



Initiativ-Stellungnahme

des Deutschen Anwaltvereins vorbereitet durch
die Ausschüsse Berufsrecht und
Informationsrecht unter Mitwirkung des
Forums für Wirtschaftskanzleien im DAV

zum Einsatz von KI in der Anwaltschaft

Stellungnahme Nr.: 32/2025

Berlin, im Juli 2025

Entsandte Berichterstatter des Arbeitskreises „KI und Anwaltschaft“ des Forums für Wirtschaftskanzleien im DAV

- Rechtsanwältin Dr. Barbara Deilmann, Düsseldorf (Sprecherin)
- Rechtsanwalt Dr. Alexander Schwarz, Düsseldorf (Sprecher)
- Rechtsanwältin Dr. Alla Drößler, Düsseldorf
- Rechtsanwalt Dr. Cornelius Böllhoff, Berlin
- Rechtsanwalt Prof. Dr. Thomas Gasteyer, Frankfurt a.M.
- Rechtsanwalt Prof. Niko Härtig, Berlin
- Rechtsanwalt Dr. Robert Heine, Berlin
- Rechtsanwalt Fabian Reinholtz, Berlin
- Rechtsanwältin Isabelle van Sambeck, Düsseldorf
- Rechtsanwältin Alina Wiegand, Düsseldorf
- Rechtsanwältin Sabine Wildfeuer, Berlin
- Rechtsanwalt Daniel Wulle, München

Mitglieder des Ausschusses Berufsrecht

- Rechtsanwalt Prof. Dr. Thomas Gasteyer, Frankfurt a.M. (Vorsitzender)
- Rechtsanwalt Dr. Peter Bachmann, München
- Rechtsanwalt Dr. Jürgen Christoph, Ratzeburg
- Rechtsanwalt Prof. Dr. Wolfgang Ewer, Kiel
- Rechtsanwalt Dr. Joachim Frhr. von Falkenhausen, Hamburg
- Rechtsanwältin Dr. Clarissa Freundorfer, Berlin
- Rechtsanwältin und Notarin Silvia C. Groppler, Berlin
- Rechtsanwalt Markus Hartung, Berlin
- Rechtsanwalt Markus Hauptmann, Frankfurt
- Rechtsanwältin Claudia Leicht, Hamburg
- Rechtsanwältin Ruth Nobel, Bochum
- Rechtsanwalt und Notar Eghard Teichmann, Achim
- Rechtsanwalt Prof. Dr. Dirk Uwer, Düsseldorf
- Rechtsanwalt (BGH) Dr. Peter Wessels, Karlsruhe

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

Mitglieder des Ausschusses Informationsrecht

- Rechtsanwalt Prof Niko Härtig, Berlin (Vorsitzender)
- Rechtsanwalt Dr. Simon Assion, Frankfurt a.M. Main
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Prof. Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwalt Dr. Helmut Redecker, Bonn
- Rechtsanwältin Dr. Kristina Schreiber, Köln
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Christine Martin, Geschäftsführerin, Berlin
- Rechtsanwältin Nicole Narewski, Geschäftsführerin, Berlin

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt ca. 60.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

Glossar

I.	Einleitung	3
II.	Executive Summary	4
III.	Use Cases & Chancen des KI-Einsatzes	6
IV.	Aspekte des Berufsrechts	8
V.	Aspekte des Datenschutzrechts	17
VI.	KI-VO	19
VII.	Urheberrecht	21
VIII.	§ 23 GeschGehSchG	22
IX.	Fazit	22

I. Einleitung

Künstliche Intelligenz ("KI") hält insbesondere in ihrer Ausprägung als generative KI ("GKI") verstärkt Einzug in die anwaltliche Praxis. GKI kann mithilfe maschineller Lernverfahren neue, originäre Inhalte wie Texte, Bilder, Audio und Programmcodes erstellen. Bekannte Anwendungen der GKI sind große Sprachmodelle (Large Language Models) wie ChatGPT und Claude oder Bildgeneratoren wie DALL-E.¹

Richtig eingesetzt, wickelt KI Routineaufgaben in Kanzleien ab und kann die rechtliche Analyse und Formulierung von Texten unterstützen, während die abschließende Bewertung, kreative Argumentation und Verantwortung weiterhin den Rechtsanwältinnen und Rechtsanwälten vorbehalten bleibt. Die Fähigkeit der

¹ Technisch unterscheidet sich generative KI von einem wesentlichen Teil herkömmlicher (traditioneller) KI dadurch, dass letztere primär vorhandene Daten nach festen Regeln oder Mustern analysiert und darauf basierende Entscheidungen oder Klassifikationen trifft, während generative KI neue Inhalte aus Mustern der Trainingsdaten erzeugen kann (die auch inhaltlich unzutreffend sein können (sogenanntes „Halluzinieren“)), wohingegen herkömmliche KI oft regelbasierte oder eng begrenzte Systeme umfasst, die auf vordefinierte Aufgaben spezialisiert sind (etwa automatisierte Datenanalysen oder Entscheidungsbäume).

GKI, eigenständig Inhalte zu produzieren, stellt einen bedeutenden Fortschritt dar und eröffnet in kurzer Zeit vielfältige neue Anwendungsmöglichkeiten – auch für die Anwaltschaft. Wer wettbewerbsfähig bleiben will, kommt auch im Anwaltsberuf nicht um die KI-Nutzung herum. Da sowohl korporative als auch individuelle Mandanten zunehmend selbst KI nutzen, erwarten sie von ihren Rechtsanwältinnen und Rechtsanwälten ebenfalls einen kompetenten Einsatz von KI-Technologien.

Dieses Papier bietet einen Überblick über die wesentlichen Aspekte des Einsatzes der KI in der anwaltlichen Praxis. Es fasst die wichtigsten Anwendungsfelder und Chancen (siehe hierzu unter III.) sowie die zentralen Herausforderungen des Einsatzes von KI-Systemen zusammen. Im Mittelpunkt stehen dabei die berufsrechtlichen Anforderungen (siehe hierzu unter IV.), insbesondere die gewissenhafte Berufsausübung sowie die Wahrung der anwaltlichen Verschwiegenheit und die datenschutzrechtlichen Vorgaben (siehe hierzu unter V.). Nicht ausgeräumte rechtliche Vorbehalte gegen die Cloud-Nutzung in der Anwaltschaft werden dabei in bekannter oder neuer Form sichtbar und werden von den Verfassern diskutiert und widerlegt. Behandelt wird auch die Frage, inwieweit der neue Rechtsrahmen für die Nutzung von KI, die EU-KI-Verordnung (Regulation (EU) 2024/1689), auch AI-Act genannt, für anwaltstypische Nutzung von KI-Systemen² praktisch relevant ist (siehe hierzu unter VI.) und welche urheberrechtlichen (siehe hierzu unter VII.) Punkte zu beachten sind.

Das Papier geht dabei auf die wesentlichen Themen ein, erhebt jedoch keinen Anspruch auf eine abschließende Darstellung aller rechtlichen Fragen im Zusammenhang mit dem Einsatz von KI. Vielmehr soll das Papier einen Überblick über die wichtigsten Eckpunkte geben, die es beim Einsatz von KI in der Anwaltschaft zu beachten gilt, zur Klärung der häufig diskutierten Fragen beitragen und die weitere Diskussion anregen. Ziel ist es, Rechtsanwältinnen und Rechtsanwälten eine praxisnahe Orientierungshilfe für den sicheren, verantwortungsvollen und zukunftsfähigen Umgang mit KI zu geben.

II. Executive Summary

Im Ergebnis kommen die Verfasser zu dem Schluss, dass es zwar diverse gesetzliche Vorgaben zu beachten gilt, sich diese jedoch durchweg bewältigen lassen. Der Anwaltschaft steht es frei, die ihr durch KI eröffneten Möglichkeiten zu nutzen.

² Ein KI-Modell ist abstrakt betrachtet das zugrundeliegende lernfähige mathematische Modell bzw. die Algorithmik (etwa ein trainiertes neuronales Netz), während das KI-System das fertige Produkt darstellt, das auf einem oder mehreren KI-Modellen basiert. Ein KI-Modell allein ist also noch keine funktionsfähige Anwendung – erst zusätzliche Komponenten wie z.B. eine Nutzeroberfläche, Datenvorverarbeitung und spezifische Anwendungslogik machen daraus ein KI-System.

