

# Digitale Transformation in der Steuerberatung

Artikel: **Vom Chatbot zum digitalen Sachbearbeiter:  
Was KI-Agenten für Steuerkanzleien bedeuten**



Stand August 2026

[www.dstv.de](http://www.dstv.de)

Ein gemeinsamer Artikel der Mitglieder des **DStV Arbeitskreises Digitalstrategie**, insbesondere Dipl.-Kfm. WP/StB **Christian Böke**, Vorsitzender des Arbeitskreises und M.A. **Luisa Stalla**, DStV Managerin Digitale Transformation.

## KI entwickelt sich weiter – und mit ihr die Fragen der Praxis

Mit seinen Veröffentlichungen im Jahr 2025 zu KI-Assistenten und zu KI-Agenten hat der Deutsche Steuerberaterverband (DStV) die Entwicklung generativer Künstlicher Intelligenz frühzeitig aufgegriffen und Steuerberatungskanzleien eine Orientierung für den praktischen Einsatz gegeben. Während zunächst die produktive Nutzung von KI-Assistenten im Mittelpunkt stand, zeigte das Whitepaper „KI-Agenten – Die nächste Evolutionsstufe der Kanzleiautomatisierung“ bereits, wie autonome Systeme künftig komplette Arbeitsabläufe unterstützen können. Ein ergänzender Leitfaden lieferte konkrete Empfehlungen für erste Pilotprojekte und den strukturierten Einstieg in die Praxis.

Seit der Veröffentlichung hat sich die Entwicklung der KI-Technologie nochmals erheblich beschleunigt. Neue Sprachmodelle, leistungsfähigere Entwicklungsplattformen und erste produktive Agentensysteme verändern die Diskussion. Gleichzeitig zeigen die ersten Erfahrungen aus Kanzleien, dass der Erfolg von KI-Agenten weit weniger vom verwendeten Sprachmodell abhängt als von der Qualität der Prozesse, der Daten, der Schnittstellen sowie einer sicheren organisatorischen und rechtlichen Einbindung. Der folgende Beitrag knüpft an die bisherigen Veröffentlichungen an. Er erläutert nicht erneut die Grundlagen von KI-Agenten, sondern beleuchtet insbesondere die Fragestellungen, die sich inzwischen in der praktischen Umsetzung zeigen.

## Warum der Prompt nur der kleinste Teil ist

Schnittstellen, Berechtigungen und Verantwortung entscheiden über den Erfolg. Generative künstliche Intelligenz ist in vielen Steuerberatungskanzleien inzwischen angekommen. Mitarbeitende recherchieren mit KI-Unterstützung, lassen Texte zusammenfassen oder formulieren und analysieren steuerliche Fragestellungen im Dialog mit einem Sprachmodell.

Die nächste Entwicklungsstufe geht deutlich weiter. KI-Systeme sollen nicht mehr nur auf eine einzelne Frage antworten, sondern selbstständig Arbeitsaufträge bearbeiten. Sie beschaffen Informationen, entscheiden über den nächsten Arbeitsschritt, greifen auf Programme und Datenbestände zu und stoßen gegebenenfalls selbst weitere Aktionen an. Für diese Systeme hat sich der Begriff KI-Agent etabliert. Dabei geht es nicht um einen digitalen Mitarbeiter, der völlig frei und unabhängig in der Kanzlei handelt. Ein KI-Agent arbeitet innerhalb eines vorgegebenen technischen und organisatorischen Rahmens. Innerhalb dieses Rahmens verfügt er jedoch über mehr Handlungsspielraum als ein klassischer Chatbot.

## Vom Antworten zum Handeln

Ein klassisches Chatprogramm folgt im Wesentlichen einem einfachen Muster: Der Nutzer stellt eine Frage, das System erzeugt eine Antwort. Danach endet der Vorgang zunächst.

