifikation und Beispiele;
☐	Pflicht zur Anonymisierung bzw. Klarstellung, dass Pseudonymisierung nicht genügt;
☐	fachliche Prüf- und Freigabestufen;
☐	Regeln für Datei-Uploads, Websuche, Connectoren, Meeting-Aufzeichnung und Agenten;
☐	Dokumentation im KI-Register;
☐	Verhalten bei Fehlversand, Datenleck oder auffälligem KI-Ergebnis;
☐	KI-Kompetenz, Schulung und Ansprechpartner;
☐	Kontrolle mit Augenmaß und Beschäftigtendatenschutz;
☐	Änderungs- und Freigabeprozess.

Quellenhinweis: DStV-Muster-KI-Anwendungsrichtlinie vom 23.04.2026 als praxisorientierte Ausgangsbasis; kein unverändert zu übernehmender Standard. [S17]

9 Häufige Fragen

Darf ich ChatGPT, Microsoft Copilot, Claude, Gemini oder andere KI verwenden?

Ja, aber die Antwort hängt nicht nur vom Namen ab. Zu prüfen sind konkrete Produktvariante, Vertrag, Datenregion, Trainingsnutzung, Subdienstleister, Funktionen und Anwendungsfall. Ein privates Konto kann für allgemeine öffentliche Inhalte vertretbar sein, ist für Mandatsdaten aber regelmäßig nicht die freizugebende Umgebung.

Darf ich Mandantendaten in ein Business- oder Enterprise-Tool eingeben?

Nur wenn § 62a StBerG, § 203 StGB und DSGVO für die konkrete Konfiguration erfüllt sind. Business/Enterprise ist ein Indiz für bessere Kontrollen, kein automatischer Freibrief.

Brauche ich immer eine Einwilligung des Mandanten?

Nein. § 62a erlaubt allgemeine Dienstleistungen ohne Einwilligung, wenn die gesetzlichen Anforderungen erfüllt sind. Eine Einwilligung ist aber nach Abs. 5 erforderlich, wenn die Dienstleistung unmittelbar einem einzelnen Mandat dient. Bei sensibler fallbezogener KI-Analyse ist die Einordnung offen; eine konkrete Einwilligung kann konservativ sinnvoll sein.

Kann ich mir in der Mandatsvereinbarung pauschal jede KI-Nutzung genehmigen lassen?

Eine transparente Grundinformation und Einwilligung in klar benannte Kategorien kann sinnvoll sein. Ein pauschaler Blankoscheck für alle heutigen und künftigen Tools, Staaten, Daten und Zwecke ist nicht belastbar und ersetzt die Anbieterprüfung nicht.

Was ist der Unterschied zwischen Einwilligung und Verzicht nach § 62a Abs. 6?

Die Einwilligung erlaubt die mandatsbezogene Dienstleistung. Der ausdrückliche Verzicht kann Anforderungen an Auswahl und Vertrag aus Abs. 2 und 3 abbedingen. Ein Verzicht sollte nur ausnahmsweise, spezifisch und nach dokumentierter Aufklärung genutzt werden.

Löst ein Verzicht Datenschutz und § 203?

Nein. DSGVO, allgemeine Sorgfalt und die strafrechtlichen Voraussetzungen sind eigenständig. Zudem kann der Mandant nur über Geheimnisse verfügen, zu deren Offenlegung er befugt ist.

Reicht es, Namen und Steuernummer zu entfernen?

Oft nicht. Branche, Ort, Beträge, Vertragsdetails, seltene Sachverhalte, Dateimetadaten oder Kombinationen können die Re-Identifikation ermöglichen. Pseudonymisierte Daten bleiben geschützt.

Reicht ein Serverstandort in Deutschland oder der EU?

Nein. Speicherort ist nur ein Element. Inferenz, Logs, Support, Backups, Websuche, Connectoren und Subprozessoren müssen ebenfalls geprüft werden.

Muss ich jede KI-Nutzung gegenüber dem Mandanten offenlegen?

Es gibt keine allgemeine berufsrechtliche Pflicht, jede Textassistenz zu benennen. Transparenz kann aus DSGVO, Einwilligung, Mandatsgestaltung oder Art. 50 KI-VO folgen. Bei mandatsbezogener Einwilligung muss der Einsatz selbstverständlich konkret erläutert werden.