- Unter Einhaltung bestimmter Vorgaben ist der Einsatz von KI- und Cloud-Diensten berufsrechtlich zulässig:
 - Beim Einsatz von KI in der Anwaltschaft ist der Grundsatz der Gewissenhaften Berufsausübung (§ 43 BRAO) zu beachten. Rechtsanwältinnen und Rechtsanwälte müssen die von KI generierten Ergebnisse sorgfältig überprüfen und sicherstellen, dass sie den rechtlichen Standards und den Erwartungen der Mandanten entsprechen. Wünscht der Mandant hingegen die Verwertung eines KI-Ergebnisses ohne weitere anwaltliche Prüfung, ist dies zulässig und verstößt nicht gegen das Gebot der Gewissenhaftigkeit.
 - Die Nutzung von KI-Tools und Cloud-Diensten durch Rechtsanwälte ist oft mit der Verarbeitung von Mandatsdaten durch externe Dienstleister verbunden. Dabei sind sowohl die berufsrechtliche Verschwiegenheitspflicht (§ 43a Abs. 2 BRAO) als auch das strafrechtliche Offenbarungsverbot (§ 203 StGB) zu beachten.
 - Nach § 43e Abs. 1 BRAO dürfen Dienstleister ohne Mandanteneinwilligung eingebunden werden, sofern dies für die Dienstleistung erforderlich ist. Ebenso erlaubt § 203 Abs. 3 S. 2 StGB die Offenbarung gegenüber mitwirkenden Personen. Technische Zugriffsbeschränkungen sind zu berücksichtigen, jedoch besteht keine allgemeine Pflicht zur Nutzung aufwendiger Verschlüsselung, wenn dies die Nutzung der Dienstleistung unzumutbar erschwert.
- Auch die datenschutzrechtlichen Vorgaben sind erfüllbar und unterscheiden sich nicht von den bekannten datenschutzrechtlichen Anforderungen.
 - Die bekannten datenschutzrechtlichen Rechtsgrundlagen ermöglichen die Datenverarbeitung in KI-Systemen.
 - Anonymisierung oder Pseudonymisierung können dabei helfen, Risiken zu verringern, sind aber nicht zwingend, sofern die Datenverarbeitung auf die vorhandenen Rechtsgrundlagen der DSGVO gestützt werden kann.
 - Entscheidend ist, dass Anwältinnen und Anwälte datenschutzrechtliche Prinzipien beachten und zuverlässige Dienstleister wählen, um Vorteile von KI-Systemen zu nutzen und die Rechte Betroffener zu schützen.
- Mit Blick auf die EU-KI-Verordnung ist zu betonen, dass die meisten in der Anwaltskanzlei eingesetzten KI-Systeme nicht als hochriskant eingestuft werden. Der Aufbau der KI-Kompetenz ist ein wichtiges und positives Element, das letztlich den Umgang mit KI-Systemen sicherer machen wird.
- Bei der Nutzung von KI-Systemen müssen auch urheberrechtliche Vorgaben beachtet werden, insbesondere bei der Verarbeitung urheberrechtlich geschützter Inhalte. Doch auch dies ist kein Novum in der anwaltlichen Praxis,

die schon immer eine urheberrechtskonforme Verarbeitung von Inhalten voraussetze.

- Werden durch den Einsatz von KI-Systemen vertrauliche Mandatsinformationen an Dritte übermittelt, kann das Geschäftsgeheimnisschutzgesetz (GeschGehG) greifen. Der Schutz durch das GeschGehG wird jedoch in der anwaltlichen Praxis weitgehend vom Berufsrecht (§ 43a BRAO, § 2 BORA) und Strafrecht (§ 203 StGB) überlagert.

III. Use Cases & Chancen des KI-Einsatzes

1. Intelligente Recherche

KI-gestützte Recherchertools ermöglichen eine schnelle Analyse juristischer Texte (z.B. Urteile, Kommentierungen, Gesetzesbegründungen, Gutachten) sowohl in externen Datenbanken als auch in internen Kanzleibeständen. Durch den Einsatz von Natural Language Processing lassen sich für die juristische Prüfung und Beratung relevante Treffer auch bei komplexen Fragestellungen gezielt und effizient auffinden. Darüber hinaus erlauben KI-Systeme auch die intelligente Suche in nicht-juristischen Inhalten wie Fachliteratur, Branchenstudien, Pressemitteilungen oder technischen Dokumentationen, was insbesondere bei interdisziplinären Mandaten und der Sachverhaltsaufarbeitung von Vorteil ist.

2. Dokumentenanalyse

In Due-Diligence-Prozessen oder bei der Vertragsprüfung kann KI gezielt Daten extrahieren, relevante Klauseln erkennen und potenzielle Risiken hervorheben. Der Einsatz von KI unterstützt somit die Sichtung und Prüfung umfangreicher Dokumente und großer Dokumentenmengen.

Zudem eröffnen sich prognostische Einsatzmöglichkeiten: Durch Mustererkennung in juristischen Daten kann KI bei der Bewertung von Prozessrisiken und Erfolgschancen unterstützen.

3. Entwurf und Vorbereitung juristischer Dokumente

KI-gestützte Anwendungen helfen, wiederkehrende Prozesse in der Erstellung juristischer Texte zu standardisieren – etwa bei der Gestaltung von Standardverträgen und Mustern. Bereits heute werden Vertragsentwürfe, Testamente oder andere Schriftstücke in der Praxis häufig mithilfe generativer Textmodelle vorbereitet, wodurch Formularvorlagen ersetzt werden können. Besonders praxisrelevant sind auch KI-unterstützte sprachliche Anpassungen in umfangreichen Dokumenten, etwa für geschlechterbezogene Anpassungen wiederkehrender Begriffe (Kläger/Klägerin, Käufer/Käuferin) oder zur stilistischen Vereinheitlichung.

4. Zusammenfassungen juristischer Texte

Große Sprachmodelle werden eingesetzt, um umfangreiche juristische Texte auf das Wesentliche zu verdichten. Sie erstellen strukturierte Übersichten, kurze Exzerpte oder leicht verständliche Versionen komplexer Inhalte. Das erleichtert nicht nur interne Knowledge Management-Prozesse, sondern auch die externe Kommunikation: Rechtsanwältinnen und Rechtsanwälte können so komplexe Dokumente schneller erfassen und erläutern.

5. Transkription und Protokollierung

Die Transkription von Videokonferenzen und Gesprächen kann durch KI-Systeme heute weitgehend automatisiert erfolgen. So entstehen Gesprächsprotokolle, die sich wiederum mithilfe von KI zusammenfassen und aufbereiten lassen. Dies führt zu erheblicher Zeitsparnis und einer verbesserten Dokumentation.

6. KI in Marketing und Kommunikation

Auch im Marketing können Kanzleien KI gewinnbringend einsetzen. Mit Sprachmodellen lassen sich hochwertige Texte für Newsletter, Blogbeiträge oder Webseiten generieren. Bild-KIs unterstützen bei der visuellen Gestaltung. Gleichzeitig lassen sich Mandantenkontakte mit KI-gestützten Systemen strukturieren und zielgerichtet ansprechen. Die Automatisierung spart Zeit und trägt zu einer konsistenten Außendarstellung bei. Darüber hinaus lassen sich Themen, Strukturen und konkrete Inhalte für Fachbeiträge, Präsentationen oder Panelmoderationen entwickeln und ordnen – oder es entstehen kreative Impulse für Ideenfindung und Umsetzung.

7. Entwicklung und Einsatz eigener KI-Systeme

Kanzleien haben die Möglichkeit, eigene KI-gestützte Systeme (Agents; interne Work-Flows) zu entwickeln. Ob zur automatisierten Klauselanalyse, zur Prüfung von AGB oder zur Bewertung von Schriftsätzen – durch den gezielten Einsatz eigener Tools lassen sich Arbeitsprozesse optimal auf die Bedürfnisse der Kanzlei zuschneiden und vereinfachen aufwändige administrative oder mandatsbegleitende Arbeit.

8. Alltags-KI

Neben spezialisierten Anwendungen findet KI auch im Kanzleialltag zunehmend Anwendung. Übersetzungstools und Chatbots sind KI-gestützt und helfen bei der Formulierung oder Übersetzung von Texten. Diese Alltagshelfer sind niedrigschwellig einsetzbar - gerade auch in der täglichen internen wie externen Korrespondenz – und erleichtern den Einstieg in die KI-Nutzung.

IV. Aspekte des Berufsrechts

1. Gewissenhafte Berufsausübung, § 43 BRAO

a) § 43 BRAO als Generalklausel

Bei der Verwendung von KI sind vor allem zwei berufsrechtliche Kardinalpflichten relevant: die Verschwiegenheit, § 43a Abs. 2 BRAO (siehe unter 2.), und die Gewissenhaftigkeit, § 43 S. 1 BRAO. Konkretisierungen der Berufspflichten in anderen Regelungen der BRAO oder der BORA gehen § 43 BRAO vor.³ Berufsrechtliche Konkretisierungen in Bezug auf KI-Verwendung liegen naturgemäß noch nicht vor. § 2 BORA enthält eine Konkretisierung ausschließlich in Bezug auf die Verschwiegenheit. § 43 BRAO wird aber auch als "Transportnorm" angesehen, soweit nach ihrer Bedeutung im Einzelfall zu beurteilende Verstöße gegen den Mandanten geschuldeten Pflichten vorliegen, die damit berufsrechtlich relevant werden.

b) Prüfungspflicht und deren Einschränkung durch die Mandatierung

Rechtsanwältinnen und Rechtsanwälte schulden die Bearbeitung eines Mandats unter Nutzung ihrer persönlichen Fähigkeiten und Kenntnisse. Arbeitsteilige Mandatsbearbeitung und Nutzung technischer Hilfsmittel sind eingeschlossen, sei es durch KI-unterstützte Klärung von Rechtsfragen, Zusammenfassung von Rechtsprechung oder Literatur und die Erstellung oder Prüfung von Vertragsdokumenten oder Schriftsätze (siehe die Use Cases III. 1. bis 4. und 7.). Der Inhalt der geschuldeten Tätigkeit folgt aus der Mandatsvereinbarung. Will der Mandant, dass das durch bestimmte KI-Systeme generierte Ergebnis nicht nochmals überprüft wird, sondern die Arbeitsgrundlage für die weitere anwaltliche Tätigkeit darstellt, ist das zulässig und stellt keinen Verstoß gegen das Gebot der Gewissenhaftigkeit dar.