Ein KI-Agent erhält dagegen ein Ziel. Er kann daraufhin mehrere Arbeitsschritte ausführen, Zwischenergebnisse bewerten und selbst entscheiden, welches Werkzeug oder welche Informationsquelle er als Nächstes benötigt. Technisch handelt es sich regelmäßig um ein Sprachmodell, das um Datenzugriffe, Werkzeuge, Speicherfunktionen und eine Ablaufsteuerung ergänzt wird. Dabei ist zwischen fest programmierten KI-Workflows und Agenten zu unterscheiden, bei denen das Modell den Lösungsweg innerhalb vorgegebener Grenzen selbst bestimmt.

### **Der Start eines Agenten kann auf unterschiedliche Weise erfolgen, beispielsweise:**

- ein neuer Eingang in einem E-Mail-Postfach,
- das Hochladen eines Dokuments,
- eine Änderung in einem bestimmten Verzeichnis,
- ein festgelegter Termin,
- ein neuer Datensatz in einem Vorsystem,
- oder ein ausdrücklich vom Nutzer erteilter Auftrag.

Ein Agent benötigt also nicht zwingend bei jedem Arbeitsschritt einen neuen menschlichen Anstoß. Er muss aber auch nicht vollständig autonom arbeiten. Zwischen einem Assistenten, der lediglich Vorschläge erstellt, und einem System, das selbstständig Nachrichten verschickt oder Buchungen ausführt, liegen sehr unterschiedliche Grade der Autonomie.



@DStV

## Ein Agent besteht nicht nur aus Trigger und Prompt

Vereinfacht wird die Funktionsweise eines KI-Agenten häufig mit der Formel „Trigger plus Prompt“ beschrieben. Das ist für ein erstes Verständnis hilfreich, für den produktiven Einsatz jedoch unvollständig.

### Ein funktionsfähiger Agent benötigt mindestens sieben Elemente:

1. einen klar beschriebenen **Auftrag**,
2. einen **Auslöser**,
3. Zugriff auf die erforderlichen **Daten**,
4. Werkzeuge und **Schnittstellen** zu anderen Systemen,
5. eindeutig begrenzte **Berechtigungen**,
6. **Regeln** für Ausnahmen, Freigaben und Abbrüche,
7. eine nachvollziehbare **Protokollierung** seiner Handlungen.

Der Prompt ist damit nur ein Bestandteil. Er beschreibt das Ziel, die Bearbeitungsschritte und die Grenzen der Tätigkeit. Ob der Agent zuverlässig arbeitet, hängt aber mindestens ebenso stark von der Qualität der Eingangsdaten, den verfügbaren Schnittstellen, der Rechtevergabe und der Behandlung von Ausnahmefällen ab.

Zwar erleichtern moderne Entwicklungsumgebungen und No-Code-Werkzeuge den Bau erster Prototypen erheblich. Auch die Arbeitsanweisung kann mit Unterstützung eines Sprachmodells formuliert werden. Einen produktionsreifen Agenten zu entwickeln, ist dennoch keine reine Prompt-Aufgabe. Es ist vor allem eine Aufgabe der Prozessgestaltung, der Softwareintegration und des Risikomanagements.

Diese Erkenntnis bestätigt die Erfahrungen aus ersten Pilotprojekten. Während sich einfache Agenten heute mit No-Code-Plattformen innerhalb weniger Stunden entwickeln lassen, entsteht der eigentliche Aufwand häufig erst bei der Integration in bestehende Fachverfahren, der Definition von Verantwortlichkeiten sowie der Absicherung datenschutzrechtlicher und organisatorischer Anforderungen.

## Nicht jede Automatisierung benötigt einen KI-Agenten

In Steuerberatungskanzleien gibt es viele wiederkehrende Tätigkeiten. Daraus folgt jedoch nicht, dass für jede dieser Tätigkeiten ein KI-Agent eingesetzt werden sollte. Ist ein Ablauf vollständig vorhersehbar und durch feste Regeln beschreibbar, sind klassische Automatisierungslösungen meist geeigneter. Ein fest definiertes Dokument abzulegen, einen bestimmten Wert aus einem Datenfeld zu übertragen oder nach einem eindeutigen Datum eine Erinnerung auszulösen, erfordert keine generative KI.