Muss jeder KI-generierte Mandantenbrief gekennzeichnet werden?

Nein. Art. 50 enthält spezifische Pflichten, keine allgemeine Kennzeichnung aller KI-Unterstützung. Ein individueller Mandantenbrief ist regelmäßig keine öffentliche Publikation; außerdem gilt für öffentliche Texte bei substanzieller menschlicher Prüfung und redaktioneller Verantwortung eine Ausnahme.

Ist normale Kanzlei-KI ein Hochrisiko-System?

Typische Text-, Recherche- oder Dokumentenassistenz ist nicht allein wegen KI hochriskant. HR-Auswahl, Leistungsüberwachung, bestimmte biometrische oder essenzielle Dienstleistungsentscheidungen können dagegen in Hochrisiko- oder Verbotsbereiche fallen.

Muss eine Datenschutz-Folgenabschätzung erstellt werden?

Nicht automatisch für jedes KI-Tool. Erforderlich ist eine Vorab-Risikoprüfung. Eine DSFA ist durchzuführen, wenn voraussichtlich ein hohes Risiko besteht, etwa bei umfangreicher sensibler Analyse, systematischer Bewertung oder entscheidungsnaher Automatisierung.

Dürfen Mitarbeitende private KI-Accounts verwenden?

Für Kanzleizwecke sollte dies grundsätzlich untersagt werden. Betriebliche Einzelaccounts mit zentralen Einstellungen, Rollen, Logging und sofortigem Entzug sind vorzuziehen.

Was gilt für Meeting-Aufzeichnungen und Transkription?

Nichtöffentliche Gespräche dürfen nicht heimlich aufgezeichnet werden. Vorab sind Beteiligte zu informieren und gegebenenfalls einzuwilligen; außerdem gelten Berufsrecht, DSGVO, Löschfristen und Anbieterprüfung. [S19]

Was gilt für mit KI erstellte Apps?

Entscheidend ist die fertige App. Wird sie lokal und deterministisch betrieben, fließen spätere Mandantendaten nicht automatisch an den Code-Assistenten. Ruft die App im Betrieb APIs, Telemetrie, Cloudspeicher oder Modelle auf, entstehen entsprechende Datenflüsse. Code, Abhängigkeiten, Berechtigungen und Netzwerkverkehr müssen technisch geprüft werden.

Muss ich programmieren können, um eine KI-erstellte App zu prüfen?

Nicht zwingend selbst auf Quellcode-Niveau, aber die Kanzlei muss eine qualifizierte technische Prüfung organisieren. Dazu gehören Architektur- und Berechtigungsprüfung, Abhängigkeits-/Schwachstellenscan, Datenfluss- und Netzwerktest, Geheimnis- und Schlüsselmanagement, Protokollierung und Abnahmetests. Verantwortung kann delegiert, aber nicht ignoriert werden.

10 Musterbausteine und Prüfvermerke

HINWEIS Muster sind Ausgangspunkte, keine fertigen Rechtsprodukte

Die folgenden Bausteine müssen an Anbieter, Produkt, Mandat, Datenfluss, Vertretungsbefugnis und Datenschutz angepasst werden. Sie sind nicht für pauschale Einholung in allen Mandaten gedacht. Bei Drittgeheimnissen, besonderen Datenkategorien, Auslandsverarbeitung oder Teilverzicht ist individuelle Prüfung erforderlich.

10.1 Muster: Mandatsbezogene Einwilligung und begrenzte Entbindung

Bezeichnung: „Einwilligung in die mandatsbezogene Einschaltung eines KI-Dienstleisters und begrenzte Entbindung von der Verschwiegenheitspflicht“

Mandant / Vertretung _____

Mandat / Vorgang _____

Anbieterin / Produkt _____

Konkreter Zweck _____

_____

Datenkategorien _____

_____

Verarbeitungsorte _____

Unterauftragnehmer _____

Speicher-/Löschfrist _____

Mustertext:

„Ich/Wir willige(n) ein, dass die Kanzlei für den oben bezeichneten Zweck die genannte KI-Dienstleisterin und die offengelegten, wirksam zur Geheimhaltung verpflichteten Unterauftragnehmer einschaltet. Die Kanzlei darf diesen Stellen diejenigen mandatsbezogenen Informationen zugänglich machen, die für den beschriebenen Zweck erforderlich sind. Insoweit entbinde(n) ich/wir die Kanzlei gegenüber den benannten Empfängern von der beruflichen Verschwiegenheitspflicht.