Fehlt es an dieser Begrenzung des Mandats, steht die ungeprüfte Übernahme und Weitergabe von ausschließlich durch KI gewonnenen Ergebnissen im Gegensatz zum geschuldeten Einsatz der persönlichen Kenntnisse eines Anwalts. Sie verletzt nicht nur den Anwaltsvertrag, sondern in groben und dann meist vorsätzlichen Fällen auch das Gebot der Gewissenhaftigkeit.⁴ In Extremfällen kann sogar bezweifelt werden, ob das Arbeitsprodukt noch als Ergebnis anwaltlicher Tätigkeit gelten kann.

c) Prüfungskriterien

Gewissenhaft handeln Rechtsanwältinnen und Rechtsanwälte also nur, wenn sie das Ergebnis der KI kritisch prüfen, sofern eine solche Überprüfung nicht explizit

³ Inwieweit diese Norm als Generalklausel Wirkung entfaltet, ist Gegenstand umfangreicher Diskussion in der Literatur. Siehe *Prütting*, in: Henssler/Prütting, BRAO, 6. Aufl. 2024, § 43 Rn. 19 ff. und *Träger*, in: Weyland, BRAO, 11. Aufl. 2024, § 43 ff., jeweils mit Verweisen.

⁴ Ähnliche Fälle finden sich bei *Prütting*, in: Henssler/Prütting, BRAO, § 43 Rn. 29.

im Mandatsvertrag ausgeschlossen ist. Eine praktische Orientierung bietet dabei die übliche Pflicht zur Überprüfung des Arbeitsergebnisses eines Mitarbeiters. Implizite Beurteilungskriterien sind dabei regelmäßig: Plausibilität und Überzeugungskraft, die Beachtung und Ausschöpfung der juristischen Methodenlehre sowie des eigenen aktuellen Wissens. Bei Zweifeln sind Kommentare und andere Fachliteratur heranzuziehen. Belegstellen in KI-Texten sind vollständig zu prüfen, auch wenn keine konkreten Hinweise auf Halluzinationen vorliegen. Das geht sicher über die Prüfung des Entwurfs einer Kollegin oder eines Kollegen hinaus, ist aber geboten. Ein "Grundvertrauen" wie in langjährige, erfahrene und zuverlässige Mitarbeitende kann KI-generierten Arbeitsprodukten (jedenfalls noch) nicht entgegengebracht werden.

d) Risikobewusstsein

Die unter c) aufgeführten Kriterien setzen in aller Regel voraus, dass sich die prüfende Rechtsanwältin oder der Rechtsanwalt im betroffenen Sachgebiet bereits auskennt. Während eine Spezialisierung nicht erforderlich ist, müssen gewisse Grundlagenkenntnisse vorhanden sein, um sich ein eigenständiges Urteil bilden zu können. KI sollte daher nicht als alleinige Grundlage dienen, um sich in neue Sachgebiete einzuarbeiten.

Die typischen Risiken bei der Arbeit mit KI sollten bekannt sein (Art 4 KI-VO; dazu VI.). Ein Beispiel ist das Risiko des Halluzinierens – also die Erzeugung falscher oder "erfundener" Informationen, die von der KI überzeugend als Fakten dargestellt werden. KI-Modelle verfügen über kein echtes Weltwissen, sondern generieren Antworten durch statistische Vorhersagen auf Basis ihrer Trainingsdaten. Selbst bei korrekten Trainingsdaten können sie falsche Inhalte produzieren, da sie probabilistisch den wahrscheinlichsten nächsten Text vorhersagen, ohne zu "wissen", ob dieser der Realität entspricht. Rechtsanwältinnen und Rechtsanwälte sollten sich dieser grundsätzlichen Beschränkung stets bewusst sein. Es ist nicht erforderlich, das Phänomen technisch erklären zu können, wohl aber, zu wissen, dass Halluzinationen unvorhersehbar auftreten können.

2. Zulässiger Einsatz externer Cloud-Anbieter und KI-Dienstleister

Die Nutzung von KI-Systemen durch Rechtsanwältinnen und Rechtsanwälte ist regelmäßig mit der Nutzung von Cloud-Diensten und bei GKI häufig mit der Verarbeitung von Mandatsdaten durch Externe verbunden. Einzelheiten zum Mandat können sich zum Beispiel aus Verträgen, Gerichtsentscheidungen, Schriftsätze oder sonstigen mandatsbezogenen Schriftstücken ergeben, soweit diese mithilfe einer KI-Anwendung erstellt oder bearbeitet bzw. zusammengefasst oder analysiert werden (siehe die Use Cases III. 2. bis 4.). Dasselbe gilt für das Transkribieren digitaler Meetings (siehe der Use Case III. 5.). Dies wirft zwangsläufig Fragen nach der allgemeinen Verschwiegenheitspflicht auf.

a) Verschwiegenheitspflicht nach § 43a Abs. 2 BRAO und Einsatz externer Dienstleister nach § 43e BRAO

Nach § 43a Abs. 2 BRAO haben Rechtsanwältinnen und Rechtsanwälte über Mandat und Mandanten zu schweigen. Sie dürfen Dritten grundsätzlich nicht den Zugang zu den ihnen im Rahmen ihrer Berufsausübung anvertrauten Geheimnissen eröffnen. § 43a Abs. 2 BRAO wird von § 203 StGB flankiert, der die vorsätzliche Offenbarung fremder Geheimnisse unter Strafe stellt.

Nach der Gesetzesbegründung wird bereits die bloße Möglichkeit, Einblick in mandatsbezogene Tatsachen zu erlangen, als Offenlegung gewertet. Danach ist bereits der bloße Speichervorgang von Mandantendaten auf den Servern eines externen KI- und/oder Cloud-Anbieters ein Zugänglichmachen bzw. Offenbaren im Sinne der genannten Vorschriften, da Mitarbeiter des Dienstleisters potenziell darauf zugreifen könnten.

Die Einbindung externer Dienstleister war daher lange Zeit rechtlich schwierig und erforderte häufig die ausdrückliche Einwilligung der Mandanten. Der Gesetzgeber hat im Jahr 2017 mit der Einführung des § 43e Abs. 1 BRAO und der Neufassung des § 203 StGB durch das Berufsgeheimnisschutzgesetz⁵ eine neue Rechtsgrundlage für die Einschaltung externer Dienstleister geschaffen und wollte damit der bestehenden Unsicherheit ein Ende setzen⁶.

So dürfen nach § 43e Abs. 1 BRAO Rechtsanwältinnen und Rechtsanwälte Dienstleistern den Zugang zu geschützten Tatsachen (§ 43a Abs. 2 S. 1 BRAO) auch ohne Einwilligung der Mandantinnen und Mandanten eröffnen, soweit dies für die Inanspruchnahme der Dienstleistung erforderlich ist. Nach § 203 Abs. 3 S. 2 StGB dürfen Rechtsanwältinnen und Rechtsanwälte fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist. Der in § 43e BRAO verwendete Begriff der Zugangseröffnung entspricht inhaltlich dem des "Offenbahrens" in § 203 StGB.

Trotz dieser klaren gesetzlichen Regelung bestehen in der Praxis weiterhin erhebliche Vorbehalte gegenüber dem Einsatz von KI- und Cloud-Dienstleistern. Die dabei vorgebrachten Argumente und Missverständnisse sollen im Folgenden beleuchtet werden.

b) Begriff des Dienstleisters bzw. sonstiger mitwirkender Personen

Die Ausnahme von der allgemeinen Verschwiegenheitspflicht in § 43e Abs. 1 BRAO genauso wie die Ausnahme von dem eigentlich strafbewehrten Offenbaren

⁵ Gesetz zur Neuregelung zum Schutz von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen, BGBl. 2017 I, 3618.

⁶ BT-Drs. 18/11936, 33; *Gasteyer*, in: *Hartung/Scharmer*, Berufs- und Fachanwaltsordnung, 8. Aufl. 2022, § 43 BRAO Rn. 1; *Henssler*, in: *Henssler/Prütting*, BRAO, § 43e Rn. 4; *Nöker*, *Weyland*, BRAO, § 43 Rn. 1

in § 203 Abs. 3 S. 2 StGB knüpft im ersten Schritt an die Qualifikation eines Dritten als Dienstleister bzw. sonstige mitwirkende Person an.

