www.betriebs-berater.de

Betriebs Berater

BB

45 | 2025

Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ...

3.11.2025 | 80. Jg.
Seiten 2561–2624

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Dr. Christian Pisani, LL.M. (London), RA

KI-Compliance: Zur Wechselwirkung von Sorgfaltsmaßstab und Vertrauensschutz beim Einsatz von ChatGPT – Vertrauen schützen, Sorgfalt wahren

Unternehmen nutzen immer häufiger Künstliche Intelligenz (KI). Die Nutzung von ChatGPT stellt sich dabei als Innovationstreiber dar, ist aber gleichzeitig mit Risiken und Limitationen verbunden. Die KI-VO (VO (EU) 2024/1689) gibt insoweit den Regulierungsrahmen vor, ohne selbst ein (abschließendes) Haftungsregime zu schaffen. Vor diesem Hintergrund sollen im folgenden Beitrag Kriterien für die Bestimmung des anwendbaren Sorgfaltsmaßstabes entwickelt werden. Es wird sich zeigen, dass dieser nicht allgemein gültig ist, sondern abhängig vom schutzwürdigen Vertrauen der betroffenen Verkehrskreise. Vertrauen bildet so Grund und Grenze des Sorgfaltsmaßstabs. Diese Erkenntnis kann zur Haftungsminimierung bei der Ausgestaltung interner Prozesse und der Vertragsgestaltung genutzt werden.

I. Einleitung

Sam Altman von Open AI bewirbt ChatGPT-5, das Anfang August 2025 der Öffentlichkeit vorgestellt wurde,[1] als Experten mit Doktortitel auf jedem Gebiet.[2] Insbesondere soll laut Open AI diese jüngste Version von ChatGPT weniger zum Halluzinieren[3] neigen. Im März 2025 waren hingegen noch Bedenken an der Sicherheit von ChatGPT bekannt geworden.[4] Um das volle Potential von ChatGPT auszuschöpfen, bedarf es in dieser Spannungslage also das Wissen und das Verständnis der Nutzer um die technischen Möglichkeiten und die sich daraus ergebenden Innovationschancen, aber auch um die mit der Nutzung verbundenen Risiken und Limitationen. Fehlt es aber an entsprechender KI-Kompetenz im Unternehmen, kann dies mit der Bundesnetzagentur als designierter Marktaufsichtsbehörde[5] eine haftungsbegründende Sorgfaltspflichtverletzung darstellen.[6]

KI-Systeme auf der Basis sog. Large Language Modells (LLMs), wie etwa ChatGPT, Gemini, Llama oder Claude,[7] mit ihrem allgemeinen

1 https://openai.com/de-DE/index/introducing-gpt-5/ (Abruf: 21.10.2025).
2 *Lindner*, in: FAZ vom 9.8.2025, 21.
3 S. zu diesem KI-spezifischen Risiko: III. 2. b) aa).
4 *Cridole*, Concerns raised after OpenAI slashes time taken to test potential risks of latest models, FT Weekend v. 12.4.2025, 11.
5 Zum Gesetzgebungsverfahren des Gesetzes zur Durchführung der KI-Verordnung https://bmds.bund.de/service/gesetzgebungsverfahren/gesetz-zur-durchfuehrung-der-ki-verordnung mit aktuellem Referentenentwurf (Stand: 11.9.2025) (Abruf: 21.10.2025); zu einem älteren Entwurf s. *Wünschelbaum*, MMR 2025, 259.
6 Bundesnetzagentur, Hinweispapier – KI-Kompetenz nach Art. 4 KI-Verordnung (Stand: Juni 2025) (im Folgenden: Hinweispapier) unter https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/7_Kompetenz/start.html (Abruf: 21.10.2025), S. 3.
7 Im Interesse der besseren Lesbarkeit wird im Folgenden von ChatGPT gesprochen, soweit es sich nicht um unterschiedliche LLMs handelt, s. hierzu unter https://digital-strategy.ec.europa.eu/de/faqs/ai-literacy-questions-answers (Abruf: 21.10.2025).

Verwendungszweck werden zunehmend in Geschäftsprozesse integriert. So nutzen zwischenzeitlich 40,9 % deutscher Unternehmen KI.[8] Dabei müssen sie seit dem 2.2.2025 (Art. 113 lit. b) KI-VO) ihren Mitarbeitern gem. Art. 4 der Verordnung über künstliche Intelligenz (KI-VO)[9] entsprechende KI-Kompetenz vermitteln. Gleichwohl wurden bislang erst 20 % der Mitarbeiter geschult,[10] während der großen Mehrheit weiterhin keine KI-Fortbildungen angeboten wurden. KI-Tools bleiben so eine Black Box und deren Output ist für ihre Nutzer letztlich nicht nachvollziehbar. Dies stellt sich als wesentliche Herausforderung für die KI-Compliance dar.

Vor diesem Hintergrund sollen im Folgenden Überlegungen angestellt werden, welchen Sorgfaltsmaßstab Unternehmen beim Einsatz von ChatGPT zu beachten haben und Gestaltungsoptionen zur Haftungsminimierung aufgezeigt werden.

II. Rechtsrahmen

Die KI-VO gilt als Verordnung gem. Art. 288 Abs. 2 AEUV unmittelbar, ohne dass es eines Umsetzungsaktes der einzelnen Mitgliedstaaten bedürfte. Regelungstechnisch fügt sich die Verordnung in den sog. neuen Rechtsrahmen (*new legislative framework*) ein[11] und stellt einen weiteren Baustein im Gefüge des EU-Produktsicherheitsrechts dar.[12] Die KI-VO verfolgt einen risikobasierten Ansatz,[13] indem sie sektorenunabhängig einen möglichst umfassenden Regulierungsrahmen für KI-Systeme statuiert.[14] So begründet die KI-VO für Anbieter, Produkthersteller, Einführer und Händler im Wesentlichen produktbezogene Pflichten,[15] die durch Pflichten für deren Betreiber ergänzt werden. Der Betreiber-Begriff ist dabei in Art. 3 Nr. 4 KI-VO denkbar weit gefasst und erfasst jeden, der in eigener Verantwortung ein KI-System zu beruflichen Zwecken verwendet, wobei den einzelnen Arbeitnehmer keine entsprechenden Pflichten treffen.[16]

