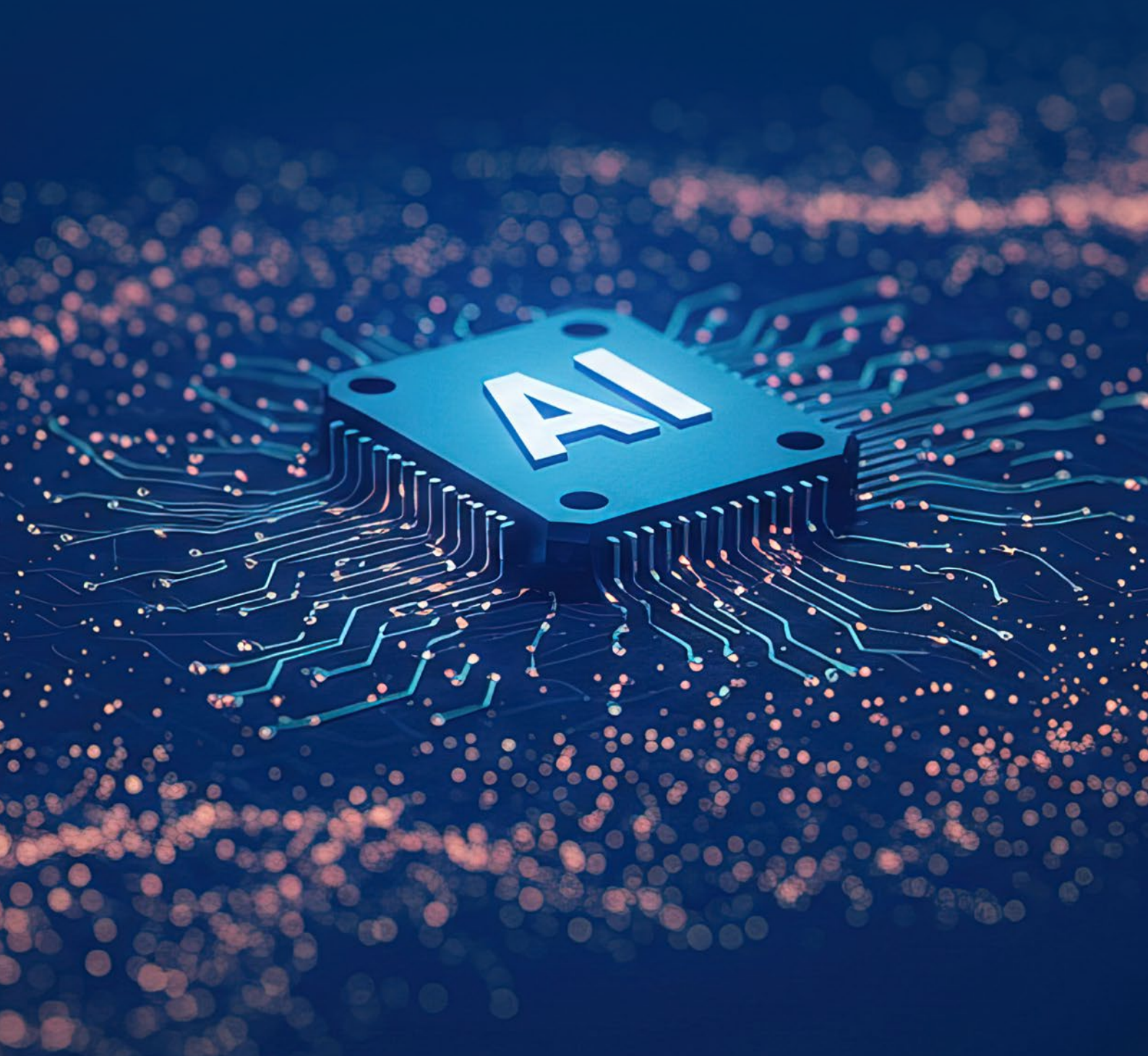


KÜNSTLICHE INTELLIGENZ (KI) IN ANWALTSKANZLEIEN



Die Österreichischen
Rechtsanwältinnen
und Rechtsanwälte

KÜNSTLICHE INTELLIGENZ (KI) IN ANWALTSKANZLEIEN

Werden KI-Systeme von der Kanzlei eingesetzt, ist sicherzustellen, dass die rechtsanwaltlichen Kernpflichten wie die Verschwiegenheit und die Einhaltung berufsrechtlicher und datenschutzrechtlicher Anforderungen gewahrt bleiben. Die Verantwortung für den Schutz sensibler Mandantendaten und die sorgfältige Prüfung der Ergebnisse bleibt auch beim Einsatz künstlicher Intelligenz uneingeschränkt bei der Rechtsanwältin und dem Rechtsanwalt. Der Einsatz von KI-Tools erfordert eine sorgfältige Auswahl des Anbieters und klare vertragliche Regelungen.

In dieser Anleitung finden sich praktische Tipps und Empfehlungen zur Sicherstellung eines rechtskonformen und sicheren Einsatzes von künstlicher Intelligenz in Ihrer Kanzlei.

1. Grundlagen der KI in der Rechtspraxis

- **Was ist KI und wie funktioniert sie?** Künstliche Intelligenz (KI) bezeichnet Systeme, die menschenähnliche Verhaltensweisen wie Lernen, Schlussfolgern und Problemlösen simulieren. In der Rechtspraxis basieren viele Werkzeuge auf maschinellem Lernen und großen Sprachmodellen (sogenannten Large Language Models, LLMs), die darauf trainiert wurden, riesige Mengen an Text- und Sprachdaten zu verarbeiten, Muster zu erkennen und Inhalte zu generieren.

- **Arten von KI-Tools für Anwaltskanzleien:** Der Einsatz von KI ist vielfältig und umfasst unter anderem:

Dokumentenanalyse und e-Discovery: Schnelles Durchsuchen und Kategorisieren großer Datenmengen (zB in Due-Diligence-Prüfungen oder Ermittlungsverfahren).

Juristische Recherche: Unterstützung bei der Suche nach relevanter Judikatur, Gesetzen und Fachliteratur durch semantisches Verständnis von Fragestellungen.

Vertragsanalyse und -erstellung: Identifizierung von Risiken, fehlenden Klauseln und Abweichungen von Standards sowie die Erstellung von Vertragsentwürfen.

Zusammenfassung und Aufbereitung: Erstellung von prägnanten Zusammenfassungen von Akten, Urteilen oder Korrespondenzen zur schnellen Einarbeitung.

Die Nutzung von KI-Systemen kann mit oder ohne Personen- bzw. Mandantenbezug erfolgen. Die Pflichten, die im Rahmen dieses Leitfadens beschrieben werden, beziehen sich primär auf die Nutzung von KI-Systemen mit Mandantenbezug.

- **Grenzen und aktuelle Herausforderungen von KI-Systemen:** Trotz der Vorteile ist Vorsicht geboten. KI-Systeme können fehlerhafte oder frei erfundene Informationen („Halluzinationen“)

generieren. Die anwaltliche Sorgfaltspflicht erfordert daher eine **ausnahmslose** Überprüfung und Verifizierung **aller** KI-generierten Ergebnisse. Zudem ist das "Wissen" vieler Modelle auf einen bestimmten Datenstand begrenzt und bildet keine tagesaktuellen Rechtsentwicklungen ab. Die Letztverantwortung für jede juristische Aussage verbleibt stets bei der Rechtsanwältin bzw. beim Rechtsanwalt.