Ein Dienstleister i.S.d. § 43e BRAO ist eine andere Person oder Stelle, die von Rechtsanwältinnen und Rechtsanwälten im Rahmen ihrer Berufsausübung mit Dienstleistungen beauftragt wird. Eine "sonstige mitwirkende Person", muss nach § 203 Abs. 3 StGB an der beruflichen Tätigkeit von Rechtsanwältinnen und Rechtsanwälten mitwirken, sodass der in § 203 Abs. 3 S. 2 StGB verwendete Begriff der "sonstigen mitwirkenden Person" dem Begriff des Dienstleisters in § 43e Abs. 1 S. 2 BRAO entspricht.⁷

Voraussetzung ist damit eine bewusste Einbindung in die berufliche Tätigkeit. Dies wird bei externen Cloud- und/oder KI-Dienstleistern, die von Rechtsanwältinnen und Rechtsanwälten nach Maßgabe des § 43e BRAO ausgesucht und zur Verschwiegenheit verpflichtet wurden, regelmäßig der Fall sein.

Bei frei im Internet verfügbaren Versionen von KI-Systemen bzw. Cloud-Anwendungen ist dieses Kriterium hingegen nicht erfüllt. Die Eingabe von Berufsgeheimnissen in öffentlich zugängliche Übersetzungstools oder Sprachmodelle stellt daher eine unzulässige Offenbarung gegenüber Dritten dar – mit entsprechenden berufs- und strafrechtlichen Konsequenzen.

c) Notwendigkeit der Anonymisierung oder Pseudonymisierung?

Wollen Rechtsanwältinnen und Rechtsanwälte solche frei verfügbaren Anwendungen nutzen, besteht für sie die Pflicht zur vollständigen vorherigen Anonymisierung und/oder Pseudonymisierung der unter das Berufsgeheimnis fallenden Inhalte (vgl. auch unter V.). Denn in dieser Konstellation muss ein Zugänglichmachen bzw. Offenbaren von Berufsgeheimnissen zwingend verhindert werden.

Handelt es sich bei den Tools aber um solche, die von einem nach Maßgabe des § 43e BRAO ausgewählten und verpflichteten Dienstleister angeboten werden, steht es Rechtsanwältinnen und Rechtsanwälten frei, von der ihnen gesetzlich eingeräumten Befugnis der Nutzung solcher Dienstleister Gebrauch zu machen. Eine allgemeine Pflicht zur vorherigen Pseudonymisierung oder gar Anonymisierung besteht in diesen Konstellationen nicht und würde den Einsatz vieler KI-Systeme und Cloud-Dienste verhindern und Rechtsanwältinnen und Rechtsanwältinnen letztendlich die ihnen vom Gesetzgeber 2017 eingeräumte Erleichterung wieder entziehen.

⁷ Als Dienstleister werden in § 43e Abs. 1 S. 2 BRAO Personen oder Einrichtungen definiert, die von einem Berufsgeheimnisträger für die Erbringung von Diensten im Zuge seiner beruflichen Tätigkeit beauftragt sind. Ähnlich wie in der Gesetzesbegründung zu § 203 StGB führt der Gesetzgeber explizit IT-Dienste, Büroservices wie Schreiarbeiten, Telefon-, Postdienste oder Druckservice sowie Buchführung, die externe Zertifizierung der Kanzlei und Steuerberatungsdienstleistungen als Beispiele auf (BT-Drs. 18/11936, 34). Die Aufzählung ist natürlich nicht abschließend, sodass insbesondere auch Cloud- und KI-Dienstleistungen von der Definition erfasst sind. (Ausdrücklich zu Cloud-Dienstleistungen: Gasteyer, in: Hartung/Scharmer, Berufs- und Fachanwaltsordnung, § 43 BRAO Rn. 4; Hessler, in: Hessler/Prütting, BRAO, § 43e Rn. 9.).

d) Erforderlichkeit

Doch auch gegenüber Dienstleistern i.S.d. § 43e BRAO ist die Offenlegung nicht uneingeschränkt möglich. Denn nur wenn die Zugangseröffnung bzw. das Offenbaren des Berufsgeheimnisses erforderlich ist, bleibt die Verschwiegenheitspflicht gewahrt und die Offenbarung straffrei.

aa) Bezugspunkt

Der Bezugspunkt der Erforderlichkeit ist der Zweck des Zugänglichmachens bzw. der Offenlegung. Es geht nicht um die Frage, ob die Dienstleistung für die Ausübung des anwaltlichen Berufs erforderlich ist oder ob die Rechtsanwältin oder der Rechtsanwalt die Tätigkeit selbst hätten vornehmen können. Dies bleibt die unternehmerische Entscheidung der Rechtsanwältinnen und Rechtsanwälte und liegt in deren Ermessen.⁸ Eine Abwägung zwischen den wirtschaftlichen Interessen von Rechtsanwältinnen und Rechtsanwälten und den Schutzinteressen des Mandanten ist nach der Grundsatzentscheidung des Gesetzgebers nicht erforderlich, um die Dienste des Dritten in Anspruch zu nehmen und/oder den Umfang des Offenzulegenden zu bestimmen.

bb) Schwelle

Allerdings haben Rechtsanwältinnen und Rechtsanwälte zumutbare und angemessene Sicherungsmaßnahmen zu ergreifen, um die Kenntnisnahme auf das Erforderliche einzuschränken.⁹ Der Gesetzgeber hat in der Begründung zu § 43e BRAO darauf hingewiesen, dass für die Erforderlichkeit strenge Maßstäbe gelten, um dem hohen Gut der anwaltlichen Verschwiegenheit gerecht zu werden.¹⁰ Dort heißt es in Bezug auf die Erforderlichkeit:

"Hierbei sind auch technische Zugriffsbeschränkungen zu berücksichtigen. Mietet etwa ein Rechtsanwalt lediglich Speicherplatz auf einem externen Server an, ist es nicht erforderlich, dass der Vertragspartner Zugang zu Tatsachen erhält, die der Verschwiegenheit nach § 43a Absatz 2 Satz 1 BRAO unterliegen; denn regelmäßig können diese Daten verschlüsselt gespeichert werden."¹¹

Diese in vielen Abhandlungen teilweise wörtlich wiedergegebene Stelle wird ausgehend von dem Verständnis, dass bereits die reine Möglichkeit der

⁸ Gasteyer, in: Hartung/Scharmer, Berufs- und Fachanwaltsordnung, § 43 BRAO Rn. 6; Henssler, in: Henssler/Prütting, BRAO, § 43e Rn. 8.

⁹ Gasteyer, in: Hartung/Scharmer, Berufs- und Fachanwaltsordnung, § 43 BRAO Rn. 6.

¹⁰ BT-Drs. 18/11936, 34; Günther, BeckOK BRAO, 27. Edition, Stand: 01.02.2025, § 43e Rn. 6; Henssler, in: Henssler/Prütting, BRAO, § 43e Rn. 8; a.A.: Brüggemann/Rein, DStR 2017, 2572, 2574.

¹¹ BT-Drs. 18/11936, 34.

Kenntnisnahme eine Zugangseröffnung i.S.d. § 43e Abs. 1 BRAO darstellt, dahin verstanden, dass der Zugriff von Cloud- und/oder KI-Dienstleistern auf die Mandatsdaten technisch ausgeschlossen sein muss. Eine solche Interpretation negiert jedoch das Wort "regelmäßig" und basiert auf einem realitätsfernen technischen Verständnis.

Zwar existieren Verschlüsselungsmethoden, die einen Zugriff des Dienstleisters vollständig ausschließen (z.B. "Hold-your-own-key" (HYOK) Verschlüsselung). Diese sind jedoch mit erheblichem technischem Aufwand, organisatorischen Risiken (z.B. bei Daten- oder Schlüsselverlust) sowie praktischen Einschränkungen verbunden. Daher wäre ihre verpflichtende Verwendung gegenüber Cloud- und/oder KI-Dienstleistern kontraproduktiv für die Erreichung der Zwecke der mit § 43e BRAO verwirklichten Reform und praxisfern wegen der existenzbedrohenden Risiken im Fall des Schlüsselverlusts. Wenn eine Verschlüsselungsmethode dazu führen würde, dass die begehrte Dienstleistung faktisch nicht nutzbar ist oder mit einem erheblichen Aufwand auf Seiten der Rechtsanwältinnen und Rechtsanwälte verbunden ist, kann sie nicht zur Pflicht erhoben werden.