Die KI-VO selbst sieht kein eigenes (abschließendes) Haftungsregime vor. Sie wird vielmehr durch die am 8.12.2024 in Kraft getretene Produkthaftungsrichtlinie flankiert,[17] soweit es sich um Schäden durch fehlerhafte Produkte handelt. Die Produkthaftungsrichtlinie erfasst gem. ihrem Art. 4 Nr. 1 (endlich) ausdrücklich auch Software, einschließlich KI-Systeme.[18] Eine angekündigte KI-Haftungsrichtlinie[19] wird hingegen derzeit nicht weiterverfolgt.[20] Dies ist bedauerlich, da beide Richtlinien sich – auch im Selbstverständnis der Kommission – als Gesamtpaket dargestellt haben.[21]

III. Allgemeine Kriterien für die Bestimmung des Sorgfaltsmaßstabes bei der Nutzung von ChatGPT

Mangels eines unionsrechtlich abschließenden Regimes für die Haftung des KI-Betreibers ist auf der Ebene des deutschen Rechts entscheidend, ob diesen eine Sorgfaltspflichtverletzung zur Last fällt. Entsprechende Pflichten können sich aus Vertrag oder Gesetz ergeben.[22] Lässt man Fälle des Vorsatzes sowie einer ausnahmsweise bestehenden verschuldensunabhängigen Garantiehaftung, etwa im Falle der Halterhaftung gem. § 7 StVO, außer Betracht, so setzt dies eine schuldhafte, also zumindest fahrlässige Verletzung voraus, die dem KI-Betreiber zugerechnet werden kann. Damit gewinnt die Bestimmung des für den KI-Betrieb spezifischen Sorgfaltsmaßstabes an überragender Bedeutung.

1. Allgemeine Prinzipien

Im Interesse des Vertrauensschutzes des allgemeinen Rechtsverkehrs geht § 276 BGB bei der Bestimmung des Sorgfaltsmaßstabes von einem objektiv-abstrakten Maßstab aus.[23] Dieser ist gruppenbezogen entsprechend der jeweils betroffenen Verkehrskreise unter Berücksichtigung deren speziellen Anschauungen und Bedürfnissen zu bestimmen,[24] wobei die mit dem jeweiligen Verhalten typischerweise verbundenen Gefahren zu berücksichtigen sind.[25]

Rechtsnormen, (technische) Regelwerke, wie etwa DIN-Normen,[26] können insoweit zur weiteren Ausfüllung herangezogen werden, ohne jedoch einen absoluten Sorgfaltsmaßstab zu begründen.[27] Wenn aufgrund konkreter Umstände im Einzelfall besondere Vorsichtsmaßnahmen angezeigt oder die anzuwendenden (technischen) Regeln erkennbar sicherheitstechnisch unzureichend sind, kann daher mit der Rechtsprechung[28] der verkehrserforderlichen Sorgfalt trotz Befolgung der anwendbaren Regelwerke nicht genügt sein. Andererseits begründet die Nicht-Beachtung nicht schon ohne Weiteres eine Sorgfaltsverletzung, wenn gleichwertige oder bessere sicherheitstechnische Lösungen gewählt wurden. Gleichzeitig haben Regelwerke Indizwirkung.[29] Gebrauchsanweisungen des Herstellers als solche sind hingegen nicht geeignet, den Sorgfaltsmaßstab zu bestimmen, es sei denn sie folgen den o. g. einschlägigen sicherheitsrelevanten technischen Regeln. In einem solchen Fall gelten dieselben gerade angesprochenen Grundsätze.[30]

Zudem ist in der ständigen höchstrichterlichen Rechtsprechung anerkannt, dass derjenige, der eine Gefahrenquelle – gleich welcher Art – schafft, grundsätzlich verpflichtet ist, die notwendigen und zumutba-

8 S. https://www.ifo.de/fakten/2025-06-16/unternehmen-setzen-immer-staerker-auf-kuenstliche-intelligenz (Abruf: 21.10.2025).
9 VO (EU) 2024/1689 vom 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der VO (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der RL 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. L, 2024/1689, 12.7.2024; vgl. zur Historie der KI-VO *Ashkar/Schröder*, BB 2024, 771, 771 f.
10 Bitkom e. V., Presseinformation vom 7.7.2025, unter https://www.bitkom.org/Presse/Presseinformation/Ein-Fuenftel-im-Job-zu-KI-geschult (Abruf: 21.10.2025).
11 Erwägungsgrund 9 der KI-VO.
12 *Rohrßen*, ZfPC 2024, 1111.
13 Erwägungsgrund 26 der KI-VO; *Orssich*, EuZW 2022, 254 ff.
14 *Ashkar/Schröder*, BB 2024, 771 f.; *Stief/Pisani*, in: FS Gassner, 2022, S. 467, 472.
15 S. für Anbieter Art. 16 ff. KI-VO, für Einführer Art. 23 KI-VO oder Händler Art. 24 KI-VO.
16 *Ebers*, in: Ebers/Quarch, Rechtshandbuch ChatGPT, 2024, § 2, Rn. 110 m. w. N. auch zur Gegenansicht.
17 RL (EU) 2024/2853 vom 23.10.2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der RL 85/374/EWG des Rates (Text von Bedeutung für den EWR), ABl. L, 2024/2853, 18.11.2024. Diese ist gem. Art. 22 Abs. 1 Produkthaftungsrichtlinie bis 9.12.2026 in nationales Recht umzusetzen (vgl. hierzu auch der Referentenentwurf des BMJV vom 11.9.2025, https://www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_Produkthaftung.pdf?__blob=publicationFile&v=2 (Abruf: 21.10.2025); allg. zur Produkthaftungsrichtlinie *Wagner*, VersR 2025, 129 ff.
18 S. hierzu Erwägungsgrund 13 der KI-VO.
19 Vorschlag für eine RL des Europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung), COM/2022/496 final, unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex:52022PC0496 (Abruf: 21.10.2025); vgl. hierzu *Wagner*, JZ 2023, 123 ff.; *Staudenmayer*, NJW 2023, 894 ff.
20 Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Arbeitsprogramm der Kommission 2025, KOM(2025) 45 endg., 11.2.2025, Anhang IV. Ziff. 32.
21 *Wagner*, JZ 2023, 123, 127.
22 Allg. *Schaub*, NJW 2023, 2145 ff.
23 Statt aller *Grüneberg*, in: Grüneberg, BGB, 25. Aufl. 2025, § 276 BGB, Rn. 15 m. w. N.
24 *Lorenz*, in: Bamberger u. a., BGB, 5. Aufl. 2023, § 276 BGB, Rn. 22 m. w. N.
25 Statt aller *Grüneberg*, in: Grüneberg, BGB, 25. Aufl. 2025, § 276 BGB, Rn. 15 m. w. N.
26 Vgl. etwa BGH, 11.12.1979 – VI ZR 141/78, NJW 1980, 1219, 1221; BGH, 1.3.1988 – VI ZR 190/87, NJW 1988, 2667.
27 *Lorenz*, in: Bamberger u. a., BGB, 5. Aufl. 2023, § 276 BGB, Rn. 24 m. w. N.
28 BGH, 23.10.1984 – VI ZR 85/83, NJW 1985, 620, 621.
29 *Caspers*, in: Staudinger, BGB, Stand: Oktober 2019, § 276 BGB, Rn. 40 m. w. N.
30 *Caspers*, in: Staudinger, BGB, Stand: Oktober 2019, § 276 BGB, Rn. 41 m. w. N.

