STEUER BERATER INSTITUT SACHSEN

LIVE-Online-Seminar

KI sicher nutzen: Stolpersteine und Umsetzungstipps

Dozent

Dirk Munker
Geschäftsführer Munker Privacy Consulting GmbH

Termin

DI
28
APR

Live-Online-Seminar
09.00 - 11.00 Uhr

Stand: April 2026

LIVE-Online-Seminar

KI sicher nutzen: Stolpersteine und Umsetzungstipps

Dozent

Dirk Munker
Geschäftsführer Munker Privacy Consulting GmbH

Stand: April 2026

KI sicher nutzen - Stolpersteine und Umsetzungstipps

Referenten

Dirk Munker, Dipl. Staatswissenschaftler (Univ.)

Geschäftsführer der Munker Privacy Consulting GmbH

IT-Sicherheitsbeauftragter, AI Officer
und Datenschutz-Auditor (TÜV)

Berater Cyber Risiko Check nach DIN SPEC 27076

Mehr als 20 Jahre Erfahrung in Datenschutz, IT-Sicherheit und Hinweisgebersystem:

- in Steuerkanzleien,
- in KMU
- im medizinischen Umfeld,
- im behördlichen Umfeld...

MUNKER
Privacy Consulting

Referenten

Christine Munker, Diplom-Kauffrau, MBA
Geschäftsführerin der Munker Privacy Consulting GmbH

Datenschutzbeauftragte (TÜV)
Datenschutzmanager (TÜV)

AI Specialist
Datenschutz-Manager (TÜV)
Qualitätsmanagementbeauftragte (TÜV)

Mehr als 25 Jahre Erfahrung in der Organisationsberatung von Steuerkanzleien.

MUNKER
Privacy Consulting

„Wie sicher fühlen Sie sich aktuell im Umgang mit KI-Tools im Kanzleialltag?“

MUNKER
Privacy Consulting

Wandel im Kanzleialltag

Die zunehmende Digitalisierung, Cloud- und Rechenzentrums-lösungen, Arbeit aus dem Homeoffice und der Einsatz von KI prägen den neuen Arbeitsalltag in der Kanzlei.

Gleichzeitig nehmen regulatorische Anforderungen zu, genauso wie die Gefahren durch Cyberangriffe auf die verschiedenen Systeme der Kanzlei.

- Digitalisierung
- Homeoffice
- Zunehmender Einsatz von KI
- IT-Sicherheitsrisiken und Cyberbedrohungen

MUNKER
Privacy Consulting

KI verändert den Kanzleialltag – schneller, als viele denken.

- Mandantendaten gehören zu den sensibelsten Daten überhaupt
- KI-Tools werden täglich genutzt – oft ohne klare Regeln
- Kleine Fehler können große Folgen haben: Datenschutz, IT-Sicherheit, Haftung
- Der EU AI Act macht rechtssicheren KI-Einsatz verpflichtend
- Gute Nachricht: Mit wenigen strukturierten Maßnahmen ist viel machbar

MUNKER
Privacy Consulting

Viele Kanzleien nutzen KI, aber selten strukturiert.

Typische Situationen:

- Mitarbeiter nutzen ChatGPT & Co. – aber niemand weiß „wie genau“
- Tools werden ausprobiert, bevor Datenschutz & Risiken geklärt sind
- Unterschiedliche Sicherheitsniveaus bei verschiedenen KI-Tools sind nicht bekannt
- Fehlende Dokumentation → keine Nachweisfähigkeit bei Prüfungen
- „Ich dachte, das geht schon…“ – ist kein Schutz vor Haftung

MUNKER
Privacy Consulting

Ihr Nutzen heute

- Grundlagen verstehen: wie denkt künstliche Intelligenz?
- ChatGPT & Co.: öffentliche Sprachmodelle und Cloudlösungen
- Die KI in Officelösungen: Microsoft Copilot
- KI auf Ihrem Server: Anforderungen an lokal installierte KI-Tools
- KI-Verordnung – Spielregeln und Hinweise
- Zusammenfassung und Ausblick

MUNKER
Privacy Consulting

Grundlagen verstehen:
wie denkt künstliche Intelligenz?

Künstliche Intelligenz: eine Definition

- Künstliche Intelligenz steht für die maschinelle Simulation jedes Aspekts von Lernen und anderer Fähigkeiten der menschlichen Intelligenz, wie Sprachverständnis, Abstraktion und Entwicklung von Ideen.
  (Artificial Intelligence McCarthy, 1955)

- Ein „KI-System“ ist ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können. (KI-VO, Art. 3)

MUNKER
Privacy Consulting

Erste Formen der künstlichen Intelligenz

- Touring-Test: Von Alan Turing in 1950 formuliert: Ein menschlicher Fragesteller kommuniziert über eine Tastatur und einen Bildschirm ohne Sicht- und Hörkontakt mit zwei ihm unbekannten Gesprächspartnern. Der eine Mensch, der andere Maschine. Wenn der Fragesteller nicht klar sagen kann, welcher der Gesprächspartner die Maschine ist, hat die Maschine den Test bestanden. Bis heute hat das keine Maschine geschafft.

- ELIZA – der erste Chatbot wurde zwischen 1964 und 1966 von Joseph Weizenbaum am Massachusetts Institute of Technology entwickelt. ELIZA simuliert einen Psychotherapeuten und zeigt so beispielhaft die Möglichkeiten der Kommunikation zwischen einem Menschen und einem Computer über natürliche Sprache auf.

MUNKER
Privacy Consulting

IBM Watson: der Jeopardy-Test

- Jeopardy!

  Die berühmte US-amerikanische Quizshow wurde zum ersten großen Erfolg einer KI-Lösung. IBM Watson spielte im Februar 2011 gegen Ken Jennings und Brad Rutter, die beiden besten Jeopardy-Spieler, und gewann.

- IBM Watson war die erste echte KI, die bis heute beeindruckt:
  - Sie kann verstehen.
  - Sie kann Prognosen treffen und auf deren Basis entscheiden.
  - Sie kann lernen.
  - Sie kann interagieren.

MUNKER
Privacy Consulting

Weitere Entwicklung in den letzten Jahren

- 2012: Durchbruch im Bereich der Bilderkennung

  Bereits 2015 erzielte Microsoft mit seiner Bilderkennungssoftware eine Fehlerquote von nur 3,5%. Die menschliche Fehlerquote liegt bei 5%.