Rechtsanwältinnen und Rechtsanwälte sollen nach der Gesetzesbegründung einen "*Spielraum für verantwortliche unternehmerische Entscheidungen*" behalten.¹² Der Gesetzgeber hat bereits 2007 erkannt, dass gegenüber IT-Spezialisten das Offenbaren im Sinne der Ermöglichung der Kenntnisnahme erforderlich ist, damit Berufsgeheimnisträger deren Tätigkeit (Wartung, Einrichtung etc. der IT-Anlagen) überhaupt sinnvoll in Anspruch nehmen können.¹³ Diese Aussage ist im Jahr 2025 auf KI und/oder Cloud-Dienstleister zu erweitern. Zwar ist eine verschlüsselte Datenübertragung gängiger Standard und muss eingehalten werden. Bei der Verarbeitung von Daten in der Cloud ist es aber notwendig, dass diese für die Verarbeitung vorübergehend entschlüsselt¹⁴ oder im Falle von Wartungen oder Problemlösungen nur unter strengen organisatorischen Vorgaben eingesehen werden. Diese Vorgänge sind als erforderlich im Sinne des § 43e Abs. 1 BRAO bzw. § 203 Abs. 3 StGB zu verstehen. Dasselbe gilt für die KI-Systeme. Entscheiden sich Rechtsanwältinnen und Rechtsanwälte z.B. in Massenverfahren, KI-Systeme einzusetzen, um Schriftsätze schneller bearbeiten zu können, und werden diese KI-Systeme von externen Dienstleistern betrieben, kommt es zu einem Zugänglichmachen i.S.d. § 43e Abs. 1 BRAO bzw. einem Offenbaren i.S.d. § 203 Abs. 3 StGB von Mandatsgeheimnissen. Dieses ist dann als erforderlich zu werten und kann nicht beanstandet werden.

¹² BT-Drs. 18/11936, 34.

¹³ BT-Drs. 18/11936, 28.

¹⁴ So auch: *Henssler*, in: *Henssler/Prütting*, BRAO, § 43e Rn. 8 m.w.N.

e) Verschwiegenheitsvereinbarung

§ 43e Abs. 3 BRAO stellt Mindestanforderungen an die vertragliche Vereinbarung zwischen Rechtsanwältinnen und Rechtsanwälten und dem externen Dienstleister. So müssen Rechtsanwältinnen und Rechtsanwälte den Dienstleister in Textform unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit verpflichten. Dies liegt auch im ureigenen Interesse der Rechtsanwältinnen und Rechtsanwälte, da sie sich nach § 203 Abs. 4 S. 2 Nr. 1 StGB strafbar machen, wenn der von ihnen eingesetzte Dienstleister Berufsgeheimnisse offenbart und der Berufsgeheimnisträger nicht dafür Sorge getragen hat, dass der Dienstleister zur Geheimhaltung verpflichtet wurde. Mit der Erfüllung der Pflicht nach § 43e Abs. 3 Nr. 1 BRAO verhindern Rechtsanwältinnen und Rechtsanwälte damit ihre Strafbarkeit, selbst wenn es zu einem Geheimnisbruch durch den Dienstleister kommt.

Manche Cloud- bzw. KI-Anbieter scheuen die Unterzeichnung entsprechender Verschwiegenheitsvereinbarungen. Dies beruht teilweise auf dem Missverständnis, dass erst die Unterzeichnung der Verschwiegenheitsvereinbarung oder die darin enthaltene strafrechtliche Belehrung die Strafbarkeit begründeten. Dies ist offensichtlich unzutreffend, da die für den Dienstleister relevanten Straftatbestände nicht durch die Unterzeichnung der Verschwiegenheitsverpflichtung erfüllt oder begründet werden. Vielmehr knüpfen die Tatbestände an die Offenlegung des anvertrauten Geheimnisses (§ 203 Abs. 4 S. 1 StGB) bzw. die fehlende Verpflichtung der eingesetzten Unterauftragnehmer (§ 203 Abs. 4 S. 2 Nr. 2 StGB) an. Die Verschwiegenheitsvereinbarung in § 43e Abs. 3 S. 2 Nr. 1 BRAO dient insoweit "nur" dem Zweck, den Dienstleister auf die ohnehin für ihn bestehende Strafdrohung des § 203 StGB hinzuweisen.

Neben einer Regelung über den Einsatz von Subunternehmern (§ 43e Abs. 3 S. 2 Nr. 3 BRAO) muss die Vereinbarung den Dienstleister dazu verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist (§ 43e Abs. 3 S. 2 Nr. 2 BRAO).¹⁵ In der Praxis bedeutet dies, dass der Dienstleister keine Dritten ohne vorherige Zustimmung einschalten darf bzw. seinerseits vertraglich verpflichtet wird, allen eigenen Mitarbeitern oder Subunternehmern dieselben Geheimhaltungspflichten aufzuerlegen. Ein entsprechender Passus wird i.d.R. in den Dienstleistervertrag aufgenommen, um Kettenweitergaben zu verhindern. Bei KI-Dienstleistern ist zudem zu regeln, dass die Daten nicht zu Trainingszwecken eingesetzt werden dürfen, da das KI-Training mit Mandatsdaten die Erforderlichkeitsschwelle nicht erreichen dürfte.

¹⁵ Gasteyer, in: Hartung/Scharmer, Berufs- und Fachanwaltsordnung, § 43 BRAO Rn. 20 ff.; Henssler, in: Henssler/Prütting, BRAO, § 43e Rn. 24 ff.

f) Einwilligung der Mandanten nur bei "unmittelbar [in] einem einzelnen Mandat" eingesetzten Tools

Es bestehen keine allgemeinen Berufspflichten, den Mandanten über den Einsatz von KI zu informieren. Eine ausdrückliche Einwilligung des Mandanten ist nach § 43e Abs. 5 BRAO nur notwendig, wenn der Einsatz der KI- und/oder Cloud-Dienste unmittelbar einem konkreten Einzelmandat dient und nicht Teil der allgemeinen Kanzleiinfrastruktur ist. Entscheidend für die Einordnung ist, ob die Dienstleistung "unmittelbar" einem einzelnen Mandat dient oder ob es sich um ein allgemein in der Kanzlei eingesetztes Werkzeug handelt.¹⁶

Wird ein KI-System oder eine Cloud-Anwendung aufgrund der Organisationsentscheidung der Kanzlei in einer Vielzahl von Mandaten als allgemeines Arbeitsmittel eingesetzt, liegt kein Fall des § 43e Abs. 5 BRAO vor.

g) Angemessener Berufsgeheimnisschutz bei KI-Dienstleistern im Ausland

§ 43e Abs. 4 BRAO bestimmt, dass Rechtsanwältinnen und Rechtsanwälte Dienstleistern im Ausland nur dann Zugang zu Mandatsgeheimnissen eröffnen dürfen, wenn dort ein vergleichbarer Schutz der Geheimnisse wie im Inland besteht. Für EU-Mitgliedsstaaten unterstellt die Gesetzesbegründung ein vergleichbares Schutzniveau.¹⁷ Jedes andere Ergebnis wäre EU-rechtswidrig.¹⁸

In der Praxis hat sich die richtige Vorgehensweise etabliert, wonach ein angemessenes Schutzniveau i.S.d. § 43e Abs. 4 BRAO entsprechend den datenschutzrechtlichen Maßstäben angenommen wird (siehe unter V.).

3. Verhältnis zwischen § 43e BRAO und § 203 StGB

Zwischen § 43e BRAO und § 203 StGB besteht dem Wortlaut nach kein vollständiger Gleichlauf. Vielmehr geht § 43e BRAO über die Anforderungen des § 203 StGB hinaus. So muss gemäß § 43e Abs. 3 BRAO mit dem Dienstleister ein Vertrag mit bestimmtem Inhalt in Textform abgeschlossen werden und § 43e Abs. 4 BRAO enthält spezielle Vorgaben bezüglich im Ausland ansässiger Dienstleister. Insoweit ist fraglich, ob trotz eines berufsrechtswidrigen Verhaltens das Offenbaren von Berufsgeheimnissen nach § 203 Abs. 3 S. 2 StGB straffrei sein kann (etwa, wenn das eben skizzierte Textformerfordernis nicht eingehalten wird).

Im Ergebnis ist davon auszugehen, dass kein Gleichlauf beider Normen besteht und vor diesem Hintergrund nicht jedes berufsrechtswidrige Verhalten zwingend zu einem strafbaren Verhalten führt. In der Beschlussempfehlung des

¹⁶ BT-Drs. 18/11936, 36; *Günther*, BeckOK BRAO, § 43e Rn. 15; *Henssler*, in: *Henssler/Prütting*, BRAO, § 43e Rn. 35.

¹⁷ BT-Drs. 18/11936, 35; *Gasteyer*, in: *Hartung/Scharmer*, Berufs- und Fachanwaltsordnung, § 43 BRAO Rn. 29; *Günther*, BeckOK BRAO, § 43e Rn. 14; *Henssler*, in: *Henssler/Prütting*, BRAO, § 43e Rn. 28.

¹⁸ *Gasteyer*, in: *Hartung/Scharmer*, Berufs- und Fachanwaltsordnung, § 43 BRAO Rn. 29 m.w.N.