ren (organisatorischen) Vorkehrungen zu treffen, eine Schädigung anderer möglichst zu verhindern, und in geeigneter, zumutbarer, ausreichend deutlicher und verständlicher Weise über die entsprechenden Gefahren zu informieren.[31] Dasselbe gilt bei Verwendung weitgehend unerprobter Techniken.[32]

So hat etwa der BGH für die Nutzung von Medizinprodukten[33] zur Bestimmung des von einem Arzt insoweit anzuwendenden fachlichen Standards festgestellt, dass der Arzt zwar nicht mehr alle technischen Einzelheiten der ihm verfügbaren Geräte erfassen vermag. Dies entbinde ihn jedoch nicht von der Pflicht, sich mit der Funktionsweise insbesondere von Geräten, deren Einsatz für den Patienten vitale Bedeutung hat, wenigstens insoweit vertraut zu machen, wie dies einem naturwissenschaftlich und technisch aufgeschlossenen Menschen möglich und zumutbar ist. Ganz unabhängig von der Risikoklassifizierung des jeweiligen Medizinproduktes nimmt der BGH[34] insoweit im Fall erkennbar ernster möglicher Gesundheitsschäden durch deren Einsatz (gesteigerte) Organisations- und Kontrollpflichten an.

Mangels abschließender gesetzlicher Konkretisierung des anwendbaren Sorgfaltsmaßstabes sind es somit letztlich Gerichte, die diesen im Interesse der Einzelfallgerechtigkeit (flexibel) bestimmen. Regelmäßig ist dies für Betreiber aufgrund der damit verbundenen fehlenden Vorhersehbarkeit und der mit den infolge einer ex-post-Beurteilung verbundenen Rückschaufehlern naturgemäß unbefriedigend.[35]

2. Grundsätzliche Anforderungen an den Sorgfaltsmaßstab bei der Nutzung von ChatGPT

Dem Grunde nach stellt sich ChatGPT als technisches Hilfsmittel (zur Vertragserfüllung) dar.[36] Mangels eigener Rechtspersönlichkeit[37] verbleibt es bei der Haftung des jeweiligen Betreibers.[38]

Welche Sorgfaltsanforderungen der Betreiber von ChatGPT im Einzelnen zu erfüllen hat, hängt vom schutzwürdigen Vertrauen der betroffenen Verkehrskreise ab.

a) Vertrauensschutz in regelkonforme Nutzung von ChatGPT

Bei der Bestimmung des Sorgfaltsmaßstabes ist Vertrauen des Rechtsverkehrs ein entscheidendes Kriterium. Auch der Unionsgesetzgeber sieht seinerseits die Notwendigkeit, Vertrauen in die KI aufzubauen und stellt dieses ins Zentrum des Regulierungsrahmens für eine vertrauenswürdige KI (*trustworthy ai*).[39] Das so in der KI-VO statuierte (möglichst) umfassende Pflichtenregime für sämtliche Akteure, einschließlich Betreiber,[40] dient diesem Zweck.

So haben Unternehmen, die ChatGPT nutzen, gem. Art. 4 KI-VO ihrem Personal und den von ihnen beauftragten Personen ausreichend KI-Kompetenz zu vermitteln[41] und Maßnahmen zu ergreifen, gem. Art. 5 KI-VO verbotene Praktiken im KI-Bereich zu verhindern. Sonstige (Vertrags-)Pflichten, etwa aufgrund Datenschutz-, Nichtdiskriminierungs-, Verbraucherschutz-, Wettbewerbsrechts oder Urheberrechts,[42] bleiben im Übrigen unberührt. Diese so statuierten (Organisations-)Pflichten stellen sich als notwendige und zumutbare Vorkehrungen zur Schadensvermeidung dar, zu deren Erfüllung derjenige, der eine Gefahrenlage schafft mit der ständigen höchstrichterlichen Rechtsprechung (s. oben III. 1.) verpflichtet ist. So darf der Rechtsverkehr in schutzwürdiger Weise darauf vertrauen, dass Organisationen, die ChatGPT nutzen, über die erforderlichen Fähigkeiten und Kenntnisse, insbesondere zur Minimierung der jeweiligen KI-spezifischen Risiken, verfügen.[43]

b) KI-spezifische Risiken als Herausforderung für den Vertrauensschutz

Mit dem Einsatz von ChatGPT ist ganz allgemein ein besonderes Autonomie- und Opazitätsrisiko verbunden, das vor dem Hintergrund des Vertrauensschutzes interessengerecht den einzelnen Beteiligten zuzuordnen ist.[44]

aa) Autonomierisiko infolge selbständiger Fehlentscheidungen durch ChatGPT

Unter Autonomierisiko[45] ist die Gefährdungslage infolge autonomer Entscheidungen von KI-Systemen zu verstehen, die zu schadensbegründenden selbständigen Fehleinschätzungen führen können, und die dabei für sämtliche Akteure letztlich zufällig sind.