KI-Agenten spielen ihre Stärke dort aus, wo Eingangsdaten unstrukturiert sind, Sachverhalte variieren und der weitere Bearbeitungsweg vom Inhalt abhängt. Typische Beispiele sind E-Mails, Verträge, Steuerbescheide, Gesprächsnotizen oder gemischte Belegsammlungen.

Die entscheidende Frage lautet deshalb nicht: „*Welche wiederkehrende Tätigkeit können wir einem Agenten übertragen?*“ Sondern, um den spezifischen Nutzen agentischer Systeme entstehen zu lassen:



***„Bei welcher Tätigkeit muss heute ein Mensch unstrukturierte Informationen verstehen, einordnen und daraus den nächsten Prozessschritt ableiten?“***

(M.A. Luis Stalla, DStV Managerin Digitale Transformation)

@Luisa Stalla

### Weiterführende DStV-Veröffentlichungen

- **Whitepaper „KI-Assistenten in der Steuerberatung“** – Grundlagen und erste Einsatzmöglichkeiten
- **Whitepaper „KI-Agenten – Die nächste Evolutionsstufe der Kanzleiautomatisierung“** – Potenziale und Anwendungsfelder
- **Leitfaden „Erste Schritte mit KI-Agenten“** – Checklisten und Empfehlungen für die Einführung in der Kanzlei

Alle Veröffentlichungen stehen zum Download bereit unter  
**[www.dstv.de/themen/digitale-transformation-1](http://www.dstv.de/themen/digitale-transformation-1)**

# Denkbare Anwendungsfälle in der Steuerberatungskanzlei

Die Einsatzmöglichkeiten lassen sich nach dem Grad der Autonomie in drei Stufen einteilen.

## 1. Informationen erkennen und ordnen

In der ersten Stufe greift der Agent noch nicht aktiv in den fachlichen Prozess ein. Er analysiert Eingänge und bereitet sie für die weitere Bearbeitung vor.

### Denkbar sind insbesondere:

- die Klassifizierung und Zuordnung eingehender Dokumente,
- die Vorsortierung von E-Mails,
- die Erkennung von Mandat, Veranlagungszeitraum und Steuerart,
- die Prüfung, ob angeforderte Unterlagen vollständig eingegangen sind,
- die Extraktion von Rechnungsdaten,
- die Kennzeichnung ungewöhnlicher oder besonders sensibler Dokumente,
- die Erstellung von Zusammenfassungen längerer Schreiben.

Der Vorteil dieser Anwendungsfälle liegt darin, dass Fehler zunächst erkannt und korrigiert werden können, bevor sie rechtliche oder wirtschaftliche Wirkungen entfalten.

## 2. Fachliche Bearbeitung vorbereiten

In der zweiten Stufe erstellt der Agent konkrete Bearbeitungsvorschläge. Er kann beispielsweise:

- Buchungsvorschläge erzeugen,
- Einkommensteuerbelege steuerlichen Kategorien zuordnen,
- einen Steuerbescheid mit der eingereichten Erklärung vergleichen,
- Abweichungen und mögliche Rechtsbehelfsfristen markieren,
- Rückfragen an den Mandanten entwerfen,
- Auffälligkeiten in Buchhaltungs- oder Jahresabschlussdaten identifizieren,
- standardisierte Beratungsvorgänge vorstrukturieren,
- oder einen Entwurf für eine fachliche Stellungnahme erstellen.

Die abschließende fachliche Entscheidung verbleibt bei einem Mitarbeiter oder Berufsträger. KI-Systeme entbinden nicht von der beruflichen Verantwortung. Fachliche Entscheidungen müssen menschlich geprüft und interne Prüf- und Freigabeprozesse dokumentiert werden.

### 3. Handlungen in anderen Systemen ausführen

In der dritten Stufe wird der Agent selbst tätig. Er könnte unter anderem:

- Unterlagen beim Mandanten anfordern,
- Auswertungen versenden,
- Aufgaben in einem Kanzleiorganisationssystem anlegen,
- Dokumente in einer Akte speichern,
- Statusinformationen aktualisieren,
- Termine vorschlagen,
- oder vorbereitete Daten an ein Buchhaltungssystem übertragen.