Ausschusses für Recht und Verbraucherschutz zum Berufsgeheimnisschutzgesetz¹⁹ heißt es dementsprechend:

"Liegen die Voraussetzungen des strafrechtlichen Erlaubnistarbestandes in § 203 Absatz 3 Satz 2 des Strafgesetzbuches in der Entwurfsversion (StGB-E) vor, macht sich der Berufsgeheimnisträger – unabhängig von den berufsrechtlichen Regelungen – nicht strafbar. Die Berufsrechtswidrigkeit eines Verhaltens führt also nicht zwingend dazu, dass das Verhalten auch strafbar ist."²⁰

Für eine Rechtfertigung nach § 203 Abs. 3 S. 2 StGB kommt es damit gerade nicht auf den überschließenden Teil des § 43e BRAO, sondern allein auf die Einhaltung der Anforderungen des § 203 Abs. 3 S. 2 StGB an. Für diese Ansicht spricht, dass andernfalls formale Verstöße gegen berufsrechtliche Vorschriften zu einer Strafbarkeit führen würden. Da entsprechende berufsrechtliche Vorschriften für andere von § 203 StGB erfasste Berufsgruppen teilweise nicht existieren (schon aufgrund mangelnder Gesetzgebungskompetenz des Bundes), würde dies zu einer Ungleichbehandlung der verschiedenen Gruppen von Berufsgeheimnisträgern und einer Ausweitung der Strafbarkeit für Rechtsanwältinnen und Rechtsanwälte führen.²¹ Daneben bestünden auch erhebliche Bedenken hinsichtlich des Bestimmtheitsgrundsatzes, sofern berufsrechtliche Regelungen eine Strafbarkeit erweitern bzw. erst statuieren würden.

Gleichwohl kann trotz fehlender Strafbarkeit ein berufsrechtlicher Verstoß vorliegen. Ein nach § 203 Abs. 3 S. 2 StGB gerechtfertigtes Offenbaren von Berufsgeheimnissen ist aufgrund der im Vergleich zu § 203 StGB überschließenden Regelungen des § 43e BRAO nicht zwangsläufig im Einklang mit berufsrechtlichen Vorschriften. Vor dem Hintergrund eben dieser überschließenden Regelungen ist eine Strafbarkeit jedenfalls bei Einhaltung der berufsrechtlichen Befugnisnorm § 43e BRAO ausgeschlossen, da dann der Berufsgeheimnisträger nicht "unbefugt" im Sinne des § 203 StGB handelt²²; so auch die Beschlussempfehlung des Ausschusses für Recht und Verbraucher zum Berufsgeheimnisschutzgesetz: "Allerdings ist ein berufsrechtlich erlaubtes Verhalten niemals strafbar nach § 203 StGB. Denn in diesen Fällen handelt der Berufsgeheimnisträger nicht unbefugt."²³

¹⁹ Gesetz zur Neuregelung zum Schutz von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen, BGBl. 2017 I, 3618.

²⁰ BT-Drs. 18/12940, 8.

²¹ Eisele, in: Tübinger Kommentar, 31. Aufl. 2025, § 203 StGB Rn. 54; Kargl, in: Kindhäuser/Neumann/Paeffgen/Saliger, Strafgesetzbuch, 6. Aufl. 2023, § 203 StGB Rn. 79.

²² BT-Drs. 18/11936, 19, 24; Eisele, in: Tübinger Kommentar, 31. Auflage 2025, § 203 StGB Rn. 54; Kargl, in: Kindhäuser/Neumann/Paeffgen/Saliger, Strafgesetzbuch, 6. Auflage 2023, § 203 StGB Rn. 77.

²³ BT-Drs. 18/12940, 8.

V. Aspekte des Datenschutzrechts

Der Schutz des Mandatsgeheimnisses wird – jedenfalls dann, wenn es sich um Informationen zu natürlichen Personen handelt (Art. 4 Nr. 1 DS-GVO) – von datenschutzrechtlichen Vorgaben (vornehmlich der DS-GVO und des BDSG) flankiert. Angaben mit Personenbezug finden sich in zahlreichen Dokumenten, seien es Korrespondenz, Gesprächsprotokolle und Adresslisten oder Gerichtsentscheidungen, Schriftsätze, Vertragsrubren (siehe insbesondere die Use Cases III. 2 bis 5 und 8.) Bei der Nutzung und der eigenständigen Entwicklung von KI-Systemen, welche solche Dokumente verarbeiten, sind Rechtsanwältinnen und Rechtsanwälte bzw. die Berufsausübungsgesellschaft entweder allein oder mit anderen gemeinschaftlich datenschutzrechtlich verantwortlich (etwa gemeinschaftlich mit Beratungsunternehmen oder anderen Kanzleien (vgl. hierzu die Vorgaben des Art. 26 DS-GVO), wobei die Anbieter von KI-Systemen regelmäßig als Auftragsverarbeiter im Sinne von Art. 28 DS-GVO eingebunden werden.

Die mit dem KI-Einsatz einhergehende Datenverarbeitung wird man zulässig gestalten können, wenn vorab die Datenflüsse genau definiert und dokumentiert werden: So ist zu unterscheiden, ob bei dem KI-Einsatz personenbezogene Informationen von Mandanten, Gegnern, Dritten und Mitarbeitern verarbeitet werden, welchen Zwecken die Datenverarbeitung dient (konkrete Mandatsbearbeitung, Marketingzwecke) und ob diese Zwecke nicht auch anonymisiert oder zumindest pseudonymisiert erreicht werden können. Konkret: Zu prüfen ist vor jeder KI-Implementierung, ob der Einsatz nicht auch mit Informationen ohne Personenbezug (dann anonymisiert, vgl. Erwägungsgrund 26 der DS-GVO, d.h. außerhalb der Anwendung des Datenschutzrechts) oder pseudonymisiert, also etwa ohne direkte Namensnennung, ersetzt durch ein Kennzeichen (vgl. Art. 4 Nr. 5 DS-GVO; es verbleibt bei einer Anwendung des Datenschutzrechts), erfolgen kann. Während die Abgrenzung beider Begriffe aus datenschutzrechtlicher Sicht streitig ist und nicht zwingend dem natürlichen Sprachgefühl folgt, lässt ein aktuelles EuGH-Verfahren auf eine pragmatische Rechtsauffassung hoffen (vgl. den bisherigen Verfahrensgang zu C-413/23 P). Häufig wird man hierdurch datenschutzrechtliche Risiken minimieren können, ohne die Praktikabilität des KI-Einsatzes zu beeinträchtigen.

Kommt es dennoch zur Verarbeitung personenbezogener Daten, ist zu unterscheiden, ob es sich um einfache personenbezogene Daten unter dem Regelungsregime des Art. 6 DS-GVO oder um besondere Kategorien personenbezogener Daten – etwa Gesundheitsdaten – unter den deutlich strengerem Vorgaben des Art. 9 DS-GVO handelt. Die Verarbeitung personenbezogener Daten wird man – u.a. nach vorheriger Prüfung – auf die Erforderlichkeit für die Durchführung des Vertrages (Art. 6 Abs. 1 lit. b DS-GVO), auf berechtigte Interessen (Art. 6 Abs. 1 lit. f DS-GVO) und bei sensiblen Daten auf Art. 9 Abs. 2 lit. b oder f DS-GVO stützen können. Die für die Nutzung des KI-Systems notwendige Übermittlung solcher Daten an den Anbieter des KI-Systems

(soweit dieses wie regelmäßig anzunehmen cloudbasiert ist), bedarf dann keiner zusätzlichen Rechtsgrundlage, soweit der Anbieter als Auftragsverarbeiter tätig wird (was die Regel darstellen wird).

Bei alledem sollten die üblichen datenschutzrechtlich gebotenen Compliance-Maßnahmen innerhalb der Kanzlei – insbesondere die Einbindung des Datenschutzbeauftragten, die Durchführung von Schwellwertanalysen bzw. soweit geboten einer Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) und die ausreichende Dokumentation im Verarbeitungsverzeichnis – beachtet werden. Dabei ist auch auf eine sorgfältige Auswahl der Dienstleister, deren KI-Systeme für die Datenverarbeitung als Auftragsverarbeiter eingesetzt werden, zu achten (vgl. Art. 28 Abs. 1 DS-GVO).

Gerade hinsichtlich des oftmals notwendigen Transfers der Daten in Jurisdiktionen außerhalb der EU / des EWR (insbesondere, weil die meisten Anbieter von KI-Systemen aus solchen Drittstaaten (z.B. den USA) heraus ihre Dienstleistungen erbringen) sind die Voraussetzungen der Art. 44 ff. DS-GVO zu beachten. Vor dem Hintergrund der weiter vorherrschenden, oftmals kritischen Haltung der Aufsichtsbehörden zu Drittstaatentransfers und entsprechender anhängiger Gerichtsverfahren (u.a. vor dem EuG in der Sache T-553/23 zur Nichtigkeitserklärung des Privacy Frameworks), ist es empfehlenswert, die dynamische Entwicklung in diesem Bereich zu verfolgen. All dies sind jedoch keine Spezialfragen des KI-Einsatzes in der anwaltlichen Praxis, sondern betreffen jedwede Datenverarbeitung, d.h. sind auch im Zusammenhang mit dem Einsatz "normaler" Cloud- oder IT Systeme zu beachten. Der technische Vorsprung von Dienstleistern, die ihre Dienste von außerhalb der EU / des EWR erbringen, lässt aktuell einen Rückgriff auf diese unabdingbar oder jedenfalls wesentlich attraktiver erscheinen. Jedoch ist aktuell die datenschutzrechtlich begrüßenswerte Tendenz erkennbar, dass außerhalb der EU / dem EWR ansässige Cloudanbieter zunehmend eine Infrastruktur aufbauen, die es ihnen ermöglicht, ihre Dienstleistungen (jedenfalls weitestgehend) über Tochtergesellschaften aus der EU / dem EWR heraus erbringen zu können, d.h. ohne Transfers von Daten in Drittstaaten.