ChatGPT ist als LLM allein ein Sprachmodell zur Textgenerierung auf der Grundlage eines computerlinguistischen Wahrscheinlichkeitsmodells, das statistische Wort- und Satzfolge-Beziehungen aus einer Vielzahl von Textdokumenten durch einen rechenintensiven Trainingsprozess erlernt hat.[46] Damit verbunden ist das Risiko, dass die KI halluziniert, also Inhalte generiert, die zwar realistisch erscheinen, aber von den vorgegebenen Quelleninputs abweichen. Hierbei ist zwischen fehlender Übereinstimmung (*faithfulness*) oder mangelnder faktischer Richtigkeit (*factualness*) zu unterscheiden.[47] ChatGPT kann somit (bis auf Weiteres) gerade nicht die erzeugten Texte auf ihre Richtigkeit überprüfen. Hierauf weist im Übrigen ChatGPT selbst in den anwendbaren Nutzungsbedingungen hin,[48] schränkt so die Nutzung von ChatGPT ein und begründet im Ergebnis Mitwirkungsobliegenheiten von Nutzern. Ob die Allgemeinen Geschäftsbedingungen (AGB) von ChatGPT insgesamt überhaupt wirksam einbezogen werden und die genannte Klausel einer AGB-rechtlichen Prüfung standhält, bliebe dabei noch einer eingehenden Prüfung vorbehalten.[49]

31 Beispielhaft BGH, 22.5.2025 – VII ZR 157/24, NJW 2025, 2027, 2028 m. w. N.
32 BGH, 24.9.1992 – VII ZR 213/91, BB 1993, 26, NJW-RR 1993, 26.
33 BGH, 11.10.1977 – VI ZR 110/75, NJW 1978, 584, 585 m. w. N.
34 BGH, 15.3.1994 – VI ZR 44/93, NJW 1994, 1594, 1595.
35 *Zech*, ZfPW 2019, 198, 211.
36 Für die Anwaltshaftung *Schnabl*, RDi 2025, 8, 12.
37 *Buchardi*, EuZW 2022, 685, 686 m. w. N.
38 European Commission: Directorate-General for Justice and Consumers, Liability for artificial intelligence and other emerging digital technologies, Publications Office, 2019, unter https://data.europa.eu/doi/10.2838/573689 (Abruf: 21.10.2025), S. 38.
39 Vgl. etwa Erwägungsgrund 6 der KI-VO; Hochrangige Expertengruppe (HEG-KI), unter https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (Abruf: 21.10.2025), S. 5.
40 Hierzu kritisch für Pflichten von Betreibern von Hochrisiko-Systemen *Stief/Pisani*, in: FS Gassner, 2022, S. 467, 479 ff.
41 Webinar zu KI-Kompetenz der Kommission unter https://www.youtube.com/live/Dyf4ZVts9HY (Abruf: 21.10.2025).
42 S. hierzu Erwägungsgründe 28 f., 45, 105 der KI-VO; zum Verbraucherschutz vgl. das Vorabentscheidungsersuchen des Sofiyski rayonen sad (Bulgarien), eingereicht am 25.11.2024 – Yettel Bulgaria EAD/FB (Rs. C-806/24, YETTEL BULGARIA) (C/2025/1080) unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:C_202501080 (Abruf: 21.10.2025), Frage 3 f.
43 Für dieses Erfordernis bei der Bestimmung des Sorgfaltsmaßstabes, statt aller *Grüneberg*, in: Grüneberg, BGB, 84. Aufl. 2025, § 276 BGB, Rn. 15.
44 Allg. *Burchardi*, EuZW 2022, 685 ff.
45 *Staudenmayer*, NJW 2023, 894, 895.
46 Vgl. Wikipedia-Eintrag zu Large Language Model unter https://de.wikipedia.org/wiki/Large_Language_Model (Abruf: 21.10.2025).
47 Allg. hierzu *Farquhar et al.*, Detecting hallucinations in large language models using semantic entropy, Nature 630, 625–630 (2024) unter https://doi.org/10.1038/s41586-024-07421-0 (Abruf: 21.10.2025).
48 Nutzungsbedingungen für Europa (Stand: 29.4.2025) unter dem Stichwort „Genauigkeit", unter https://openai.com/de-DE/policies/terms-of-use/ (Abruf: 21.10.2025).
49 Zu den AGBs einzelner LLM-Anbieter, vgl. *von Appen*, MMR 2025, 330 ff.

bb) Opazitätsrisiko infolge mangelnder Nachvollziehbarkeit

Das Opazitätsrisiko ergibt sich aus der mangelnden Nachvollziehbarkeit von Entscheidungswegen von KI-Systemen.[50]

Dass Entscheidungen auf nicht-nachvollziehbarer Basis getroffen werden, ist infolge Arbeitsteiligkeit nicht ungewöhnlich. Das der KI inhärente Opazitätsrisiko ist also letztlich nicht neu. Die Gefährdungslage ähnelt insoweit unternehmerischen Entscheidungen, bei denen der Vorstand bzw. Geschäftsführer auf einer Informationsgrundlage entscheiden muss, die er aufgrund seiner eigenen Fachlichkeit nicht notwendigerweise in letzter Konsequenz nachvollziehen kann.

Dabei konkretisiert § 93 AktG für das Aktienrecht den Sorgfaltsmaßstab des § 276 Abs. 2 BGB, § 347 Abs. 1 HGB für das einzelne Vorstandsmitglied.[51] Dieses ist infolge der regelmäßig erforderlichen Arbeitsteiligkeit primär Delegationsorgan und trifft Entscheidungen regelmäßig auf der Grundlage von Tatsachen und (rechtlichen) Einschätzungen, die – von Dritten vorbereitet – von den jeweiligen Entscheidungsträgern selbst nicht abschließend ermittelt werden können.[52] Gleichzeitig lässt die Delegation die (Letzt-)Verantwortung der Geschäftsleitung regelmäßig unberührt und ändert allein inhaltlich deren Pflichten. Entscheidend wird damit insbesondere, inwieweit die Geschäftsleitung Informationen vertrauen kann, die sie selbst nicht ermittelt hat,[53] und welcher Sorgfaltsmaßstab an eine insoweit erforderliche Plausibilitätsprüfung zu stellen ist.[54]