2. Berufsrechtliche und datenschutzrechtliche Rahmenbedingungen

- **Anwaltliche Verschwiegenheit bei KI-Nutzung:** Die anwaltliche Verschwiegenheitspflicht (§ 9 Abs 2 RAO) gilt auch uneingeschränkt beim Einsatz von KI-Technologien. Die Eingabe von mandatsbezogenen oder sonstigen vertraulichen Informationen in öffentliche oder ungesicherte KI-Systeme stellt einen Bruch der Verschwiegenheit dar und ist standesrechtlich unzulässig. Die Verantwortung für den Schutz der anvertrauten Geheimnisse bleibt vollständig bei der Rechtsanwältin bzw. beim Rechtsanwalt. Die Rechtsanwältin bzw. der Rechtsanwalt müssen daher die Pflichten des § 40 Abs 3 RL-BA einhalten und dürfen nur KI-Anbieter beauftragen, die die in § 40 Abs 3 RL-BA normierten Pflichten erfüllen.

- **Welche Pflichten treffen die Rechtsanwältin bzw. den Rechtsanwalt bei der Auswahl von KI-Anbietern?** Analog zur Beauftragung externer IT-Dienstleister, müssen KI-Anbieter sorgfältig ausgewählt werden. Rechtsanwältinnen und Rechtsanwälte müssen prüfen, ob der Anbieter ausreichende technische und organisatorische Maßnahmen zum Schutz der Daten ergriffen hat und wo die Daten verarbeitet und gespeichert werden. Es ist sicherzustellen, dass die Interessen des Klienten jederzeit gewahrt bleiben. Zuletzt muss der KI-Anbieter verpflichtet werden, im Falle einer Hausdurchsuchung die Rechtsanwältin bzw. den Rechtsanwalt zu informieren. Von dieser Pflicht gibt es eine Ausnahme: KI-Anbieter, die Daten nur kurzzeitig, nicht dauerhaft für das Generieren einer Ausgabe erhalten, müssen nicht vertraglich zur Information verpflichtet werden (§ 40 Abs 3 Z 4 RL-BA). **Wichtig** ist, dass der KI-Anbieter in keinem Fall Eingaben der



Rechtsanwältin bzw des Rechtsanwalts für das Training von KI-Modellen verwenden darf, wenn in den Eingaben Rückschlüsse auf Mandanten möglich sind.

- **In welchen Fällen muss der KI-Anbieter nicht schriftlich verpflichtet werden, im Falle der Hausdurchsuchung die Rechtsanwältin bzw den Rechtsanwalt zu informieren?**

Spezialisierte KI-Anbieter (etwa in Europa ansässige Verlage oder österreichische Anbieter juristischer Software) betreiben – in der Regel – selbst keine aktuellen KI-Systeme, sondern nutzen die LLMs von großen, meist amerikanischen KI-Anbietern als „Sub-KI-Anbieter“.

Dazu speichern die *Spezialisierten KI-Anbieter* die Daten in Österreich bzw Europa und senden Teile der Daten über sogenannte Schnittstellen zur Bearbeitung an Sub-KI-Anbieter in die ganze Welt. Die Verarbeitung bei den Sub-KI-Anbietern dauern in der Regel nur wenige Sekunden, der Sub-KI-Anbieter löscht (in der Regel) die verarbeiteten Daten im Anschluss. Sofern der Sub-KI-Anbieter die übermittelten Daten **ausschließlich**

- ① kurzzeitig und nicht dauerhaft speichert und
- ② die Verarbeitung automationsunterstützt (ohne Unterstützung bzw Zugriff eines Menschen) erfolgt, ist eine Vereinbarung gem § 40 Abs 3 Z 3 RL-BA nicht notwendig.

Wichtig ist, dass die übrigen Anforderungen gem § 40 Abs 3 RL-BA auch von jedem Sub-KI-Anbieter erfüllt werden müssen. Natürlich muss der *Spezialisierte KI-Anbieter* sämtliche Anforderungen des § 40 Abs 3 RL-BA erfüllen und auch verpflichtet werden, die Rechtsanwältin bzw den Rechtsanwalt im Falle einer Hausdurchsuchung unverzüglich zu informieren.