Die Verarbeitung ist auf den beschriebenen Zweck, die bezeichneten Datenkategorien und den erforderlichen Umfang beschränkt. Eine Nutzung der Eingaben, Dateien oder Ausgaben für allgemeines Modelltraining, Werbung oder eigene Produktverbesserungszwecke der Anbieterin ist nicht gestattet. Die Kanzlei bleibt für die fachliche Bewertung und Freigabe verantwortlich.

Mir/Uns wurden Funktionsweise, Empfänger, Verarbeitungsorte, wesentliche Risiken, Speicherfrist und eine gegebenenfalls verfügbare Alternative ohne diesen Dienst erläutert. Diese Erklärung erfasst nur Geheimnisse, über die ich/wir verfügungsbefugt bin/sind. Gesetzliche Datenschutzpflichten und Rechte betroffener Dritter bleiben unberührt. Die Einwilligung kann mit Wirkung für die Zukunft widerrufen werden; die Auswirkungen auf die weitere Mandatsbearbeitung wurden erläutert.“

Ort / Datum _____

Unterschrift(en) _____

GESTALTUNGSHINWEIS Keine versteckte Klausel

Die Erklärung sollte hervorgehoben, konkret und verständlich sein. Bei juristischen Personen sind Vertretungsbefugnis und zugleich enthaltene Individualgeheimnisse natürlicher Personen zu prüfen. Ein Widerruf macht bereits rechtmäßig erfolgte Verarbeitung nicht rückwirkend unzulässig, kann aber den weiteren Einsatz beenden.

10.2 Optionaler ausdrücklicher Teilverzicht nach § 62a Abs. 6 StBerG

AUSNAHMEINSTRUMENT Nicht als Standardklausel verwenden

§ 62a Abs. 6 erlaubt einen ausdrücklichen Verzicht auf Anforderungen aus Abs. 2 und 3. Ein solcher Verzicht kann den Schutz des Mandanten erheblich reduzieren. Er sollte nur eingesetzt werden, wenn die konkrete Abweichung notwendig, verständlich erklärt und rechtlich/technisch vertretbar ist. Ein Verzicht auf zentrale Geheimhaltungs- oder Subdienstleisterpflichten ist regelmäßig nicht zu empfehlen.

Musterüberschrift: „Ausdrücklicher, auf einzelne Anforderungen begrenzter Verzicht nach § 62a Abs. 6 StBerG“

Mandant / Mandat _____

Dienstleister / Produkt _____

Nach gesonderter Erläuterung soll - ausschließlich für die oben bezeichnete Dienstleistung - auf folgende Anforderung(en) verzichtet werden:

☐	Anforderung an die sorgfältige Auswahl des Dienstleisters nach § 62a Abs. 2 Satz 1 StBerG (regelmäßig nicht empfohlen).
☐	Anforderung an die Beendigung der Zusammenarbeit bei nicht gewährleisteter Vertragseinhaltung nach § 62a Abs. 2 Satz 2 StBerG (regelmäßig nicht empfohlen).
☐	Textform des Dienstleistervertrags nach § 62a Abs. 3 Satz 1 StBerG.
☐	Bestimmte, genau zu bezeichnende Vertragsvorgabe nach § 62a Abs. 3 Satz 2 Nr. 1 (Geheimhaltung/Belehrung - regelmäßig nicht empfohlen).
☐	Bestimmte, genau zu bezeichnende Vertragsvorgabe nach § 62a Abs. 3 Satz 2 Nr. 2 (Begrenzung der Kenntnisnahme - regelmäßig nicht empfohlen).
☐	Bestimmte, genau zu bezeichnende Vertragsvorgabe nach § 62a Abs. 3 Satz 2 Nr. 3 (weitere Dienstleister - regelmäßig nicht empfohlen).