- 2012: OCR-Erkennung von Handschrift

  Maschinelle Digitalisierung handschriftlicher Texte erweitert die digitale Wissensbasis signifikant.

MUNKER
Privacy Consulting

Weitere Entwicklung in den letzten Jahren

- 2014: Gesichtserkennung

  Facebook-Lösung mit einer Genauigkeit von 97%, das entspricht menschlichem Niveau. Heute erkennen diese Lösungen auch Alter oder Emotionen.

- 2018: Sprachgenerierung

  Google Duplex vereinbarte selbständig Restaurantbesuche und Friseurtermine. Die Sprache war kaum von menschlicher Sprache zu unterscheiden. Duplex wird aktuell in Google Pixel Telefonen genutzt.

MUNKER
Privacy Consulting

Aktueller Stand: was kann KI verarbeiten und erzeugen?

- Sensordaten
- Videodaten
- Bilddaten
- Audiodaten
- Text
- Verkehrsdaten
- ...

Diese Informationen können beliebig kombiniert werden, z.B. bei der Verarbeitung von Gesundheitsdaten.

MUNKER
Privacy Consulting

Der Unterschied zwischen schwacher und starker KI

- **Schwache KI:**
  Wertet vorhandene Informationen aus, muss mit einer Wissensbasis trainiert werden. Sie fokussiert sich auf die Lösung von spezifischen Anwendungsfällen (z.B. OCR-Texterkennung).

- **Starke KI = Generative KI, selbst lernende Systeme**
  Besitzt die Fähigkeit zu verallgemeinern und selbst zu lernen. Hier ist das Ziel, Maschinen zu bauen, die mindestens ein menschliches oder sogar noch höheres Intelligenzniveau erreichen, und zwar nicht nur in sehr spezifischen Einsatzbereichen, sondern für ein breites Anwendungsspektrum.

  Beispiel: AlphaZero und das japanische Brettspiel Go (AlphaGo Zero). AlphaZero erlernte Go, Schach & Shogi mit einem einzigen Algorithmus und hat sich selbst bis zur Perfektion weiterentwickelt.

MUNKER
Privacy Consulting

Wie denkt KI?

- KI denkt nicht wie ein Mensch, sie berechnet Wahrscheinlichkeiten
- Sprachmodelle (z. B. ChatGPT, Copilot)
- erhalten einen Text als Eingabe
  - sagen das wahrscheinlich nächste Wort oder den nächsten Satz voraus
  - Grundlage: riesige Mengen an Texten, aus denen Muster gelernt werden
- Kein eigenes Verständnis, keine Intuition, kein „gesunder Menschenverstand“

MUNKER
Privacy Consulting

Was bedeutet das für die Praxis?

- Stärken
  - extrem schnell beim Erkennen von Mustern
  - kann große Textmengen zusammenfassen
  - liefert kreative Vorschläge und Formulierungen
- Schwächen / Risiken
  - erfindet manchmal scheinbar plausible, aber falsche Antworten („Halluzinationen“)
  - kennt keinen rechtlichen Kontext und keine Haftung
  - übernimmt nicht automatisch die Sicht der Kanzlei oder der Berufsordnung
- Konsequenz
  - KI liefert Entwürfe und Ideen
  - der Mensch entscheidet, prüft und trägt die Verantwortung

MUNKER
Privacy Consulting

KI-Verordnung – Spielregeln und Hinweise

Rechtliche Herausforderungen

- Urheberrecht
  - Frage nach dem geistigen Eigentum bisher ungeklärt: wer hat die IP-Rechte an den trainierten Modellen?

- Qualität der Trainingsdaten
  - Jedes Modell ist so gut, wie seine Wissensbasis: hinterfragen, welcher Input vorhanden ist und auf welcher Basis beurteilt wird, um z.B. Diskriminierung von Gruppen aufgrund politischer Gesinnung etc. zu vermeiden.
  - Ist die Datenbasis öffentlich oder privat? Ist sie bekannt, einsehbar, anpassbar? Können falsche Daten gelöscht werden?

- Die Logik verstehen
  - Welcher Algorithmus liegt den Ergebnissen einer KI zu Grunde? Darf überhaupt genutzt werden, was nicht nachvollzogen werden kann?
  - Wie kommen die Entscheidung zu Stande, wie wurden die Faktoren gewichtet?

MUNKER
Privacy Consulting

Rechtliche Herausforderungen

- Auftragsverarbeitung oder gemeinsame Verantwortlichkeit?
  - Klassische Anforderungen an AV, Ausfallsicherheit etc müssen gewährleistet sein.
  - Aber: liegt überhaupt faktisch eine Verarbeitung im Auftrag vor? Aktuell stellt z.B. OpenAI einen AVV zur Verfügung und definiert sich als Auftragsverarbeiter.
  - Wenn AVV, dann auch **Verpflichtung nach § 203 StGB!**

- Die KIVO (und die DSGVO) als Wettbewerbsvorteil
  - EU könnte Vorreiter in Sachen Datensicherheit und Datenhoheit werden und die wachsenden Sorgen der Anwender damit entkräften.