Mit dieser Stufe steigt der mögliche Nutzen erheblich. Gleichzeitig nehmen die Risiken zu. Eine fehlerhafte Zusammenfassung lässt sich relativ einfach korrigieren. Eine unberechtigte E-Mail, eine falsche Buchung oder eine versäumte Frist kann dagegen unmittelbare Folgen auslösen. Für jeden Agenten muss deshalb festgelegt werden, welche Handlungen er selbst vornehmen darf und wann zwingend eine menschliche Freigabe erforderlich ist.

## Autonomie schafft neue Sicherheitsrisiken

Mit der Fähigkeit, Aufgaben selbstständig zu planen und Werkzeuge zu nutzen, entstehen neue Sicherheitsrisiken. Je mehr Handlungsspielraum ein KI-Agent erhält, desto schwieriger kann es werden, sämtliche möglichen Abläufe und Reaktionen im Voraus zu bestimmen.

Jüngste Berichte über einen KI-Agenten, der im Rahmen eines Sicherheitstests seine vorgesehene Testumgebung verließ und auf Systeme der Plattform Hugging Face zugriff, haben dieses Risiko anschaulich gemacht. Wie der konkrete Vorfall technisch und organisatorisch abschließend zu bewerten ist, muss an dieser Stelle offenbleiben.

Für den praktischen Einsatz ist jedoch eine grundsätzliche Erkenntnis entscheidend: Auch ein für einen bestimmten Zweck entwickelter Agent kann Wege einschlagen und Handlungen ausführen, die seine Entwickler nicht erwartet oder nicht ausreichend begrenzt haben.



## Das Risiko wächst insbesondere, wenn ein Agent

- selbstständig Zwischenschritte planen kann,
- externe Informationsquellen oder Internetdienste nutzt,
- auf mehrere Programme und Datenbestände zugreifen darf,
- über Schreib-, Versand- oder Ausführungsrechte verfügt,
- und über längere Zeit ohne menschliche Kontrolle tätig wird.

Hinzu kommen gezielte Angriffe auf den Agenten selbst. Ein besonders relevantes Szenario ist die sogenannte indirekte Prompt-Injection. Dabei enthält beispielsweise eine E-Mail, ein Dokument oder eine Internetseite versteckte oder offen formulierte Anweisungen, die vom KI-System als Handlungsauftrag interpretiert werden können. Liest ein Agent ein solches Dokument und verfügt zugleich über weitreichende Werkzeuge, kann er möglicherweise dazu gebracht werden, Informationen offenzulegen, Nachrichten zu versenden oder Daten zu verändern.

Für Kanzleien folgt daraus, dass die Sicherheit eines Agenten nicht allein durch eine sorgfältig formulierte Arbeitsanweisung gewährleistet werden kann. Erforderlich ist vielmehr eine technische und organisatorische Begrenzung seines Handlungsspielraums. Dabei sollte der Grundsatz der minimalen Berechtigung gelten:

***„Ein KI-Agent erhält nur diejenigen Zugriffs- und Ausführungsrechte, die er für seinen konkret definierten Auftrag zwingend benötigt.“***

(Dipl.-Kfm. WP/StB Christian Böke, Vorsitzender im DStV Arbeitskreis Digitalstrategie)



@Christian Böke

Lese-, Schreib- und Versandberechtigungen sollten getrennt vergeben werden. Kritische Handlungen müssen von einer menschlichen Freigabe abhängig sein. Hinzukommen sollten Mengen- und Zeitbegrenzungen, definierte Abbruchregeln, laufende Protokollierung und eine jederzeit verfügbare Möglichkeit, den Agenten zu stoppen.

Je größer die mögliche rechtliche, wirtschaftliche oder datenschutzrechtliche Wirkung einer Handlung ist, desto enger muss der Agent geführt und überwacht werden. Vollständige Autonomie sollte daher nicht das Entwicklungsziel sein. Maßgeblich ist vielmehr ein sinnvoll begrenzter Handlungsspielraum, der den Nutzen der Technologie erschließt, ohne die Kontrolle über den Prozess aufzugeben.