Konkrete Abweichung _____

_____

Warum erforderlich _____

_____

Erläuterte Risiken _____

_____

Schutzmaßnahmen _____

_____

„Ich/Wir verzichte(n) ausdrücklich und ausschließlich im oben bezeichneten Umfang auf die Einhaltung der angekreuzten Anforderung(en) des § 62a Abs. 2 bzw. 3 StBerG. Mir/Uns wurde erläutert, welche Schutzwirkung die jeweilige Anforderung hat, welche konkrete Abweichung vorgesehen ist, welche Risiken daraus folgen und welche Alternative besteht.

Der Verzicht erstreckt sich nicht auf die DSGVO, das BDSG, § 203 StGB, die allgemeinen Berufspflichten, technische Sicherheitsanforderungen, Drittlandvorgaben oder Geheimnisse und Rechte Dritter. Er ist keine allgemeine Ermächtigung zur Nutzung anderer KI-Dienste, Zwecke, Datenarten oder Staaten.“

Ort / Datum _____

Unterschrift(en) _____

10.3 Muster: Use-Case-Prüfvermerk

Use Case / Prozess _____

_____

Fachlich Verantwortliche _____

Tool / Tarif / Version _____

Anbieter / Vertragspartner _____

Geplantes Startdatum _____

Entscheidungsnachweis	
☐	Datenklassen: ☐ öffentlich ☐ intern ☐ pseudonymisiert ☐ Mandatsdaten ☐ besondere Kategorien ☐ Zugangsdaten (nicht zulässig)
☐	Zweck und Erforderlichkeit der Daten dokumentiert.
☐	§ 62a Abs. 1 bis 4 erfüllt; Vertrag und Nachweise abgelegt.
☐	Einzelmandatsbezug geprüft: ☐ nein ☐ ja ☐ offen; Einwilligung: ☐ nicht nötig ☐ eingeholt.
☐	Teilverzicht nach § 62a Abs. 6: ☐ nein ☐ ja, gesondert begründet.
☐	§ 203-Offenbarungsbefugnis und weitere Mitwirkende geprüft.
☐	DSGVO-Rolle und Rechtsgrundlage dokumentiert; Art.-28-/Art.-26-Regelung vorhanden.
☐	Training / Eigenzwecke ausgeschlossen; Speicher-/Löschkonzept geprüft.
☐	Drittland- und Auslandsprüfung abgeschlossen.
☐	DSFA-Vorabprüfung: ☐ kein hohes Risiko ☐ DSFA erforderlich / durchgeführt.
☐	AI Act: Rolle, Verbot, Hochrisiko, Art. 4 und Art. 50 geprüft.
☐	Fachliche Kontrollstufe und Freigabeverantwortung festgelegt.
☐	Technische Kontrollen (MFA, Rollen, Connectoren, Logs, Limits) getestet.
☐	Mitarbeitende geschult; Richtlinie und Meldeweg bekannt.
☐	Neubewertung spätestens am: _____

Freigabe Kanzleileitung _____

Datenschutz / IT (falls nötig) _____

Anmerkungen _____

_____

_____

10.4 Muster: Kurzform für das KI-Register

Das Register erfasst die tatsächlich freigegebene Produktvariante und den konkreten Use Case. Wesentliche Versions-, Vertrags-, Funktions- oder Datenflussänderungen lösen eine Neubewertung aus.

Nr.	Tool/Tarif	Use Case	Datenklasse	Risiko/Doku	Verantwortlich	Freigabe bis
KI-01						
KI-02						
KI-03						
KI-04						
KI-05						
KI-06						
KI-07						
KI-08						
KI-09						
KI-10						
KI-11						
KI-12						
KI-13						
KI-14						
KI-15						
KI-16						
KI-17						
KI-18						

11 Quellen und weiterführende Materialien

Die Quellen wurden vorrangig aus amtlichen Normtexten, Gesetzesmaterialien, Veröffentlichungen der Bundessteuerberaterkammer, des DStV, der Datenschutzkonferenz und der Europäischen Kommission ausgewählt. Abruf- und Prüfstand: 28. Juli 2026.