Für Rechtsauskünfte gilt mit der höchstrichterlichen Rechtsprechung,[55] dass trotz mangelnder eigener (Rechts-)Kenntnisse ein haftungsbegründendes Verschulden des Organmitglieds zu bejahen ist, wenn dieses einem schuldhaft verursachten Rechtsirrtum unterlegen ist. Es sind insoweit strenge Maßstäbe anzulegen. So hat ein Organmitglied, die Rechtslage sorgfältig zu prüfen, soweit erforderlich Rechtsrat einzuholen und die höchstrichterliche Rechtsprechung sorgfältig zu beachten.[56] Hierbei trifft grundsätzlich den Schuldner das Risiko, die Rechtslage zu verkennen.[57] Entschuldigt ist ein Rechtsirrtum nur dann, wenn der Irrende bei Anwendung der im Verkehr erforderlichen Sorgfalt mit einer anderen Beurteilung durch die Gerichte nicht rechnen musste.[58]

Die Plausibilitätsprüfung soll dabei nicht in einer rechtlichen Überprüfung der erhaltenen Rechtsauskunft bestehen.[59] Sie beinhaltet vielmehr eine Überprüfung, ob dem Berater nach dem Inhalt der Auskunft alle erforderlichen Informationen zur Verfügung standen, er die Informationen verarbeitet hat und alle sich in der Sache für einen Rechtsunkundigen aufdrängenden Fragen widerspruchsfrei beantwortet hat oder sich aufgrund der Auskunft weitere Fragen aufdrängten.[60]

Für Rechtsfragen hat die höchstrichterliche Rechtsprechung so hohe Maßstäbe an die Plausibilitätsprüfung aufgestellt, um eine Enthaftung durch das Einholen von Gefälligkeitsgutachten zu verhindern[61] und betont damit die (Letzt-)Verantwortung des Entscheidungsträgers.

3. Allgemeine Konsequenzen für die Bestimmung des Sorgfaltsmaßstabes

Die KI-VO dient mit ihrem risikobasierten Ansatz der Schaffung eines regulatorischen Rahmens,[62] um die Chancen[63] und Risiken[64] von KI zu nutzen, und begründet insoweit ein abgestuftes Pflichtenregime zur Schaffung vertrauenswürdiger KI (*trustworthy ai*) und deren Nutzung. Dabei lässt der KI-Einsatz sonstige Pflichten des Betreibers jedenfalls unberührt. Gleichzeitig hat der Unionsgesetzgeber im (vorliegenden) Entwurf einer KI-Haftungsrichtlinie bewusst auf die Schaffung einer Gefährdungshaftung des Betreibers[65] verzichtet. Diese gesetzgeberischen Entscheidungen auf Unionsebene dürften bei der weiteren Konkretisierung des Sorgfaltsmaßstabes durch deutsche Gerichte zu berücksichtigen bleiben. Überzogene Anforderungen sollten daher vermieden werden, um so nicht faktisch eine Gefährdungshaftung des Betreibers zu begründen.

Sorgfaltspflichten verbleiben jedenfalls bei den einzelnen Akteuren in der Wertschöpfungskette entsprechend deren jeweiligen Sphären und der damit verbundenen (Organisations-)Verantwortung.[66] Primärer Haftungsadressat sollte dabei der Hersteller sein, nachdem das der KI immanente Opazitäts- bzw. Autonomierisiko letztlich seiner Sphäre zuzuordnen ist.[67]

Gleichzeitig treffen den Betreiber von ChatGPT Schulungspflichten gem. Art. 4 KI-VO. Zudem hat er jedenfalls den Einsatz von ChatGPT für die in Art. 5 KI-VO genannten verbotenen Praktiken auszuschließen sowie seine sonstigen (Vertrags-)Pflichten zu beachten. So darf der Rechtsverkehr darauf vertrauen, dass Betreiber die notwendigen und zumutbaren Vorkehrungen getroffen haben, um eine Schädigung infolge der Nutzung von ChatGPT möglichst zu verhindern. Hierbei ist – außerhalb der sonstigen (Vertrags-)Pflichten – kein absoluter Maßstab anzusetzen, sondern auf die Risikolage im Einzelfall abzustellen (s. oben III. 1.), wobei der Rechtsverkehr mit der ständigen Rechtsprechung[68] zu Verkehrssicherungspflichten aufgrund der Eröffnung einer Gefahrenquelle einen umfassenden Schutz vor jeglicher Schädigung als utopisch nicht erwarten darf. Auch dürfte sich die Nutzung von ChatGPT aufgrund der vergleichsweise hohen Fehleranfälligkeit menschlichen Handelns letztlich als weniger riskant erweisen.[69] Allerdings stellt die Rechtsprechung (s. oben III. 1.), unabhängig von der Risikoklassifikation des eingesetzten Tools auf die jeweilige tatsächliche Gefährdungslage im Einzelfall ab. Dies bleibt bei der Nutzung von ChatGPT zu beachten.