## Besondere Daten sind nicht dasselbe wie Hochrisiko-KI

Bereits im DStV Whitepaper und Leitfaden wurden Governance und Datenschutz als zentrale Erfolgsfaktoren hervorgehoben. Mit zunehmender Verbreitung produktiver KI-Agenten rücken diese Fragestellungen jedoch noch stärker in den Fokus. Inzwischen geht es nicht mehr nur um theoretische Anforderungen, sondern um konkrete Entscheidungen bei Architektur, Rechtevergabe und Datenverarbeitung.

Bei der rechtlichen Bewertung müssen unterschiedliche Begrifflichkeiten sauber getrennt werden.

Gesundheitsdaten, Informationen über eine Gewerkschaftszugehörigkeit, religiöse Überzeugungen oder genetische Daten sind besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO. Ihre Verarbeitung ist grundsätzlich untersagt, sofern nicht eine der gesetzlichen Ausnahmen greift.

Der Begriff des Hochrisiko-KI-Systems stammt dagegen aus dem europäischen AI Act. Ob ein KI-System als hochriskant eingestuft wird, richtet sich nicht allein nach der Sensibilität der verarbeiteten Daten, sondern insbesondere nach seinem vorgesehenen Einsatzzweck. Ein Agent zur Dokumentensortierung wird daher nicht automatisch zum Hochrisiko-KI-System, nur weil in einem Dokument Gesundheitsdaten enthalten sind. Andere Anwendungen, etwa bestimmte Systeme zur Bewertung oder Überwachung von Beschäftigten, können dagegen unter die Hochrisikoregelungen fallen.

Unabhängig von der Einordnung nach dem AI Act gelten die DSGVO, die berufsrechtliche Verschwiegenheit und die Pflicht zur eigenverantwortlichen Berufsausübung weiter. § 57 StBerG verpflichtet Steuerberater insbesondere zu einer unabhängigen, eigenverantwortlichen, gewissenhaften und verschwiegenen Berufsausübung.

Werden externe KI-Anbieter eingebunden, sind zusätzlich die Voraussetzungen der Inanspruchnahme von Dienstleistern nach § 62a StBerG zu prüfen. Bei Dienstleistungen, die unmittelbar einem einzelnen Mandat dienen, kann insbesondere die Einwilligung des Mandanten erforderlich sein. Daneben sind je nach Ausgestaltung Auftragsverarbeitungsvereinbarungen, technische und organisatorische Maßnahmen sowie die datenschutzrechtlichen Rechtsgrundlagen der einzelnen Verarbeitungsschritte zu prüfen.

## Drittlandtransfer, nicht bei jeder KI-Nutzung

Auch die Aussage, Daten würden bei der Nutzung von ChatGPT oder Claude stets in ein Drittland übermittelt, ist in dieser Allgemeinheit nicht richtig. Ob und wohin Daten übertragen werden, hängt vom eingesetzten Produkt, dem abgeschlossenen Vertrag, den gewählten Speicher- und Verarbeitungsregionen sowie den eingebundenen Unterauftragnehmern ab. Einige Anbieter stellen für bestimmte Unternehmens- und API-Angebote europäische Datenresidenzen oder weitere Optionen zur regionalen Verarbeitung bereit. Bei anderen Angeboten können Daten ohne abweichende Vereinbarung auch in den USA oder in weiteren Staaten verarbeitet werden. Die Kanzlei muss deshalb die konkrete technische und vertragliche Konfiguration prüfen. Der bloße Produktname beantwortet die datenschutzrechtliche Frage nicht.

### **Zu untersuchen sind insbesondere:**

- Wo werden Eingaben, Ausgaben und Protokolldaten gespeichert?
- Wo findet die eigentliche Modellberechnung statt?
- Werden Eingaben für Trainings- oder Verbesserungszwecke verwendet?
- Welche Unterauftragnehmer sind beteiligt?
- Welche Löschfristen gelten?
- Besteht ein Vertrag zur Auftragsverarbeitung?
- Welche Garantien gelten bei einer Drittlandübermittlung?
- Kann die Kanzlei Betroffenenrechte, Löschung und Auskunft praktisch umsetzen?