3. Praktische Implementierung in der Kanzlei

- **Auswahl des richtigen KI-Anbieters:** Wählen Sie KI-Anbieter sorgfältig aus und bevorzugen Sie Anbieter mit Server-Standorten in der EU oder in sicheren Drittstaaten mit Angemessenheitsbeschluss (zB Schweiz, Großbritannien). Der KI-Anbieter muss bereit sein, eine Vereinbarung gem § 40 Abs 3 RL-BA abzuschließen, andernfalls nur abstrakte und anonyme Fragen (ohne Mandantenbezug) gestellt werden dürfen.

Darüber hinaus ist eine Auftragsverarbeitungsvereinbarung gem Art 28 DSGVO notwendig.

Der KI-Anbieter muss sich schriftlich verpflichten, dass eingegebene Daten nicht zum Training des KI-Modells verwendet werden dürfen und nach der Verarbeitung sicher gelöscht werden.

Bei der Einführung empfiehlt sich eine schrittweise Einführung: Definieren Sie vor der Implementierung klare Anwendungsfälle und prüfen Sie den potenziellen Nutzen für Ihre Kanzleiprozesse. Es empfiehlt sich, mit Pilotprojekten in weniger sensiblen Bereichen zu starten, um Erfahrungen zu sammeln. Führen Sie

KI-Tools schrittweise ein und evaluieren Sie deren Zuverlässigkeit und Effizienz, bevor Sie einen kanzleiweiten Einsatz in Betracht ziehen.

4. KI-Kompetenz

- **Die Nutzung von KI-Systemen ist nur zulässig**, wenn eine KI-Kompetenz der Mitarbeiterinnen und Mitarbeiter besteht.
- **Schulung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für KI-Risiken:** Führen Sie regelmäßige Schulungen für Mitarbeiterinnen und Mitarbeiter durch, um sie über die spezifischen Risiken beim Einsatz von KI aufzuklären. Sensibilisieren Sie Ihre Mitarbeiterinnen und Mitarbeiter für die Gefahren von Datenlecks, den Umgang mit vertraulichen Informationen und die Notwendigkeit, KI-generierte Inhalte kritisch zu hinterfragen.
- **Klare Richtlinien zur Nutzung von KI-Tools:** Legen Sie in einer internen Richtlinie verbindlich fest, welche KI-Anwendungen in der Kanzlei genutzt werden dürfen und für welche Zwecke. Definieren Sie eindeutig, welche Art von Daten (niemals mandatsbezogen oder personenbezogen) eingegeben werden darf und welche Anwendungsfälle strikt untersagt sind.
- **Verantwortlichkeiten für den KI-Einsatz definieren:** Definieren Sie klare Verantwortlichkeiten für den Einsatz von KI. Bestimmen Sie, wer für die Auswahl, Überprüfung und Freigabe neuer KI-Tools zuständig ist und als Ansprechperson für Fragen zur sicheren Nutzung zur Verfügung steht.
- **Umgang mit den Ergebnissen von KI-Systemen:** Etablieren Sie einen klaren Prozess, der vorschreibt, dass alle von KI-Systemen erstellten Ergebnisse einer sorgfältigen menschlichen Prüfung unterzogen werden müssen. Weisen Sie Ihre Mitarbeiterinnen und Mitarbeiter an, KI-generierte Texte, Rechtsausführungen oder Quellen niemals ungeprüft zu übernehmen. Die finale inhaltliche und juristische Verantwortung verbleibt stets bei den Berufsträgern.

5. ÖRAK-Checkliste für KI-Dienstleister

Der Österreichische Rechtsanwaltskammertag (ÖRAK) hat eine **Checkliste für KI-Dienstleister** entwickelt. Vor dem Einsatz eines KI-Dienstes muss der Anbieter die Einhaltung der in dieser Checkliste festgelegten Anforderungen **schriftlich bestätigen**. Diese Bestätigung dient als Nachweis der sorgfältigen Auswahl und stellt sicher, dass der Dienstleister die strengen standesrechtlichen Verpflichtungen zur Kenntnis genommen hat und einhält. Holen Sie diese Bestätigung unbedingt ein, bevor Sie einen KI-Dienstleister beauftragen.