MUNKER Privacy Consulting

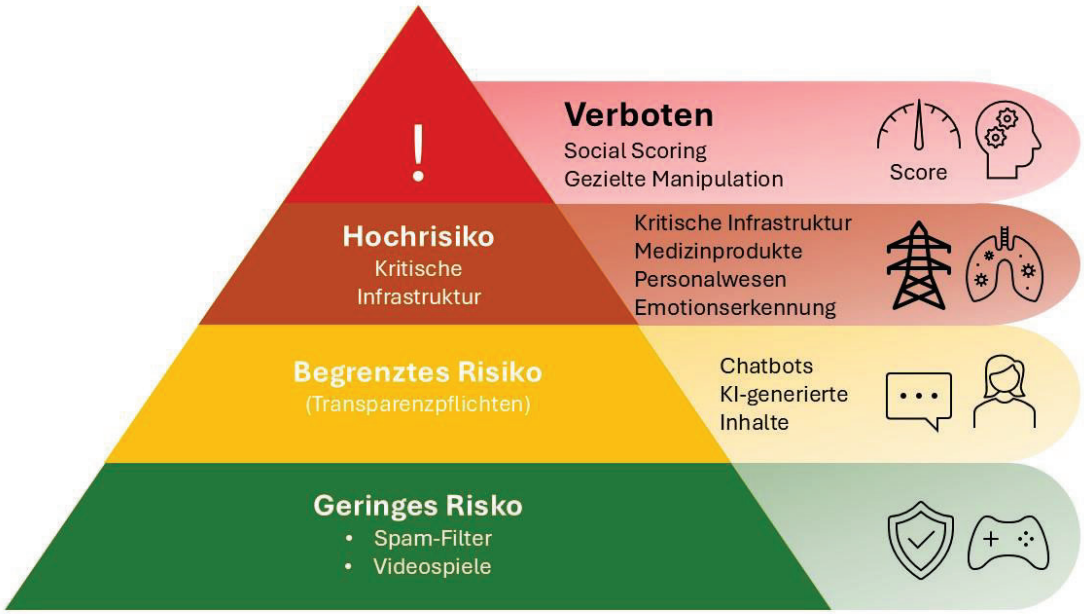
Die KI-Verordnung der EU

- Das weltweit erste KI-Gesetz wurde am 21. Mai 24 vom Rat der 27 EU Mitgliedsstaaten verabschiedet.

- Es schafft einen einheitlichen Rahmen für den Einsatz von künstlicher Intelligenz in der Europäischen Union.

MUNKER Privacy Consulting

Risiken in der KI-Verordnung der EU



MUNKER
Privacy Consulting

Artikel 5, verbotene Praktiken

- Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins, manipulative Techniken. Problem: keine geeigneten Mittel, die KI in Schach zu halten, aber ein erster regulativer Schritt.
- Techniken zur Ausnutzung der Vulnerabilität oder Schutzbedürftigkeit von Personen.
- Techniken zur Bewertung oder Einstufung von Personen auf Grundlage ihres sozialen Verhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale, die zu Schlechterstellung oder Benachteiligung führen kann.
- Techniken zur Vorhersage von Straftaten, Profiling oder Verhaltensprognose.

MUNKER
Privacy Consulting

Artikel 5, verbotene Praktiken

- Techniken zur Echtzeit-Identifikation zur Strafverfolgung auf Basis biometrischer Daten.
- Techniken zur Ableitung von Emotionen am Arbeitsplatz oder in Bildungseinrichtungen.
- Techniken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen.
- Techniken zur biometrischen Kategorisierung mit dem Zweck der Ableitung besonders sensibler personenbezogener Daten wie Rasse, Religion, sexuelle Orientierung, politische Einstellungen.

MUNKER Privacy Consulting

Artikel 6, Einstufung von Hochrisiko-KI-Systemen

Eine KI gilt als Hochrisiko-KI-System, wenn sie

- als Sicherheitsbauteil eines unter die Harmonisierungsrechtsvorschriften der Union fallenden Produkts verwendet wird oder die KI selbst ein solches Produkt ist und
- das Produkt, dessen Sicherheitsbauteil das KI-System ist oder das KI-System selbst als Produkt muss einer Konformitätsbewertung durch Dritte im Hinblick auf das Inverkehrbringen oder die Inbetriebnahme des Produkts unterzogen werden.
- ....

MUNKER Privacy Consulting

Erwägungsgrund 50

In Bezug auf KI-Systeme, die Sicherheitsbauteile von Produkten oder selbst Produkte sind, die in den Anwendungsbereich bestimmter, im Anhang dieser Verordnung aufgeführter Harmonisierungsrechtsvorschriften der Union fallen, ist es angezeigt, sie im Rahmen dieser Verordnung als hochriskant einzustufen, wenn das betreffende Produkt gemäß den einschlägigen Harmonisierungsrechtsvorschriften der Union dem Konformitätsbewertungsverfahren durch eine als Dritte auftretende Konformitätsbewertungsstelle unterzogen wird. Dabei handelt es sich insbesondere um **Produkte wie Maschinen, Spielzeuge, Aufzüge, Geräte und Schutzsysteme zur bestimmungsgemäßen Verwendung in explosionsgefährdeten Bereichen, Funkanlagen, Druckgeräte, Sportbootausrüstung, Seilbahnen, Geräte zur Verbrennung gasförmiger Brennstoffe, Medizinprodukte, In-vitro-Diagnostika, Automobile und Flugzeuge**.

MUNKER
Privacy Consulting

Die KI-Verordnung der EU und die DSGVO

- Die KI-Verordnung wurde im Mai 2024 von den Mitgliedsstaaten beschlossen
- Voraussetzung für die Verarbeitung personenbezogener Daten mit Hilfe einer KI: Die Durchführung einer Risikobewertung und ggf. einer Datenschutz-Folgenabschätzung.
- Es wird also ein Datenschutzkonzept notwendig, das beschreibt, wie die erkannten Risiken bewältigt werden sollen. Es muss erarbeitet und weiterentwickelt werden.

MUNKER
Privacy Consulting

Die KI-Verordnung der EU und die DSGVO

- Verfahren mit Einbezug der KI werden ähnlich behandelt wie alle anderen Verfahren: es gilt auch hier die DSGVO.
- Der Datenschutz verlangt bei KI-Verfahren das gleiche Datenschutzniveau wie bei allen anderen Verfahren.
- Dieses Datenschutzniveau ist beim Einsatz von KI-Lösungen aber ggf. schwerer einzuhalten und nachzuweisen, da die Systeme komplexer sind und auf Algorithmen zurückgehen, die nicht bekannt sind.
- Grundsätzliche Frage: Gibt es ein „milderes Mittel“, kann das unternehmerische Ziel auch mit weniger Risiko ohne KI erreicht werden?

MUNKER Privacy Consulting

Unterscheidung nach Art der Datenverarbeitung

- **Verarbeitung von personenbezogenen Daten**
  - Nur Daten ohne Personenbezug
  - Mandantendaten / Mitarbeiterdaten

- **Verarbeitung von sensiblen Informationen**
  - Komplexe, erfolgsrelevante Informationen (Berufsgeheimnisse)
  - Allgemeingültige Informationen, die öffentlich verfügbar sind

MUNKER Privacy Consulting

Welche Lösungen kommen in Frage und welche Regelungen sind notwendig?