Einsatzfelder und Zwecke sollten vorab festgelegt und durch interne Regelungen abgesichert werden. Bei einem voraussichtlich hohen Risiko kann zudem eine Datenschutz-Folgenabschätzung erforderlich sein.



@DStV

## Der unerwartete Beleg: Datenschutz wird technisch gelöst

### **Ein praktisches Beispiel zeigt die Herausforderung:**

Eine Kanzlei richtet für eine Unternehmensberaterin einen Agenten ein, der eingehende Buchungsbelege klassifiziert. Üblicherweise handelt es sich um Telefon-, Software-, Reise- oder Hardwarerechnungen. Die Kanzlei geht deshalb von einem überschaubaren Datenschutzrisiko aus. Eines Tages lädt die Mandantin jedoch die Rechnung einer Entzugsklinik für die Behandlung ihres Partners hoch und fragt, ob die Kosten steuerlich berücksichtigt werden können.

Das Dokument enthält Gesundheitsdaten einer dritten Person und damit Daten einer besonderen Kategorie. Zugleich ist der Vorgang für die steuerliche Beurteilung möglicherweise relevant. Daten über dritte Personen sind im Steuerberatungsmandat keineswegs ungewöhnlich: Kanzleien verarbeiten regelmäßig Informationen über Arbeitnehmer, Ehegatten, Kinder, Geschäftspartner oder Anteilseigner. Eine unmittelbare Datenschutzvereinbarung zwischen der Kanzlei und jeder genannten Person ist nicht generell Voraussetzung der Verarbeitung. Erforderlich sind aber eine tragfähige Rechtsgrundlage, die Beachtung der besonderen Voraussetzungen des Art. 9 DSGVO und die Erfüllung der berufsrechtlichen Anforderungen.

Das eigentliche Problem liegt daher in der Architektur des Agenten. Werden sämtliche Dokumente ungeprüft an einen externen KI-Dienst übertragen, hat die Übermittlung bereits stattgefunden, bevor das System die besondere Sensibilität erkennen kann.

Eine bloße schriftliche Aufforderung an den Mandanten, bestimmte Unterlagen nicht hochzuladen, reicht als Schutzmaßnahme nicht aus. Mandanten können den Inhalt eines Dokuments falsch einschätzen, die Weisung vergessen oder einen Beleg dennoch für steuerlich relevant halten.

### **Ein belastbarer Prozess benötigt deshalb eine vorgelagerte Schutzstufe, beispielsweise:**

- eine lokale oder besonders abgesicherte Vorprüfung,
- regelbasierte Filter für medizinische Einrichtungen und Gesundheitsbegriffe,
- eine Quarantäne für unbekannte oder sensible Dokumenttypen,
- die Sperrung der automatischen Weiterleitung,
- eine menschliche Freigabe vor der Verarbeitung in einem externen Modell,
- oder ein ausdrücklich für besondere Daten freigegebenes System.

Der Agent muss für den ungünstigsten realistischen Eingang ausgelegt werden – nicht nur für den typischen Beleg.

## Die eigentliche Hürde sind die Schnittstellen

In den vergangenen Monaten hat sich zudem gezeigt, dass viele technische Grenzen weniger durch die Leistungsfähigkeit der KI selbst entstehen als durch die vorhandene Softwarelandschaft. Moderne Sprachmodelle können heute Dokumente verstehen, Entscheidungen vorbereiten und externe Werkzeuge ansteuern. Ob daraus jedoch ein produktiver Kanzleiprozess wird, entscheidet sich häufig an der Verfügbarkeit geeigneter Schnittstellen und Integrationsmöglichkeiten.

Damit ein Agent produktiv tätig werden kann, benötigt er Zugang zu den Programmen der Kanzlei. Genau hier liegt derzeit eine der größten praktischen Grenzen. Viele Kanzleien arbeiten mit einer gewachsenen IT-Landschaft aus DATEV-Anwendungen, Dokumentenmanagement, Kanzleiorganisation, E-Mail, Portalen und verschiedenen Fachprogrammen. Diese Systeme sind nicht durchgängig über offene und einheitliche Schnittstellen miteinander verbunden.