CHECKLISTE FÜR KI-ANBIETER

Diese Checkliste ist vom KI-Anbieter auszufüllen bzw. der Inhalt zu bestätigen.
Hinweis: Diese Checkliste prüft nur die Mindestanforderungen. Daneben können noch weitere Pflichten bestehen.

Bestätigung der Einhaltung berufsrechtlicher Vorschriften:

Vor der Beauftragung und dem Einsatz Ihres KI-Dienstes in unserer Kanzlei benötigen wir zum Nachweis der berufsrechtlichen und datenschutzrechtlichen Verpflichtungen für Rechtsanwältinnen und Rechtsanwälte eine Bestätigung für die Einhaltung sämtlicher berufsrechtlicher Regeln. Die Bestätigung dient als Nachweis unserer sorgfältigen Auswahl.

Bitte bestätigen Sie die Einhaltung der folgenden Anforderungen:

1. Einhaltung der berufsrechtlichen und datenschutzrechtlichen Rahmenbedingungen

- Wahrung der anwaltlichen Verschwiegenheit:** Sie bestätigen, die anwaltliche Verschwiegenheitspflicht (§ 9 Abs 2 RAO) zu wahren und alle technischen sowie organisatorischen Maßnahmen zu ergreifen, um diese jederzeit sicherzustellen.
- Vereinbarung gem § 40 Abs 3 RL-BA:** Sie bestätigen, dass Sie bereit sind, eine rechtskonforme Vereinbarung gem § 40 Abs 3 der Richtlinien für die Berufsausübung (RL-BA) abzuschließen.
- Auftragsverarbeitungsvereinbarung (AVV):** Sie bestätigen, dass Sie bereit sind, eine Auftragsverarbeitungsvereinbarung gem Art 28 DSGVO abzuschließen.
- Verbot der Verwendung von Daten für Trainingszwecke:** Sie sichern zu, dass von uns eingegebene Daten unter keinen Umständen für das Training von KI-Modellen verwendet werden.
- Sichere Datenlöschung:** Sie verpflichten sich, alle von uns eingegebenen Daten nach der Beendigung der Zusammenarbeit sicher und endgültig zu löschen.

2. Datenspeicherung und -verarbeitung

- Server-Standort:** Sie bestätigen, dass die Datenverarbeitung und -speicherung auf Servern innerhalb der EU oder in einem sicheren Drittstaat mit Angemessenheitsbeschluss der EU-Kommission (zB Schweiz, Großbritannien) erfolgt.
- Umgang mit Sub-Dienstleistern:** Falls Sie Sub-Dienstleister (zB für den Betrieb von LLMs) einsetzen, bestätigen Sie, dass auch diese sämtliche relevanten Anforderungen erfüllen.
- Informationspflicht bei Hausdurchsuchungen:** Sie verpflichten sich, uns im Falle einer Hausdurchsuchung bei sich oder einem Ihrer Sub-Dienstleister unverzüglich zu informieren.
 - **Ausnahme:** Diese Verpflichtung entfällt für Ihre Sub-Dienstleister, sofern diese Daten ausschließlich kurzzeitig und nicht dauerhaft speichern und die Verarbeitung durch den Sub-Dienstleister vollständig automationsunterstützt (ohne menschlichen Zugriff) erfolgt.

3. Transparenz und Kooperation

- Nachweis technischer und organisatorischer Maßnahmen (TOMs):** Sie legen uns auf Anfrage dar, welche ausreichenden technischen und organisatorischen Maßnahmen Sie zum Schutz unserer Daten ergriffen haben.
- Sie verpflichten sich,** uns umgehend zu informieren, sollte einer der oben genannten Punkte nicht mehr zutreffen bzw die Gefahr bestehen, dass dieser nicht mehr zutrifft.

.....
Datum

.....
firmenmäßige Zeichnung