Art der KI-Lösung

- Cloud-Anwendungen, große Sprachmodelle wie ChatGPT
- Installationen auf eigenen Servern mit klar überschaubarem Anwendungsumfang

Notwendige Regelungsumfang für den Einsatz der konkreten Tools

- Technische Vorgaben / Einschränkungen (z.B. Nutzerrechte)
- KI-Richtlinie mit konkreten Anweisungen

MUNKER Privacy Consulting

Grundsätzliche Überlegungen bei der Verarbeitung personenbezogener Daten

Festlegung von Zwecken:

Einsatzszenarien der KI im Vorfeld der Nutzung genau bestimmen. Nur wenn festgelegt ist, was mit der KI gemacht wird, kann auch der Zweck der Verarbeitung und die Rechtsgrundlage bestimmt werden. Diese Zwecke sind den Mitarbeitern klar vorzugeben.

Einsatz zur Verarbeitung von Mitarbeiterdaten:

Gibt es eine Rechtsgrundlage? Auf die Einwilligung sollte so gut es geht verzichtet werden, da diese im Verhältnis Arbeitgeber / Mitarbeiter immer als „zwangbehaftet“ gelten kann.

MUNKER Privacy Consulting

Grundsätzliche Überlegungen bei der Verarbeitung personenbezogener Daten

- Aufklärung über Risiken und Gefahren organisieren:
  - Das sollte Priorität haben, sowohl beim Einsatz innerhalb der Kanzlei (Personalbereich), als auch beim Einsatz zur Verarbeitung von Mandantendaten. Informieren Sie Mandanten!
- KI-Klauseln in Datenschutzverpflichtungen der Mitarbeiter:
  - Regelungen helfen, die Interessen des Arbeitgebers zu wahren, z.B. durch Hinweis auf Risiken, Regelungen zur Freigabe bestimmter Tools, Einsatz ggf. nur nach spezieller Schulung und Anleitung.
- Betriebsrat?
  - Ggf. Mitbestimmungspflicht des Betriebsrats, sofern Kontrolle der Beschäftigten, z.B. durch die Auswertung der Nutzungsintensität oder wenn Zugang zu Chatverläufen etc. möglich.

MUNKER Privacy Consulting

Voraussetzungen für den Einsatz einer KI-Lösung

- Klare interne Arbeitsanweisungen zur Auswahl von KI-Lösungen (Einsatz überhaupt möglich bzw. unter welchen Voraussetzungen).
- Festlegung der Einbindung des Datenschutzbeauftragten
- Starker Zugangsschutz, sichere Authentifizierungsmaßnahmen
- Ausschluß vertraulicher Daten als Trainingsdaten eines KI-Dienstes
- Können Vorgaben zur Zuverlässigkeit der Datenbasis und Trainingsdaten gemacht werden? (Anforderung an den Datenbestand der Kanzlei, z.B. Aktualität der Daten, Ausschluss von Testberechnungen)

MUNKER Privacy Consulting

Voraussetzungen für den Einsatz einer KI-Lösung

- Vorgaben zur Prüfung der KI-Resultate auf Richtigkeit (u.a. Halluzinationsproblem)
- Data Privacy Framework bei Datenübermittlung in Drittstaaten? Übermittlung überhaupt zulässig?
- Schulung der Mitarbeiter (Pflicht seit 02/2025)
- Erstellung einer KI-Richtlinie

MUNKER Privacy Consulting

Inhalte zur KI in der KI-Richtlinie (der Kanzlei)

Klare interne Arbeitsanweisungen zur Auswahl von KI-Lösungen (Einsatz überhaupt möglich bzw. unter welchen Voraussetzungen, wer wählt Lösungen aus, Trainingsdaten, Testbetrieb, Drittstaaten, Betroffenenrechte...).	Festlegung der Einbindung des Datenschutzbeauftragten	Verbot der privaten Nutzung betrieblicher Dienste
Regelungen zu starkem Zugangsschutz, sichere Authentifizierungsmaßnahmen	Regelungen zum Verzicht der Nutzung personenbezogener Daten (Einsatz von Anonymisierung) oder	Regelungen zur Nutzung von KI für Aufgaben mit direktem und indirektem Personenbezug.
Vorgaben zur Zuverlässigkeit der Datenbasis und Trainingsdaten (Aktualität der Daten)	Vorgaben zur Prüfung der KI-Resultate auf Richtigkeit und Rechtskonformität (insbesondere bei öffentlichen Sprachmodellen)	Vorgaben zur Sicherstellung der Durchführung von automatisierten Entscheidungen mit menschlicher Kontrolle.

MUNKER Privacy Consulting

Voraussetzungen für den Einsatz einer KI-Lösung

- Vorgaben zur Sicherstellung der Durchführung von automatisierten Entscheidungen mit menschlicher Kontrolle.
- Möglichkeit zur Erfüllung von Betroffenenrechten:
  - Auskunftsrechte, Löschbegehren (Achtung: KI kann Personenbezug herstellen, das muss in diesem Fall ausgeschlossen werden können, ggf. nur über Anzeigefilter möglich).
  - Grundsätzliche Prüfung der datenschutzrechtlichen Voraussetzungen, Thema Auftragsverarbeitung
  - Information durch den Hersteller: wie funktionieren zum Einsatz kommende Algorithmen? Wie lernt die KI?

Fazit: Zur Verarbeitung personenbezogener Daten sollte eine eigene Installation (eigene Server oder abgegrenzte Installation im Rechenzentrum) genutzt werden.