S1	Steuerberatungsgesetz - § 57 Allgemeine Berufspflichten Gesetze im Internet.
S2	Steuerberatungsgesetz - § 62 Verschwiegenheit der Beschäftigten Gesetze im Internet.
S3	Steuerberatungsgesetz - § 62a Inanspruchnahme von Dienstleistungen Zentrale berufsrechtliche Dienstleister-Norm.
S4	Strafgesetzbuch - § 203 Verletzung von Privatgeheimnissen Strafrechtlicher Geheimnisschutz.
S5	Berufsordnung der Bundessteuerberaterkammer (BOStB) Insbesondere § 5 Verschwiegenheit.
S6	BT-Drs. 18/11936 - Regierungsentwurf zur Neuregelung des Schutzes von Geheimnissen Gesetzesbegründung zu Dienstleistern, Einzelmandat und Verzicht.
S7	BT-Drs. 18/12940 - Beschlussempfehlung und Bericht Verhältnis Berufsrecht/§ 203 und Auslands-Einwilligung.
S8	BStBK - FAQ: KI im steuerberatenden Berufsstand, Stand 27.01.2026 Hinweis im Dokument: Rechtsstand Juli 2025, kein Vollständigkeitsanspruch.
S9	BStBK/DStV - Hinweise für den Umgang mit personenbezogenen Daten, Stand Dezember 2025 Mit Muster-Zusatzvereinbarung zu § 62a/§ 203.
S10	Datenschutzkonferenz - Orientierungshilfe KI und Datenschutz Zweck, Rollen, Art. 28, DSFA, Privacy by Design.
S11	Datenschutz-Grundverordnung (EU) 2016/679 Insbesondere Art. 5, 6, 9, 12-14, 22, 25, 28, 30, 32, 35 und 44 ff.
S12	Bundesdatenschutzgesetz - § 38 Datenschutzbeauftragte nichtöffentlicher Stellen Relevanz bei DSFA-pflichtiger Verarbeitung.
S13	Verordnung (EU) 2024/1689 - KI-Verordnung Grundverordnung des EU AI Act.
S14	Verordnung (EU) 2026/1744 - Digital Omnibus on AI In Kraft seit 27.07.2026; Änderungen u. a. zu Art. 4 und Fristen.
S15	Europäische Kommission - AI Literacy: Questions & Answers Aktuelle Auslegung des geänderten Art. 4.
S16	Europäische Kommission - Leitlinien und FAQ zu Art. 50 Transparenz Anwendbar ab 02.08.2026; menschliche Prüfung und redaktionelle Verantwortung.
S17	DStV - Muster-KI-Anwendungsrichtlinie, 23.04.2026 Praxisorientierte Grundlage, an die Kanzlei anzupassen.
S18	EDPB Opinion 28/2024 zu Datenschutzaspekten von KI-Modellen Ergänzende europäische Datenschutzorientierung.

S19	Strafgesetzbuch - § 201 Verletzung der Vertraulichkeit des Wortes Zusätzlich relevant bei Aufzeichnung oder Transkription nichtöffentlicher Gespräche.

Hinweis zur Aktualisierung

KI-Produkte, Vertragsbedingungen und Aufsichtsleitlinien ändern sich schnell. Die Handreichung sollte insbesondere bei Änderungen des StBerG, neuen berufsgerichtlichen Entscheidungen, nationaler AI-Act-Durchführung, neuen EU-Leitlinien oder wesentlichen Anbieteränderungen aktualisiert werden.

Recherchestand zur speziell einschlägigen Rechtsprechung: In öffentlich zugänglichen Quellen wurde bis 28. Juli 2026 keine Entscheidung identifiziert, die den Einsatz generativer KI durch Steuerberater konkret an § 62a StBerG und § 203 StGB prüft.

SCHLUSSFOLGERUNG **Kontrollierte KI-Nutzung ist möglich - aber nur als Kanzleiprozess**

Die tragfähige Lösung ist weder ein generelles KI-Verbot noch ein pauschaler Mandantenverzicht. Sie besteht aus einer geeigneten technischen Umgebung, einer vollständigen Vertrags- und Datenschutzprüfung, konkreter Mandantentransparenz bei Bedarf, risikobasierter KI-Kompetenz sowie konsequenter fachlicher Kontrolle.

WEITERGABEHINWEIS **Standdatum und Disclaimer beibehalten**

Bei unveränderter Weitergabe sollten Standdatum, Quellenverweise und der Hinweis „keine verbindliche Kammerauffassung“ erhalten bleiben. Angepasste Mustertexte oder rechtliche Bewertungen sind als eigene Bearbeitung zu kennzeichnen und vor Verwendung im konkreten Mandat erneut zu prüfen.