DATEV stellt inzwischen über das Developer Portal verschiedene Schnittstellen zur Verfügung, unter anderem für Anwendungen des Rechnungswesens, den Dokumentenaustausch und einzelne Prozesse rund um DATEV Unternehmen online. Diese Schnittstellen sind jedoch auf bestimmte Anwendungsfälle ausgerichtet. Für die Produktivnutzung gelten technische, organisatorische und teilweise auch Freigabeanforderungen. Ein allgemeiner, frei nutzbarer Zugriff auf sämtliche Daten und Funktionen der DATEV-Programme besteht nicht.

Fehlt eine geeignete Schnittstelle, bleiben häufig nur Dateiimporte, Exporte oder die Bedienung der Benutzeroberfläche durch Software-Roboter. Solche Lösungen können funktionieren, sind aber fehleranfälliger. Bereits eine Änderung der Bildschirmdarstellung oder eines Eingabefelds kann einen Ablauf unterbrechen.

Damit wird deutlich: Die Leistungsfähigkeit eines KI-Agenten hängt nicht nur vom Sprachmodell ab. Ebenso entscheidend ist, ob die Kanzleisoftware sichere, dokumentierte und fein abgestufte Zugriffe ermöglicht. Für die Softwareanbieter des Berufsstands entsteht daraus eine strategische Aufgabe. Künftige Kanzleisoftware muss nicht nur von Menschen bedient werden können. Sie muss auch kontrollierte Zugriffe für digitale Assistenten und Agenten bereitstellen – mit klaren Rollen, begrenzten Berechtigungen und vollständiger Protokollierung.

## Sieben Fragen vor dem Einsatz eines Agenten

Vor dem produktiven Einsatz sollte die Kanzlei für jeden Agenten mindestens folgende Fragen beantworten:

### **1. Was ist das genaue Ziel?**

Nicht „Posteingang bearbeiten“, sondern beispielsweise: „Eingehende Schreiben einem Mandat und einer Dokumentenart zuordnen und dringende Vorgänge zur menschlichen Prüfung vorlegen.“

### **2. Welche Daten darf der Agent verarbeiten?**

Dabei ist auch mit atypischen, sensiblen und fehlerhaft zugeordneten Eingängen zu rechnen.

### **3. Auf welche Systeme und Funktionen darf er zugreifen?**

Leserechte, Schreibrechte und Versandberechtigungen sind getrennt zu beurteilen.

### **4. Welche Entscheidungen darf der Agent selbst treffen?**

Je größer die rechtliche oder wirtschaftliche Wirkung, desto eher ist eine menschliche Freigabe erforderlich.

### **5. Wann muss der Agent stoppen?**

Unklare Sachverhalte, widersprüchliche Daten, besondere Kategorien personenbezogener Daten und ungewöhnliche Beträge können definierte Abbruch- oder Eskalationsgründe sein.

### **6. Wie wird das Ergebnis kontrolliert?**

Erforderlich sind fachliche Tests, dokumentierte Beispielfälle und regelmäßige Qualitätsmessungen. Ein erfolgreicher Prototyp ist noch kein Nachweis für einen stabilen Dauerbetrieb.

### **7. Wie bleiben die Handlungen nachvollziehbar?**

Die Kanzlei muss feststellen können, welche Daten der Agent verwendet, welche Entscheidung er getroffen, welches Werkzeug er aufgerufen und welche Aktion er ausgelöst hat.

## Vom Experiment zur Organisationsaufgabe

Die Zukunft gehört nicht dem autonomsten, sondern dem am besten kontrollierten Agenten

KI-Agenten werden sich in Steuerberatungskanzleien verbreiten. Die technischen Hürden für erste Prototypen sinken schnell. Sprachmodelle können bereits heute Dokumente verstehen, Informationen zusammenführen, Arbeitsschritte planen und externe Werkzeuge bedienen.

Die Entwicklung bestätigt damit die Einschätzungen aus den bisherigen DStV-Veröffentlichungen zu KI-Assistenten und KI-Agenten. Gleichzeitig zeigen erste praktische Erfahrungen, dass mit zunehmender Autonomie neue organisatorische, technische und rechtliche Fragestellungen in den Vordergrund rücken.