MUNKER Privacy Consulting

Verarbeitung „unkritischer“ Daten

- Wenn kein Personenbezug gegeben auch kein Datenschutzthema.
- Hier können öffentliche Sprachmodelle grundsätzlich zum Einsatz kommen.
- Bereitstellung betrieblicher Lösungen und Zugänge (keine Nutzung privater Zugänge)

MUNKER Privacy Consulting

Verarbeitung „unkritischer“ Daten

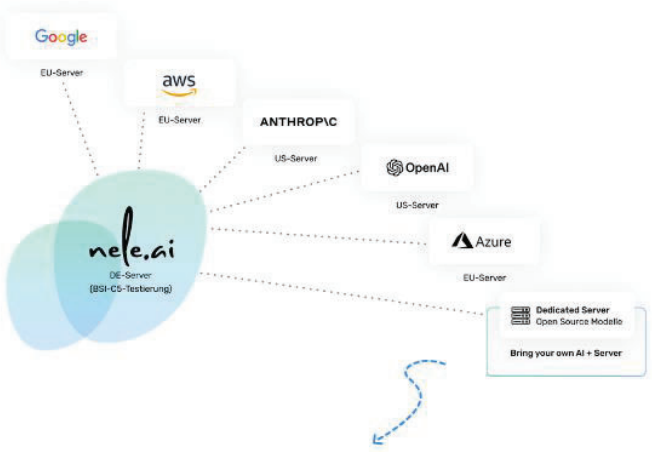
- Auch wenn Sie für Ihre Mitarbeiter Nutzerkonten z.B. für ChatGPT anlegen, werden personenbezogene Daten gespeichert (Betroffenenrechte)!
- Denken Sie diesbezüglich an Datenschutzhinweise, die Aufnahme des Verfahrens in Ihr VVT, sowie an Schutzmaßnahmen wie z.B. Kontoeinstellungen zum Datenschutz.
- KI kann u.U. Personenbezug herstellen, damit ist die Anwendbarkeit der DSGVO gegeben.
- Gerade hier Vorsicht beim Umgang mit vertraulichen Informationen bzw. Geschäftsgeheimnissen. Schaffen Sie z.B. technische Voraussetzungen, die „versehentliche Uploads“ ausschließen.

Hier hilft die Regelung der wichtigsten Nutzungsregeln in einer KI-Richtlinie und schulen, schulen, schulen!

MUNKER Privacy Consulting

Funktionsweise einer Proxy-Lösung zum Schutz der Nutzerdaten (nur als ein Beispiel…)

- Dabei werden Eingaben, Logfiles oder die Prompt-Historie nicht an die KI übermittelt.
- Daten werden vor Übermittlung an die KI an einen „datenschutzkonformen“ Server in der EU geschickt.
- Hochgeladene Informationen werden nicht in die Trainingsdaten der KI einbezogen.
- Personenbezogene Daten werden, soweit technisch möglich, pseudonymisiert an die KI geschickt und nach Antwort rückübersetzt.
- Beispiele: nele.ai, logicc.com



Quelle: https://www.nele.ai/de/ki-datenschutz

MUNKER Privacy Consulting

ChatGPT & Co.:
öffentliche Sprachmodelle und Cloudlösungen

KI in Ihrer Kanzlei: ChatGPT

- Sprachmodell von OpenAI, verfügbar im Browser und als App
- Kann Texte schreiben, korrigieren, zusammenfassen, erklären
- Einsatz für Entwürfe, Ideen, Recherchen – nicht als „fertige Rechtsquelle“
- Datenschutz: Umgang mit Mandantendaten besonders kritisch

Lizenz- und Nutzungsmodelle von ChatGPT
(Stand: April 2026)

- ChatGPT Free (kostenlos, Web/App)
  - begrenzte Funktionen, Modell/Leistung schwankend
  - Eingaben werden grundsätzlich zur Verbesserung des Dienstes genutzt, wenn man es nicht deaktiviert
  - nur für allgemeine Anfragen, nicht für sensible Kanzlei-Daten
- ChatGPT Go und ChatGPT Plus (Einzellizenz)
  - kostenpflichtig pro Person/Monat
  - Zugriff auf leistungsfähigere Modelle, zusätzliche Funktionen
  - richtet sich an einzelne Power-User
- ChatGPT Business und ChatGPT Enterprise
  - für Teams/Unternehmen, bessere Kontroll- und Verwaltungsmöglichkeiten
  - **kein Training auf Kundendaten ,** bei Enterprise: eigene Datenschutz-/Compliance-Regelungen
  - sinnvoller Ansatz, wenn eine Kanzlei ChatGPT breiter nutzen möchte

MUNKER Privacy Consulting

ChatGPT in der Steuerkanzlei – Chancen & typische Einsatzbereiche

- Formulierungshilfe für Mandantenanschreiben und E-Mails
- Entwürfe für Stellungnahmen, Gutachten, interne Notizen
- Verständliche Erklärungen komplexer steuerlicher Sachverhalte
- Erstellung von Gliederungen, Checklisten und Arbeitshilfen
- Unterstützung bei Schulungsunterlagen und Präsentationen

Entwürfe immer fachlich und rechtlich prüfen – KI ersetzt keine steuerliche Beratung!

MUNKER Privacy Consulting

Datenschutz & Risikopunkte bei ChatGPT

- Plattform von OpenAI – kein System im eigenen Kanzlei-Tenant
- Eingaben können – je nach Plan und Einstellung – zur Dienstverbesserung genutzt werden
- Mandantendaten, Personalakten, schützenswerte Daten nicht in die Standard-Versionen eingeben
- Auftragsverarbeitung / Vertragssituation prüfen (Team/Enterprise)

MUNKER Privacy Consulting

Datenschutz & Risikopunkte bei ChatGPT

- Nur für Enterprise- und API-Kunden bietet OpenAI die Möglichkeit, den Speicherort zu wählen
- Auskunftsrechte? Löschersuchen? Berufsgeheimnis?
- Interne Regeln zur Nutzung
  - welche Daten dürfen eingegeben werden?
  - wer darf ChatGPT nutzen?
  - Dokumentation der Ergebnisse im DMS