50 *Staudenmayer*, NJW 2023, 894, 895.
51 *Koch*, in: Koch, AktG, 19. Aufl. 2025, § 93 AktG, Rn. 8.
52 *Koch*, in: Koch, AktG, 19. Aufl. 2025, § 93 AktG, Rn. 22 ff. m. w. N.; s. zum KI-Einsatz für unternehmerische Entscheidungen allg. *Langheld/Haagen*, NZG 2023, 1535 ff.
53 *Langheld/Haagen*, NZG 2023, 1535, 1538; zur Delegation schon *Wagner*, BB 2018, 1097, 1098 f.
54 *Buck-Heeb*, BB 2016, 1347 für die Plausibilitätsprüfung bei Vorliegen eines Rechtsrats.
55 BGH, 20.9.2011 – II ZR 234/09, BB 2011, 2960 – Ision I.
56 Vgl. etwa BGH, 11.1.1984 – VIII ZR 255/82, NJW 1984, 1028.
57 BGH, 21.12.1995 – V ZB 4/94, NJW 1996, 1216; BGH, 29.6.2010 – XI ZR 308/09, BB 2010, 2327.
58 BGH, 12.7.2006 – X ZR 157/05, NJW 2006, 3271, 3273, BB 2006, 1819, m. w. N. aus der höchstrichterlichen Rechtsprechung.
59 BGH, 28.4.2015 – II ZR 63/14, BB 2015, 1743, Rn. 48 – Ision II.
60 *Fuhrmann/Heinen/Schilz*, NZG 2020, 1368 ff.
61 *Buck-Heeb*, BB 2016, 1347, 1348 m. w. N.
62 Erwägungsgrund 6 der KI-VO.
63 Zu den vielfältigen Chancen, insb. Erwägungsgrund 4 der KI-VO.
64 Hierzu insb. Erwägungsgrund 5 der KI-VO.
65 So aber noch Europäisches Parlament, Entschließung des Europäischen Parlaments vom 20.10.2020 mit Empfehlungen an die Kommission für eine Regelung der zivilrechtlichen Haftung beim Einsatz künstlicher Intelligenz (2020/2014(INL)), ABl. EU vom 6.10.2021, C-404, S. 107 ff., insb. der hier vorgeschlagene Art. 4 Abs. 1 zur verschuldensunabhängigen Haftung für KI-Systeme mit hohem Risiko.
66 *Wagner*, in: MüKo BGB, 9. Aufl. 2024, § 823 BGB, Rn. 1042 ff.
67 Für den Entwurf der KI-VO *Staudenmeyer*, NJW 2023, 894 ff.; s. hingegen noch die Entschließung des Europäischen Parlaments, die eine primäre Haftungsverantwortung beim Betreiber sah; Europäisches Parlament, Entschließung des Europäischen Parlaments vom 20.10. 2020 mit Empfehlungen an die Kommission für eine Regelung der zivilrechtlichen Haftung beim Einsatz künstlicher Intelligenz (2020/2014(INL)), ABl. EU vom 6.10.2021, C 404, S. 107 ff.
68 *Wagner*, in: MüKo BGB, 9. Aufl. 2024, § 823 BGB, Rn. 528 m. w. N. aus der Rspr.
69 *Burchardi*, EuZW 2022, 685, 687 m. w. N.; *Wagner*, AcP 2017, 707, 709.

Insoweit setzt die Kommission[70] voraus, dass Betreiber von ChatGPT regelmäßig um das Halluzinationsrisiko wissen. Dies stellt ein grundsätzliches Gefahrenpotential dar, das beim Einsatz von ChatGPT jedenfalls zu berücksichtigen sein dürfte, sollten hierdurch vitale Drittinteressen potentiell gefährdet sein. Dabei dürften gleichzeitig die Grundsätze der zum Umfang von Plausibilitätsprüfungen im Aktienrecht ergangenen Rechtsprechung fruchtbar gemacht werden können.[71] Der Betreiber wäre damit nicht verpflichtet, den KI-generierten Inhalt selbst abschließend zu überprüfen, vielmehr würde sich seine Prüfung darauf beschränken können, ob ChatGPT sämtliche für die Erstellung des Inhalts erforderlichen Informationen zur Verfügung standen; Eingabefehler wären aber schon jetzt regelmäßig sorgfaltswidrig. Wann ein relevanter Eingabefehler allerdings überhaupt vorliegt, würde wiederum von einer entsprechenden Bedienungsanleitung, etwa zum Prompting, abhängen, die für den (End-)Nutzer verständlich die maßgeblichen Punkte erklärt und ggf. auf Limitationen der Anwendungsfelder. Dabei bleibt im Lichte des Regelungszwecks der KI-VO, ein möglichst hohes Schutzniveau zu schaffen, abzuwarten, welche Anforderungen der Hersteller hier überhaupt an die Nutzung durch Betreiber stellen und damit Verantwortung haftungsbegrenzend verlagern kann,[72] nachdem das Halluzinationsrisiko letztlich der Herstellersphäre entstammt.[73]

Im Übrigen sieht die Rechtsprechung für den Einsatz neuer und weitgehend unerprobter Technologien Hinweispflichten zum Schutze der betroffenen Verkehrskreise vor und erkennt damit gleichzeitig an, dass Sicherheitserwartungen im Einzelnen – vertraglich im Rahmen des AGB-rechtlich Zulässigen – modifiziert werden können (s. oben III. 1.). Insoweit schafft Transparenz schutzwürdiges Vertrauen und begrenzt dieses gleichzeitig. Ob und inwieweit es sinnvoll sein kann, zur Minimierung des eigenen Haftungsrisikos auf den Einsatz von ChatGPT hinzuweisen, ist vor diesem Hintergrund im Einzelfall zu prüfen (s. unten IV. 2.).

4. Sorgfaltsanforderungen bei Implementierung, Auswahl und Organisation der Nutzung des konkreten LLMs

Um seinen Sorgfaltspflichten zu genügen, hat der Betreiber bei seiner Entscheidung, LLMs einzusetzen, zu klären, ob die Anwendung überhaupt zulässig ist, welches LLM er hierzu auswählt, und schließlich wie er die Nutzung von ChatGPT intern organisiert.

a) Allgemeine Grenzen bei der Implementierung von LLMs

ChatGPT kann in den gesetzlichen Grenzen genutzt werden, wo eine höchstpersönliche Leistungserbringung nicht (ausnahmsweise) geschuldet ist.[74] Grenzen können sich etwa aus Art. 22 DSGVO, der ausschließlich automatisierte Entscheidungen einschränkt, soweit diese nicht ausnahmsweise zulässig sind,[75] oder für unternehmerische Entscheidungen[76] ergeben. Die Möglichkeit, ChatGPT als Werkzeug bei der Erzeugung von Inhalten als Grundlage für die eigene Entscheidung bzw. Leistung zu nutzen, bleibt unberührt.

Für Hochrisiko-KI-Systeme ergeben sich mit Art. 26 Abs. 2 KI-VO Grenzen aufgrund der Verpflichtung des Betreibers, qualifiziertem Personal die menschliche Aufsicht über die KI zu übertragen. Grundsätzlich unterliegt die Nutzung von ChatGPT zwar nicht diesen Beschränkungen, wird ChatGPT jedoch als Hochrisiko-KI,[77] etwa zur (automatisierten) Sortierung von Lebensläufen im Einstellungsprozess, genutzt, so gilt es, dies zu beachten.[78]

Vor Einführung von ChatGPT in einer Organisation ist somit grundsätzlich zu klären, ob und ggf. inwieweit der Betreiber (vertraglich) hierzu überhaupt berechtigt ist. Unabhängig davon bleibt zu beachten, dass dessen Verantwortung für Schäden durch den Einsatz von ChatGPT unberührt bleibt (s. oben III. 2.).