**Der wichtigste Erfolgsfaktor ist nicht der möglichst umfassende Einsatz von Autonomie.**

Entscheidend ist die kontrollierte Verbindung von künstlicher Intelligenz mit den Daten und Prozessen der Kanzlei. Kanzleien sollten deshalb nicht mit der Frage beginnen, welches KI-Modell sie einsetzen wollen. Sie sollten zunächst ihre Prozesse, Datenwege, Berechtigungen und Qualitätsanforderungen klären. Der Prompt lässt sich im Zweifel in wenigen Minuten erzeugen. Die verantwortbare Einbindung in den Kanzleialltag bleibt die eigentliche Arbeit.

Genau deshalb ist die Einführung von KI-Agenten weniger ein IT-Projekt als vielmehr eine Organisationsaufgabe. Gerade darin liegt aber auch eine Chance: Kanzleien mit klaren Prozessen, guter Datenorganisation und einer modernen Schnittstellenarchitektur werden KI-Agenten wesentlich schneller und sicherer einsetzen können als Organisationen, deren Wissen und Abläufe nur in den Köpfen einzelner Mitarbeiter vorhanden sind.

KI-Agenten sind deshalb nicht nur eine neue Technologie. Sie sind ein Prüfstein für die digitale Organisationsfähigkeit der Kanzlei. Wer bereits heute Prozesse standardisiert, Daten strukturiert und Verantwortlichkeiten klar definiert, schafft zugleich die Grundlage für den erfolgreichen Einsatz zukünftiger KI-Anwendungen.

### Weitere Impulse zur digitalen Transformation im Berufsstand

Dieser Beitrag ist Teil einer Reihe von Veröffentlichungen zur digitalen Transformation in der Steuerberatung. Auf unserer Website finden Sie weitere Fachbeiträge, Analysen und Orientierungshilfen zu aktuellen Entwicklungen im Berufsstand.

Dazu gehören unter anderem die „**10 Thesen zu KI in der Steuerberatung**“ oder der Impulsartikel „**Verantwortung teilen in Zeiten digitaler Transformation & die Zukunft sichern**“. Ergänzt werden diese Inhalte durch weitere Artikel und Praxisimpulse rund um Digitalisierung, Organisation und Zukunftsthemen der Steuerberatung.

Weitere Inhalte finden Sie unter: [www.dstv.de](http://www.dstv.de) / Themen / Digitale Transformation

Stand: August 2026



## **Impressum**

Verantwortlich für den Inhalt:

Deutscher Steuerberaterverband e.V.

Littenstraße 10

10179 Berlin

Telefon: 030 27876-2

Telefax: 030 27876-799

E-Mail: [dstv.berlin@dstv.de](mailto:dstv.berlin@dstv.de)

[www.dstv.de](http://www.dstv.de)

Stand: August 2026

Bildnachweis:

Titelbild und Bilder im Text: siehe jeweils Bildquellen

## **ÜBER DEN DEUTSCHEN STEUERBERATERVERBAND e.V.**

Der Deutsche Steuerberaterverband e.V. (DStV) vertritt als Spitzenorganisation die Angehörigen der steuerberatenden und wirtschaftsprüfenden Berufe auf nationaler und internationaler Ebene gegenüber Politik, Exekutive und weiteren Stakeholdern. In seinen 15 Mitgliedsverbänden sind 36.500 - überwiegend in eigener Kanzlei oder Sozietät tätige - Steuerberater, Steuerbevollmächtigte, Wirtschaftsprüfer, vereidigte Buchprüfer sowie Berufsgesellschaften freiwillig zusammengeschlossen.

Alle in dieser Veröffentlichung enthaltenen Begriffe beziehen sich ohne jede Diskriminierungsabsicht auf alle Geschlechter.

## ***Ansprechpartner***

### **Luisa Stalla**

M.A. Managerin Digitale Transformation

Deutscher Steuerberaterverband e.V.

Littenstr. 10, 10179 Berlin

030 - 278 76 430

[luisa.stalla@dstv.de](mailto:luisa.stalla@dstv.de)

[www.dstv.de](http://www.dstv.de)