MUNKER Privacy Consulting

Vergleich zu Copilot in Microsoft 365

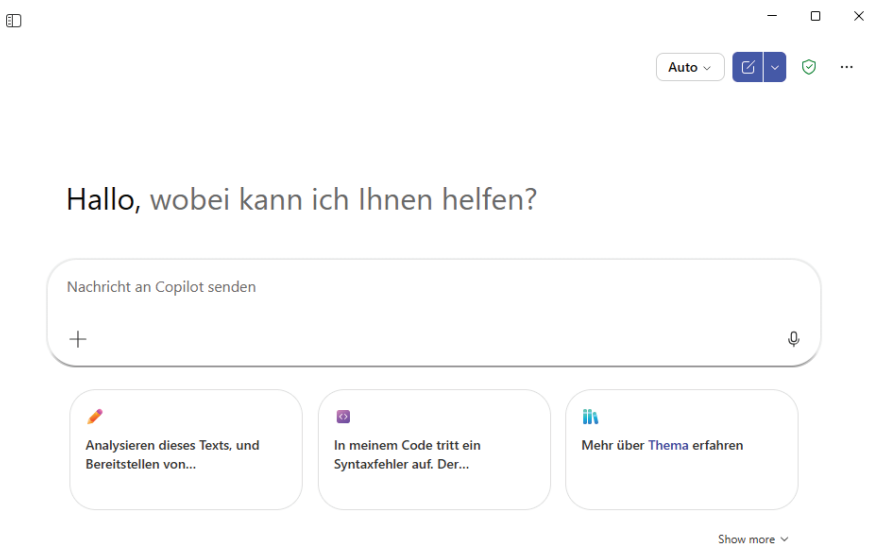
- ChatGPT
  - externer Dienst, keine direkte Integration in Ihren Kanzlei-Tenant
  - gut für allgemeine Texte, Ideen, Erklärungen
  - sensible Kanzlei-Daten nur mit strengen Vorgaben und geeigneten Verträgen

- Copilot in M365
  - arbeitet auf Ihren Daten im Microsoft-Tenant
  - respektiert bestehende Berechtigungen
  - ideal für Arbeit mit Mandantendaten, wenn Rechte sauber gepflegt sind
  - Möglichkeit zum Anschluss einer Zusatzvereinbarung zum Berufsgeheimnis

MUNKER Privacy Consulting

KI in Ihrer Office-Anwendung: Microsoft 365 Copilot

KI in Ihrer Office-Anwendung: Microsoft 365 Copilot



MUNKER Privacy Consulting

Wie funktioniert Microsoft 365 Copilot?

- Copilot ist eine eigenständige KI, die auf vorhandene öffentliche Sprachmodelle (beispielsweise GPT4) zugreift.
- Gleichzeitig hat Copilot Zugriff auf alle in Microsoft gespeicherten Informationen, auf die der aktuelle Benutzer entsprechend seiner Berechtigungen Zugriff hat (Lizenzabhängig!)
- Zur Beantwortung von Prompts nutzt Copilot beide Datenquellen gleichermaßen (Lizenzabhängig!).

MUNKER Privacy Consulting

Lizenzmodelle Microsoft 365 Copilot
(Stand April 2026)

- Kostenlose Modelle (Kritisch – nicht für Steuerberater geeignet)
  - Interaktionsdaten werden standardmäßig zum KI-Training genutzt – automatisches Opt-in!

- Copilot Chat (Eingeschränkt geeignet – abhängig vom Plan)
  - Nur bei Business/Enterprise: Daten sind durch das Data Protection Agreement geschützt – kein Training ohne Zustimmung.
  - Achtung: Zusätzliche Verschwiegenheitsverpflichtungen für Berufsgeheimnisträger abschließen!
  - Je nach Lizenzmodell: Keine Mandantendaten, Steuernummern oder personenbezogene Informationen in Prompts eingeben!

- Copilot (Business / Enterprise mit vertraglicher Absicherung)
  - Unterliegt dem Data Protection Agreement → DSGVO-Konformität wird unterstützt .
  - Kein Training mit Kundendaten ohne explizite Genehmigung.
  - Zentrale Verwaltung & Richtlinien ermöglichen Kontrolle über Datenweitergabe .

MUNKER Privacy Consulting

Auf welche Daten greift Microsoft 365 Copilot zu?

- Auf alle personenbezogenen Daten sowie sonstige Informationen, die in der Microsoft 365 Umgebung (Word, Excel, PowerPoint, Outlook, etc.) vorhanden sind.

- Die betroffenen Personen sind neben den Beschäftigten auch beispielsweise Kunden, Lieferanten, Interessenten, etc., je nachdem, wie der Verantwortliche die Microsoft 365 Umgebung nutzt.

- **Die Benutzerrechte werden zur Sicherheitszentrale für Copilot.**

- Sehr sensible Daten automatisch im Zugriff, je nach Berechtigung des Users.
  - Gefahr der Veröffentlichung sensibler und personenbezogener Daten!

MUNKER Privacy Consulting

Anmerkungen zu Microsoft 365 Copilot

- Copilot kann schnell selbst sensible Dokumente erzeugen, die geschützt werden müssen.
- Keine Transparenz: wie genau die Algorithmen auf die Daten zugreifen und was ausgewertet wird, ist nicht bekannt.
- Copilot bezieht Informationen aus OpenAI ein: sind diese immer richtig?
- Daten werden nicht in die Trainingsdaten von Microsoft selbst oder OpenAI einbezogen.
- Copilot kann nur auf abgegrenzte Daten zugreifen, der Zugriff auf Informationen eingeladener Gäste beispielsweise ist nicht möglich.

MUNKER
Privacy Consulting

KI auf Ihrem Server:
Anforderungen an lokal installierte KI-Tools

Voraussetzung für den Betrieb einer „internen“ KI

Was meinen wir mit „interner“ oder „lokaler“ KI?

Lokale Installation einer KI oder Cloudlösung auf einem dedizierten Server mit einer eigenen und jederzeit löschbaren Installation. Diese kann ggf. mit Hilfe einer Maskierung (Pseudonymisierung) auf ein LLM zugreifen um ergänzende Informationen zu erhalten.

- Einsatzzwecke definiert?
- Berufsrecht im Blick?
- Hausaufgaben IT-Sicherheit erledigt?
- Hausaufgaben Datenschutz erledigt?