So hat das LG Kiel[79] für einen Wirtschaftsinformationsdienst, der KI-generierte Inhalte veröffentlichte, entschieden, dass sich dieser nicht mit Verweis auf seine Unkenntnis der konkret generierten Inhalte seiner haftungsrechtlichen Verantwortung entziehen könnte. Auch ein entsprechender in den Nutzungsbedingungen pauschal formulierter Haftungsausschluss würde – allein schon mit Blick auf den Grundsatz von Treu und Glauben gem. § 242 BGB[80]– hieran nichts ändern. Dies gilt umso mehr, als KI ohnehin regelmäßig allein im Rahmen der gesetzlichen Grenzen zur Anwendung kommen darf.[81]

Vor diesem Hintergrund hat der Betreiber nach Anwendungsfeldern zu differenzieren und insoweit eine entsprechende Risikoanalyse anzustellen. Hierbei hat er das mögliche Schadenspotential für die jeweils betroffenen Rechtsgüter mit der Eintrittswahrscheinlichkeit in Kenntnis der konkreten Gefährdungslage, allgemein insbesondere aufgrund von Halluzinationen sowie des im Einzelfall verwandten LLMs, gegeneinander wertend abzuwägen. Dies erweist sich dann als problematisch, wenn der Betreiber nicht in der Lage ist, die mit dem Einsatz verbundenen Risiken überhaupt dem Grunde nach zu evaluieren, nachdem die Nutzung einer nicht kalkulierbaren Risikoquelle sich als (haftungsbegründende) Sorgfaltspflichtverletzung darstellt.[82]

Für Hochrisiko-KI-Systeme sieht Art. 13 Abs. 2 KI-VO vor, dass diese mit Betriebsanleitungen zu versehen sind, die präzise, vollständige, korrekte und eindeutige Informationen in einer für die Betreiber relevanten, barrierefrei zugänglichen und verständlichen Form enthalten. Vor diesem Hintergrund sind die seit 2.8.2025 geltenden (Art. 113 lit b) KI-VO) in Art. 53 Abs. 1 KI-VO statuierten Informations- und Dokumentationspflichten des Anbieters von KI-Modellen mit allgemeinem Verwendungszweck in ihrer Bedeutung nicht zu unterschätzen. Diese werden ergänzt durch unverbindliche Leitlinien der Kommission[83] als Auslegungshilfe sowie dem auf Freiwilligkeit basieren-

70 Kommission, unter https://digital-strategy.ec.europa.eu/de/faqs/ai-literacy-questions-answers (Abruf: 21.10.2025).
71 Für Unternehmensentscheidungen ist allerdings zumindest strittig, ob und inwieweit die Grundsätze der Ision-Rechtsprechung allg. auf den KI-Einsatz im Rahmen der vertikalen Delegation übertragbar sind; vgl. hierzu kritisch *Koch*, in: Koch, AktG, 19. Aufl. 2025, § 93 AktG, Rn. 24 auch m. w. N. zur Gegenansicht; zur Kritik und einem Alternativansatz, insb. *Langheld/Haagen*, NZG 2023, 1535 ff.
72 In diese Richtung dürften Ausführungen in der Zusammenfassung des Vorabentscheidungsersuchen des Sofiyski rayonen sad (Bulgarien), eingereicht am 25.11.2024 – Yettel Bulgaria EAD/FB (Rs. C-806/24, YETTEL BULGARIA) (C/2025/1080) unter https://curia.europa.eu/juris/showPdf.jsf?text=&docid=294955&pageIndex=0&doclang=de&mode=req&dir=&occ=first&part=1&cid=3754077 (Abruf: 21.10.2025), Rn. 26, zielen.
73 *Staudenmeyer*, NJW 2023, 894 ff.
74 Zur Leistungserbringung im Arbeitsrecht gem. § 613a BGB *Batista*, LTZ 2024, 118, 119 m. w. N.
75 EuGH, 7.12.2023 – C-26/22 u. C-64/22, BB 2024, 270.
76 *Koch*, in: Koch, AktG, 19. Aufl. 2025, § 93 AktG, Rn. 23 unter Verweis auf § 76 AktG Rn. 10 ff. zum grundsätzlichen Verbot der vertikalen Delegation.
77 S. hierzu Anh. III der KI-VO.
78 Anh. III der KI-VO: Nr. 4; vgl. auch Wissenschaftlicher Dienst, Maßnahmen der EU zur Regulierung von KI (Stand: 27.2.2025), unter https://www.bundestag.de/resource/blob/1065332/EU-6-001-25-pdf.pdf. (Abruf: 21.10.2025), S. 15.
79 LG Kiel, 29.2.2024 – 6 O 151/23, MMR 2025, 227 ff.
80 *Rolfes/Engeler*,ZD 2024, 496, 499 f.
81 *Langheld/Haagen*, NZG 2023, 1535, 1537 m. w. N.
82 *Zech*, PfPW 2019, 198, 210.
83 Kommission, Leitlinien zum Umfang der Verpflichtungen für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck nach dem KI-Gesetz (Stand: 18.7.2025) unter

den KI-Verhaltenskodex für allgemeine Zwecke.[84] Die so geschaffenen Transparenzpflichten soll es Anbietern von KI-Systemen ermöglichen, wiederum ihre eigenen Transparenz- und Informationspflichten gegenüber ihren (End-)Kunden zu erfüllen. Auf diese Weise dürften perspektivisch so – zumindest indirekt – Standards gesetzt werden, die für die Risikoinformation gegenüber Betreibern von Hochrisiko-KI-Systemen zu erfüllen sind, um diese in die Lage zu versetzen, ihrerseits die erforderliche Risikoanalyse anzustellen. Es bleibt abzuwarten, was dies für Betreiber von ChatGPT bedeuten wird.