Besonderes Augenmerk ist schließlich auf die Transparenzvorgaben der Art. 13 und 14 DS-GVO zu legen, die sowohl beim Beginn einer Mandatsbeziehung als auch im Laufe des Mandats immer wieder überprüft werden sollten (welche Datenverarbeitungen kommen ggf. neu hinzu, über welche Datenverarbeitungen sind Mandanten oder Dritte zu informieren). Gleches gilt für die Betroffenenrechte der Art. 15 ff. DS-GVO, wobei der Fokus den infolge der Datenverarbeitung in KI-Systemen umzusetzenden Rechten auf Berichtigung (Art. 16 DS-GVO) und Löschung (Art. 17 DS-GVO) gilt, soweit es sich bei den in den KI-Systemen dann "vorhandenen" Daten überhaupt um personenbezogene Daten handelt (vgl. hierzu etwa das Diskussionspapier des Hamburger Beauftragten für Datenschutz und Informationssicherheit "Large Language Models und personenbezogene

Daten")²⁴. Schließlich aktiviert jeglicher KI-Einsatz die notwendige Beachtung des Art. 22 DS-GVO: Die datenschutzrechtlich betroffene Person darf grundsätzlich nicht ausschließlich einer auf automatisierter Datenverarbeitung beruhenden Entscheidung unterworfen werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Dies wird jedenfalls bei der reinen Vorbereitung anwaltlicher Entscheidungen nicht der Fall sein. Datenschutzrechtlich komplexer und mit weiteren Herausforderungen verbunden ist das Training von (eigenen) KI-Systemen (siehe hierzu oben auch die Ausführungen zu berufsrechtlichen Herausforderungen in diesem Zusammenhang).

Die Ausführungen zum Datenschutzrecht zeigen insgesamt, dass sich der KI-Einsatz in der anwaltlichen Praxis gut mit den bestehenden Vorgaben der DS-GVO und des BDSG vereinbaren lässt. Soweit personenbezogene Daten verarbeitet werden, liefern die vorhandenen Rechtsgrundlagen eine solide Basis, um auch KI-Anwendungen rechtssicher einzubinden. Gleichzeitig schafft die Möglichkeit zur Anonymisierung oder Pseudonymisierung weitere Spielräume, um Datenschutzrisiken zu minimieren. Voraussetzung ist, dass Rechtsanwältinnen und Rechtsanwälte die datenschutzrechtlichen Prinzipien wie Transparenz, Zweckbindung und Datenminimierung im Blick behalten und angemessene Verträge mit sorgfältig ausgewählten Dienstleistern schließen. Auf diese Weise lassen sich die Vorteile moderner KI-Systeme nutzen, ohne die Rechte betroffener Personen zu gefährden.

VI. KI-VO

Die KI-VO²⁵ ist am 1. August 2024 in Kraft getreten und wird seit Februar 2025 stufenweise anwendbar. Sie schafft in der EU ein unmittelbar anwendbares Regelwerk für den Einsatz von KI-Systemen und verfolgt dabei einen risikobasierten Ansatz.

Anwaltliche Anwendungen wie Chatbots zur Mandantenkommunikation, generative Sprachmodelle zur Texterstellung, Software zur automatisierten Dokumentenprüfung oder Entscheidungshilfen bei der Vertragsanalyse fallen regelmäßig unter die Definition eines "KI-Systems" gemäß Art. 3 Nr. 1 KI-VO und unterliegen daher grundsätzlich den Vorgaben der Verordnung.

Rechtsanwältinnen und Rechtsanwälte können im Zusammenhang mit der Nutzung solcher Systeme entweder als Betreiber oder als Anbieter im Sinne der KI-VO qualifiziert werden. Als *Betreiber* gilt nach Art. 3 Nr. 4 KI-Verordnung jede natürliche oder juristische Person, die ein KI-System beruflich auf eigene Rechnung und eigenes Risiko verwendet. Eine *Anbieterstellung* nach Art. 3 Nr. 3

²⁴ Siehe https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf, zuletzt abgerufen am 02. Juli 2025.

²⁵ Verordnung (EU) 2024/1689 über künstliche Intelligenz.

KI-Verordnung liegt vor, wenn ein KI-System selbst entwickelt oder in Auftrag gegeben und unter eigenem Namen oder in eigener Verantwortung in Betrieb genommen wird. Erfasst ist auch der Fall, dass ein fremdes Sprachmodell – etwa GPT-4 – über eine API in eine eigene Benutzeroberfläche eingebunden wird. Auch dies kann eine Anbieterereigenschaft begründen.²⁶

Die konkreten Verpflichtungen aus der KI-VO hängen von der Einstufung des eingesetzten Systems nach dem risikobasierten Regulierungsansatz der Verordnung ab. Die strengsten Vorgaben gelten für sog. Hochrisiko-KI-Systeme im Sinne des Art. 6. Die typischerweise in der anwaltlichen Praxis eingesetzten Systeme werden allerdings in der Regel nicht in diese Kategorie fallen: Welche KI-Systeme als hochriskant einzustufen sind, ergibt sich aus u.a. Anhang III zur Verordnung. Zwar wird dort unter Nr. 8 der Bereich "Rechtspflege" geregelt – deren Organe die Rechtsanwälte gem. § 1 BRAO sind. Als hochriskant gelten nach Nr. 8 jedoch ausschließlich solche KI-Systeme, die von Justizbehörden eingesetzt werden sollen. Rechtsanwälte werden in Anhang III nicht genannt und fallen auch systematisch nicht unter den Begriff der "Justizbehörden" ("judicial authorities"), da sie keine staatlichen Hoheitsaufgaben wahrnehmen. Dies bestätigt auch Erwägungsgrund 61 der Verordnung, in dem ausdrücklich betont wird, dass der Einsatz von KI-Systemen die Entscheidungsbefugnis von Richtern und die Unabhängigkeit der Justiz nicht ersetzen dürfe.

Die in der anwaltlichen Praxis typischerweise eingesetzten KI-Systeme – etwa zur Unterstützung bei der Texterstellung, Dokumentenanalyse oder Kommunikation – fallen in der Regel in die Kategorie der KI mit geringem oder keinem Risiko. Für solche Systeme sieht die KI-VO keine verbindlichen Zulassungs- oder Konformitätsanforderungen vor. Rechtsanwältinnen und Rechtsanwälte, die solche KI-Systeme anbieten oder betreiben, müssen im Wesentlichen die Vorgaben aus der KI-VO im Hinblick auf KI-Kompetenz und Transparenz beachten.

Art. 4 KI-VO (KI-Kompetenz) verlangt im Kern, dass Rechtsanwältinnen und Rechtsanwälte als Anbieter oder Betreiber von KI-Systemen nach besten Kräften auf ein ausreichendes Maß an KI-Kompetenz bei den mit KI befassten Kanzleiangehörigen hinwirken, sie also schulen lassen. Der Umfang der Maßnahmen ist nicht festgelegt, die Norm gibt ausfüllungsbedürftige Kriterien an. Sanktionen bei Verstößen sind derzeit nicht vorgesehen. Zwar kann § 43 BRAO auch im Hinblick auf öffentlich-rechtliche Pflichten eine Transportfunktion entfalten. Das scheidet aber im Hinblick auf Art 4 KI-VO wegen dessen generalklauselartiger und sanktionsfreier Ausgestaltung aus.

²⁶ Dabei ist klarzustellen, dass eine Anwaltskanzlei durch die Bereitstellung eines KI-Systems, das auf einem vortrainierten Sprachmodell wie GPT-4 basiert, nicht zum Anbieter des zugrundeliegenden KI-Modells mit allgemeinem Verwendungszweck (General Purpose AI, GPAI) wird. Die insoweit geltenden besonderen Pflichten gemäß Art. 52 ff. KI-VO – etwa zur Risikoanalyse, technischen Dokumentation und Kennzeichnung – treffen daher ausschließlich den ursprünglichen Modellanbieter, nicht die Anwaltskanzlei.

Darüber hinaus können in bestimmten Fällen Transparenzanforderungen nach Art. 50 KI-VO zu beachten sein, etwa wenn Rechtsanwältinnen und Rechtsanwälte Chatbots zur Mandantenkommunikation anbieten. Dann ist gem. Art. 50 Abs. 1 KI-VO sicherzustellen, dass die betroffenen Personen darüber informiert werden, dass sie mit einem KI-System interagieren. KI-erzeugte Inhalte müssen nach Art. 50 Abs. 2 KI-VO in maschinenlesbarer Form gekennzeichnet werden. Hierbei handelt es sich um eine Anbieterpflicht, sie gilt also insbesondere für Kanzleien, die zur Nutzung durch Mandanten oder sonstige Dritte eigene KI-Systeme herstellen oder herstellen lassen oder fremde KI-Systeme unter eigenem Namen bereitstellen (siehe insbesondere Use Case III. 8). Kanzleien, die KI-erzeugte Marketinginhalte wie Bilder, Texte oder Videos verbreiten (siehe Use Case III. 6), müssen sich spätestens ab dem 2. August 2026 mit den Anforderungen des Art. 50 Abs. 4 KI-VO auseinandersetzen, denn zu diesem Datum erlangen die gesetzlichen Transparenzpflichten Geltung. Wer zum Beispiel durch KI erstellte Zusammenfassungen oder Auswertungen von bedeutenden Gerichtsurteilen verbreitet, könnte einer Kennzeichnungspflicht gem. Art. 50 Abs. 4 Unterabs. 2 unterliegen, es sei denn, es ist gewährleistet, dass bei solchen Beiträgen zuvor eine redaktionelle Sichtung und Bearbeitung in der Kanzlei stattfindet.