MUNKER
Privacy Consulting

Voraussetzung für den Betrieb einer „internen“ KI

- Welche Daten werden verarbeitet?
- Unbedingt unterscheiden zwischen:
  - internen „harmlosen“ Texten (Vorlagen, QM-Handbuch, interne Arbeitshinweise)
  - Personenbezogene Daten (Mitarbeiterdaten wie Einkommen, Ausbildung, Gesundheitsdaten etc.)
  - Daten, die der beruflichen Verschwiegenheit nach § 203 StGB unterliegen
- Es ist oft sinnvoll, zwei Stufen vorzusehen
  - ein Sprachmodell wie z. B. ChatGPT Nur für Recherchezwecke und zur Erzeugung von Text- oder Bilddateien
  - und ein streng abgesichertes, ggf. eingeschränktes System für mandatsbezogene Inhalte
  - Alternative: Microsoft 365 Copilot mit entsprechendem Lizenzmodell

MUNKER
Privacy Consulting

Schutzziele der Informationssicherheit

- Vertraulichkeit:
  - Nur Berechtigte sehen die Daten
- Integrität:
  - Daten sind vollständig und unverändert
- Verfügbarkeit:
  - Systeme und Daten stehen rechtzeitig zur Verfügung
- Alle drei Schutzziele sind für Steuerkanzleien kritisch

MUNKER
Privacy Consulting

Typische Bedrohungen für Steuerkanzleien

- Phishing / CEO-Fraud:
  - Gefälschte Zahlungsanweisungen, gefälschte „Finanzamt“-Mails
- Ransomware:
  - Einschleusen über Anhänge, Makros oder manipulierte Websites
- Kompromittierte Fernzugänge:
  - Offene RDP-Ports, unsichere VPN-Zugänge
- Datenabfluss (Data Breach):
  - Fehlkonfigurierte Cloud-Dienste, Schatten-IT
- Fehlende Updates / Fehlkonfigurationen

MUNKER
Privacy Consulting

IT-Sicherheit ist mehr als Technik

- Mensch:
  - Fehlklicks, Social Engineering, schwache Passwörter
- Organisation:
  - Unklare Zuständigkeiten, fehlende Prozesse und Richtlinien
- Technik:
  - Fehlende oder falsch konfigurierte Schutzmechanismen
- Fazit:
  - IT-Sicherheit = Technik + Organisation + Menschen

MUNKER
Privacy Consulting

Datenschutz vs. Informationssicherheit

- Datenschutz:
  - Schutz personenbezogener Daten (Mandanten, Mitarbeiter)
  - Vorgaben der DSGVO, BDSG
- Informationssicherheit:
  - Schutz ALLER Informationen (Mandatsstrategien, Honorare, interne Abläufe)
- Überschneidung:
  - Gute Informationssicherheit ist auch Voraussetzung für Datenschutz-Compliance

MUNKER
Privacy Consulting

Rechtlicher Rahmen für Steuerkanzleien

- DSGVO:
  - Art. 5, 24, 25, 32 – Rechenschaftspflicht, „angemessene TOMs“
- GoBD:
  - Ordnungsmäßigkeit, Nachvollziehbarkeit, Unveränderbarkeit, Verfügbarkeit
- Berufsrecht:
  - Verschwiegenheitspflicht
  - Organisation der Kanzlei
  - Hinweise des berufsrechtlichen Handbuchs („Umgang mit personenbezogenen Daten“)
- Quintessenz:
  - IT-Sicherheit ist rechtliche Pflicht, keine freiwillige Kür

MUNKER
Privacy Consulting

Besonderheiten einer lokal installierten KI

- Achtung: Whitelabeling vermeiden -> Es besteht die Gefahr des Rollenwechels (Betreiber -> Anbieter)
- KI-Richtlinie
- Nutzungsanweisung
- Schulung der Mitarbeiter

MUNKER
Privacy Consulting

Systemarchitektur einer lokal installierten KI

- Trennung von Netzen (Stichwort: Maskierung):
  - Idealerweise Segmentierung: LLM-Server in einem eigenen Netzwerksegment, zugänglich nur über definierte Schnittstellen/VPN.
- Kein unkontrollierter Internetzugang:
  - Falls das LLM überhaupt ins Internet darf, dann nur über einen Proxy mit strikten Regeln (keine Weitergabe von Inhaltsdaten).
- Protokollierung:
  - Zugriffe (wer nutzt das System, wann), aber ohne unnötige inhaltliche Protokollierung von sensiblen Prompts/Outputs.
  - Wenn Protokollierung der Eingaben notwendig ist (z.B. für Nachvollziehbarkeit): Speicherfristen streng begrenzen, Zugriff stark beschränken.

MUNKER
Privacy Consulting

Datenhaltung & Modelle einer lokal installierten KI

- Wo liegen:
  - das Modell (Weights),
  - die Indexe/Vektordatenbanken (bei Retrieval-Augmented Generation (RAG), z.B. Einlesen Ihrer Dokumente),
  - etwaige Trainings-/Fine-Tuning-Daten?
- Grundregel:
  - alles auf Kanzlei-eigener Infrastruktur oder in einem datenschutzkonformen, vertraglich klar geregelten Rechenzentrum.
- Encryption:
  - Plattenverschlüsselung für Server/Notebooks.
  - Verschlüsselte Backups, strenge Backup-Zugriffsrechte.
- Löschkonzept:
  - Wie werden Trainingsdaten, Logs, Zwischenspeicher und Vektordaten im Einklang mit Aufbewahrungs- und Löschfristen behandelt?
- Zugriff & Authentifizierung
  - Nur personalisierte Zugänge, keine „Shared Accounts“.
  - Starke Authentifizierung (mindestens sichere Passwörter, besser MFA).
  - Rollen: z.B. Admin (IT), Fachverantwortliche, normale Anwender.

MUNKER
Privacy Consulting

Umgang mit Trainingsdaten, Fine-Tuning & Wissenseinbindung einer lokal installierten KI

- Kein „unbewusstes“ Training auf Mandantendaten.
  - Das LLM sollte nicht automatisch aus jeder Eingabe dazulernen.
  - Fine-Tuning oder RAG mit Mandantendaten nur, wenn:
    - Zweck klar definiert,
    - Risiko bewertet,
    - Zugriff sauber beschränkt.
- Vorzugsweise RAG statt klassischem Training:
  - Mandatsdaten bleiben in einem berechtigungsgeschützten Dokumentensystem.
    Das LLM greift kontextbezogen lesend darauf zu (z.B. über Vektordatenbank), ohne daraus ein neues allgemeines Modell zu „backen“.
- Pseudonymisierung/Anonymisierung:
  - Wo immer möglich, mandatsbezogene Daten pseudonymisieren oder anonymisieren, bevor sie in KI-Prozessen „breiter“ genutzt werden (z.B. für Wissensaufbau, Standardformulierungen, Statistiken).
- Testbetrieb:
  - Testphase nur mit künstlichen oder anonymisierten Daten.
  - Erst nach erfolgreicher Test- und Risikoanalyse produktiver Einsatz mit Realmandaten.

MUNKER
Privacy Consulting

Governance, Verantwortlichkeiten & Dokumentation einer lokal installierten KI

- Verantwortlichkeit
  - Benennen Sie intern einen fachlich Verantwortlichen (z.B. Partner/Partnerin) und einen technischen Verantwortlichen (IT/Externer Dienstleister).
- Datenschutz-Folgenabschätzung (DSFA)
  - In vielen Steuerkanzleien ist eine DSFA zumindest wahrscheinlich erforderlich, wenn:
    - systematisch und umfangreich sensible personenbezogene Daten verarbeitet werden (Gesundheit, Strafrechtliches etc.),
    - Profilbildung möglich ist.
  - Zumindest eine strukturierte Schwellwertanalyse (Vertraulichkeit, Integrität, Verfügbarkeit, Missbrauchsszenarien) ist Pflicht.
- Monitoring: Regelmäßige Überprüfung der Funktionsweise, Fehlerraten, Sicherheits- und Datenschutzvorfälle.
  - Anpassung der Regeln bei neuen Erkenntnissen

MUNKER
Privacy Consulting

Auswahl der Lösung / des Anbieters

- Selbst wenn eine KI auf dem eigenen Server betrieben wird, gibt es fast immer externe Komponenten (Support, Updates, evtl. Remotezugriff des Dienstleisters):
- Verträge:
  - Auftragsverarbeitungsverträge (Art. 28 DSGVO) mit allen Dienstleistern, die Zugriff auf Systeme/Daten haben könnten (z.B. IT-Betreuer, Hoster, Wartungsdienstleister).
- Hersteller-/Projektwahl:
  - Prüfen Sie: Kann der Anbieter den Betrieb komplett ohne Übermittlung von Mandantendaten nach außen sicherstellen?
  - Gibt es Optionen, um Telemetrie, Cloud-Features, Usage-Analytics komplett abzuschalten?
- Zertifizierungen:
  - ISO 27001 oder gleichwertige Nachweise bei Rechenzentrums- oder Managed-Service-Betreibern sind ein Plus.

MUNKER Privacy Consulting

Fazit zum Einsatz einer “internen” KI

- Einsatz klar begrenzen
  - Definieren, wofür das LLM genutzt wird (Formulierungshilfe, interne Recherchen) und wofür ausdrücklich nicht.
  - Mandatsbezogene Daten nur sehr bewusst und möglichst minimiert einsetzen – idealerweise zuerst nur mit internen, nicht-sensiblen Kanzleidaten starten.
- Steuergeheimnis & DSGVO absichern
  - Keine Daten dürfen „nach außen“ fließen (Cloud, Telemetrie, externe Logs).
  - Transparenz gegenüber Mandanten herstellen (Datenschutzhinweise ergänzen).
  - Im Zweifel DSFA/Risikoanalyse durchführen.
- Erfordernis eines Vertrages zur Auftragsverarbeitung (AVV) checken (Wartung, Service durch Externe)
  - Falls AVV, dann zwingend auch Verpflichtung nach § 203 StGB!

MUNKER Privacy Consulting

Fazit zum Einsatz einer “internen” KI

- Technische Sicherheit auf hohem Niveau
  - LLM-Server segmentiert, Zugriff nur für Berechtigte, starke Authentifizierung.
  - Verschlüsselung, geregelte Backups, Logging nur so viel wie nötig.
- Kein unkontrolliertes Training mit Mandantendaten
  - LLM darf nicht automatisch aus allen Eingaben lernen.
  - Besser: gezielte Wissenseinbindung (RAG) mit Berechtigungskonzept und kurzen Speicherfristen.
- Klare Regeln & Schulung für Mitarbeitende
  - Schriftliche Richtlinie: welche Daten dürfen eingegeben werden, wie sind Antworten zu prüfen (immer fachlicher Review).
  - Verantwortliche benennen (fachlich + technisch) und den Einsatz regelmäßig überprüfen.
- Kosten/Nutzen-Abwägung vornehmen

MUNKER Privacy Consulting

Zusammenfassung und Ausblick

Empfehlungen und Ausblick

Frühzeitig einsteigen: Erfahrungen sammeln, beraten lassen

Mitarbeiter frühzeitig mit Ausbildungs- und Trainingsmaßnahmen vorbereiten (Motivationsfaktor)

Dokumentieren Sie: wer schreibt, der bleibt.

Zur Erfüllung der datenschutzrechtlichen Rechenschafts- und Nachweispflichten müssen Sie später dokumentieren können, welche Überlegungen Sie zum Einsatz der Lösungen angestellt haben und warum Sie zum entsprechenden Ergebnis gekommen sind.

Denken Sie an die gesetzliche Pflicht zur Durchführung von KI-Schulungen nach Art. 4 der EU-Verordnung über Künstliche Intelligenz

MUNKER Privacy Consulting

Unsere Lösung – Munker Privacy Consulting GmbH

kanzlei.protect

Sicherheit für smarte Kanzleien

KI: compliant

KI mit Köpfchen braucht klare Leitplanken. Wir setzen bestehende Vorgaben um und gestalten die KI-Welt Ihrer Kanzlei compliant und kontrollierbar.

Systeme: sicher

IT-Sicherheit ist kein Zukunftsthema mehr. Wir schaffen eine zuverlässige Systemlandschaft und schützen so die Handlungsfähigkeit Ihrer Kanzlei.

DSGVO: geprüft

Es geht um den Menschen hinter den Bytes: wir organisieren einen vertrauensstiftenden und rechtskonformen Umgang mit Ihnen anvertrauten persönlichen Daten.

MUNKER Privacy Consulting

Jetzt vernetzen und in Kontakt bleiben

LinkedIn:

Christine Munker
Geschäftsführerin
Munker Privacy Consulting GmbH

Dirk Munker
Geschäftsführer
Munker Privacy Consulting GmbH

MUNKER
Privacy Consulting

KI sicher nutzen - Stolpersteine und Umsetzungstipps

Fragen?

SIS Steuerberaterinstitut Sachsen GmbH
Bertolt-Brecht-Allee 22
01309 Dresden
T. 0351 2130020 · F. 0351 2130022
info@sis-institut.de
www.sis-institut.de