VII. Urheberrecht

Bei der Nutzung von KI-Systemen in Anwaltskanzleien ist die Beachtung des Urheberrechts unerlässlich. Dies empfiehlt sich besonders bei typischen Anwendungsfällen wie der KI-gestützten Bearbeitung urheberrechtlich als Schriftwerk geschützter juristischer Fachliteratur und der Erstellung von Zusammenfassungen solcher Werke oder deren Auswertung für die Beantwortung bestimmter Fragestellungen (siehe die Use Cases III. 1., 3. und 4.). Solche Nutzungen setzen in der Regel eine Vervielfältigung voraus - zumindest dann, wenn die Werke auf Server eines KI-Anbieters hochgeladen werden. In diesen Fällen sollte daher sichergestellt werden, dass entweder bestehende Lizenzen diese Nutzungen abdecken oder erforderliche Lizenzen erworben werden oder dass die beabsichtigte Nutzung durch eine gesetzliche Erlaubnis privilegiert ist. Das Urheberrechtsgesetz erlaubt zwar in § 44a UrhG vorübergehende Vervielfältigungen von Werken, wenn die Vervielfältigung flüchtig oder begleitend ist und nicht schon der Zugriff auf das Werk rechtswidrig erfolgt. Es ist aber mangels Rechtsprechung und mangels verfestigter Meinungen in der Literatur bislang keine klare Tendenz erkennbar, ob das Hochladen urheberrechtlich geschützter Inhalte in eine KI eine Vervielfältigung darstellt, die im Sinne der gesetzlichen Schranke als "vorübergehend" anzusehen ist. Damit hochgeladene Dokumente nicht dauerhaft auf den Servern der KI-Anbieter verbleiben, sollten zumindest die Chats nach Gebrauch gelöscht werden. Bei der Frage, ob die Nutzung von Werken zu Trainingszwecken einer KI Urheberrechte verletzt, besteht eine breite Meinungslandschaft, die das bejaht. § 44b UrhG, der die auch kommerzielle Vervielfältigung zu Zwecken des Text und Data Minings erlaubt, greift jedenfalls dann nicht, wenn sich der Rechtsinhaber die Nutzung der

Trainingsinhalte vorbehalten hat (§ 44b Abs. 3 S. 1 UrhG). Kanzleien, die nicht gewährleisten können, dass Texte vor einer Nutzung mittels KI auf wirksame Nutzungsvorbehalte geprüft werden, sollten vorsorglich sicherstellen, dass in die KI hochgeladene Texte nicht auch zu Trainingszwecken genutzt werden (bzw. dass entsprechende Einstellungen in der KI vorgenommen werden, die das verhindern).

Wichtig zu betonen ist dabei: Das Urheberrecht bildet kein grundsätzliches Hindernis für den Einsatz von KI-Technologien, sondern gibt lediglich den rechtlichen Rahmen vor, innerhalb dessen KI genutzt werden kann.

VIII. § 23 GeschGehSchG

Werden durch den Einsatz von KI-Systemen vertrauliche Mandatsinformationen an Dritte übermittelt, kann der Anwendungsbereich des Geschäftsgeheimnisschutzgesetzes (GeschGehG) eröffnet sein. Das Gesetz findet grundsätzlich auch in der anwaltlichen Berufsausübung Anwendung.²⁷ Denkbare Rechtsfolgen sind zivilrechtliche Ansprüche auf Unterlassung und Schadensersatz sowie strafrechtliche Konsequenzen bei vorsätzlicher Offenlegung (§ 23 GeschGehG).

§ 1 Abs. 3 Nr. 1 GeschGehG stellt jedoch klar, dass bestehende berufsrechtliche Geheimnisschutzregelungen unberührt bleiben. Tatsächlich wird der Schutz durch das GeschGehG weitgehend durch berufs- und strafrechtliche Vorschriften überlagert. Die anwaltliche Verschwiegenheitspflicht (§ 43a Abs. 2 BRAO, § 2 BORA) und deren strafrechtliche Absicherung (§ 203 StGB) erfassen sämtliche relevanten Fallkonstellationen. Nicht jede vertrauliche Mandatsinformation ist zudem gleich ein "Geschäftsgeheimnis" im Sinne des Gesetzes (dies setzt u.a. einen wirtschaftlichen Wert und angemessene Geheimhaltungsmaßnahmen voraus).

Zentral für die Beurteilung der Zulässigkeit des KI-Einsatzes ist § 43e BRAO. Wird KI im Rahmen dieser Vorschrift eingesetzt, insbesondere unter Einhaltung der Anforderungen an die Vertraulichkeit bei Einschaltung externer IT-Dienstleister, liegt auch aus Sicht des GeschGehG keine unbefugte Offenbarung vor (§ 3 Abs. 2 GeschGehG). Maßstab bleibt somit das Berufsrecht – nicht das GeschGehG.²⁸

IX. Fazit

Der Einsatz von KI in der anwaltlichen Praxis bietet vielfältige Chancen zur Effizienzsteigerung, vor allem bei Recherche, Dokumentenanalyse, Texterstellung, aber auch der Mandatsorganisation und dem Wissensmanagement. Gleichzeitig stellt er Rechtsanwältinnen und Rechtsanwälte auch vor Herausforderungen, die nach Ansicht des DAV jedoch beherrschbar

²⁷ Alexander, in Köhler/Feddersen, GeschGehG, 43. Aufl. 2025, § 1 Rn. 35; Siahaan, in Erbs/Kohlhaas, GeschGehG 255. EL Januar 2025, § 23 Rn. 112-118.

²⁸ Vgl. Partsch/Rump, NJW 2020, 120.

bleiben. Besonders relevant ist in diesem Zusammenhang die Einhaltung der Verschwiegenheitspflichten nach § 43e BRAO und § 203 StGB, die sorgfältige Auswahl und die vertragliche Absicherung externer Dienstleister und die Beachtung datenschutzrechtlicher Vorgaben. Hinzu treten urheberrechtliche Anforderungen, insbesondere bei der KI-gestützten Auswertung geschützter Fachliteratur. Die neue KI-VO normiert nunmehr erstmalig unionsweit anwendbare Transparenz- und Kompetenzanforderungen. Die praktische Relevanz der KI-VO für die Anwaltschaft ist derzeit zwar noch begrenzt, dürfte künftig aber zunehmen. Bei sachgerechter Implementierung sollte KI in der Anwaltschaft daher nicht als rechtliches Risiko, sondern als gestaltbarer Bestandteil moderner anwaltlicher Berufsausübung verstanden werden. Zwingende Voraussetzung für einen rechtssicheren Einsatz von KI ist jedoch stets ein informierter, verantwortungsbewusster und rechtlich fundierter Umgang mit den Anwendungen.

Verteiler

Deutschland

Bundesministerium des Innern und für Heimat
Bundesministerium der Justiz und Verbraucherschutz
Bundesministerium für Wirtschaft und Klimaschutz

Ausschuss für Inneres und Heimat im Deutschen Bundestag
Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitales im Deutschen Bundestag
Fraktionen im Deutschen Bundestag

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Die Justizministerien der Länder
Die Datenschutzbeauftragten der Bundesländer

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe e.V.
Deutscher Richterbund, Bund der Richterinnen und Richter, Staatsanwältinnen und
Bund Deutscher Verwaltungsrichter und Verwaltungsrichterinnen
Staatsanwälte e.V. (DRB)
Deutscher Notarverein
Deutscher Steuerberaterverband e.V. Berlin
Bundesverband der Deutschen Industrie e.V.
Arbeitsgemeinschaft berufsständischer Versorgungseinrichtungen e.V.
Deutscher EDV-Gerichtstag e.V.
GRUR - Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht e.V.
Bitkom e. V.
Deutsche Gesellschaft für Recht und Informatik e.V. (DGRI)
ver.di - Vereinte Dienstleistungsgewerkschaft
Gewerkschaft der Polizei
Deutsche Polizeigewerkschaft im DBB (DPolG)

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Presse

Frankfurter Allgemeine Zeitung GmbH
Süddeutsche Zeitung GmbH
Redaktion NJW
JUVE Verlag für juristische Information GmbH
Redaktion Legal Tribune Online / LTO
Redaktion Anwaltsblatt

juris GmbH
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz ZD
Redaktion heise online
DER SPIEGEL GmbH & Co. KG
Computer und Recht