Im Ergebnis muss ein Betreiber also insbesondere die Relevanz des mit Halluzinationen verbundenen Risikos, unzuverlässige Informationen seinen Entscheidungen zugrunde zu legen, für die Frage gewichten, ob im konkreten Anwendungsfeld überhaupt ChatGPT verwendet werden kann. Hierbei wären – entsprechend der Wertungen der KI-VO – die Bedeutung der betroffenen Rechtsgüter und die Risikoeintrittswahrscheinlichkeit zu bewerten.[85]

b) Auswahl des konkreten LLM für das jeweilige Anwendungsfeld

LLMs sind aufgrund ihrer Ausgestaltung und Leistungsfähigkeit für einzelne Anwendungsfelder unterschiedlich gut geeignet. Sie unterscheiden sich hierbei, insbesondere aufgrund der zugrundeliegenden Trainingsdaten, wobei deren jeweilige Sprachfassungen mit ihren entsprechenden semantischen Unterschieden abhängig vom Einsatzfeld einen Einfluss auf den Output der KI haben können.[86]

Dies gilt etwa für den KI-Einsatz in der Rechtsberatung, bei der naturgemäß die Beachtung sprachlicher Besonderheiten der jeweiligen Rechtsordnungen entscheidend für die Qualität der erzeugten Inhalte ist.[87] Ganz allgemein gilt für die Rechtsberatung, dass die verwandten LLMs (bislang) besonders anfällig für das Halluzinieren sind.[88] Zudem können vor Inverkehrbringen der jeweiligen LLMs diese unterschiedliche Sicherheits-Checks durchlaufen haben mit ggf. negativen Auswirkungen auf deren Risikoprofil.[89] Schließlich können datenschutzrechtliche Fragen bei der Auswahl zu beachten sein, die sich im Zusammenhang mit dem Hosting ergeben können.[90]

c) Organisation der Nutzung von ChatGPT

Ein Betreiber muss bei der Gestaltung seiner Organisation die notwendigen und zumutbaren Vorkehrungen treffen, eine Schädigung infolge der Nutzung von ChatGPT möglichst zu verhindern.[91] Hierzu hat er seinem Personal und den von ihm Beauftragten, die für die Nutzung von ChatGPT (zur Vertragserfüllung) erforderlichen Fähigkeiten und Kenntnisse zu vermitteln, insbesondere in (Schulungs-)Maßnahmen gem. Art. 4 KI-VO.[92] So ist zu gewährleisten, dass Nutzer von ChatGPT fundierte Entscheidungen im Anwendungsfall treffen und damit im Interesse des Vertrauensschutzes die angemessene Einhaltung und die ordnungsgemäße Durchführung der KI-VO sichergestellt ist.[93]

IV. Gestaltungsoptionen zur Haftungsminimierung

Einen allgemeinen Sorgfaltsmaßstab kennt das deutsche Recht nicht, vielmehr ist dieser im Einzelfall unter Berücksichtigung des Vertrauens der betroffenen Verkehrskreise in die gesetzeskonforme Nutzung von ChatGPT zu bestimmen. Zur möglichen Haftungsminimierung ist dies beim Aufbau entsprechender Governance-Strukturen und deren Dokumentation, zu berücksichtigen. Dem Grunde nach kann dabei der Sorgfaltsmaßstab vertraglich modifiziert werden, wobei schutzwürdige Interessen Dritter hiervon jedenfalls unberührt bleiben.

1. Governance und Dokumentation

Art. 26 KI-VO statuiert Governance- und Dokumentationspflichten allein für Betreiber von Hochrisiko-KI-Systemen. Diese Pflichten gelten damit nicht für Betreiber von ChatGPT, solange sie dieses nicht als Hochrisiko-KI-System für die in Anlage III genannten Zwecke, etwa im Recruiting, nutzen.

Unabhängig von der Risikoklassifikation bestehen jedoch Organisationspflichten des Betreibers. Insoweit hat der Betreiber gem. Art. 4 KI-VO die Pflicht, seinem Personal und sonstige von ihm Beauftragte ausreichende KI-Kompetenzen zu vermitteln. Im Interesse der Flexibilität sieht die KI-VO bewusst kein spezifisches Format oder einen sonstigen formalisierten und standardisierten Maßnahmenkatalog, etwa die Einführung eines KI-Beauftragten, vor.[94] Gleichzeitig dürfte es wegen der KI-spezifischen Risiken[95] unzureichend sein, sich als Betreiber für die Vermittlung von KI-Kompetenzen allein auf die Gebrauchsanweisung der KI-Systeme zu verlassen oder Mitarbeiter lediglich zu bitten, diese zu lesen, vielmehr dürften mit der Kommission entsprechende Schulungen und Leitlinien bereitzustellen sein.[96] Insoweit gibt die Kommission mit ihren entsprechenden Leitfragen Hinweise für die Ausgestaltung solcher unternehmensinternen KI-Kompetenzvermittlung[97] und verweist zudem auf unverbindliche Best-Practice-Beispiele.[98] Daneben benennt die Bundesnetzagentur in ihrem Hinweispapier Grundsteine, die sie für den Aufbau von KI-Kompetenz als geeignet erachtet: Entsprechend allgemeinen Compliance-Programmen reichen diese von der individuellen Bedarfsermittlung über die hierauf aufbauende Ausgestaltung von konkreten Maßnahmen, etwa im Hinblick auf den Kontext des KI-Einsatzes, bis zur

https://digital-strategy.ec.europa.eu/de/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act (Abruf: 21.10.2025).

84 KI-Verhaltenskodex für allgemeine Zwecke unter https://digital-strategy.ec.europa.eu/de/policies/contents-code-gpai (Abruf: 21.10.2025).

85 Zu möglichen (vertraglichen) Gestaltungsmöglichkeiten zur Haftungsminimierung, s. unten IV. 2.

86 *Sobieska/Starke*, The American Journal of Bioethics, 2025, S. 82 ff., die auf die möglichen Auswirkungen eines *language bias* verweisen.

87 *Jung*, in: FAZ vom 7.6.2025, 24, zum Markteintritt einer französischen legal-tech-Plattform in den deutschen Markt.

88 Für das dt. Recht s. AG Köln, 2.7.2025 – 312 F 130/25, Rn. 23 f. unter https://nrwe.justiz.nrw.de/ag_koeln/j2025/312_F_130_25_Beschluss_20250702.html (Abruf: 21.10.2025); für das US-amerikanische case law *Dahl u. a.*, Journal of Legal Analysis (2024), 64 ff., unter https://doi.org/10.1093/jla/laae003 (Abruf: 21.10.2025).

89 *Cridole*, Concerns raised after OpenAI slashes time taken to test potential risks of latest models, FT Weekend vom 12.4.2025, 11.

90 Gerade im Fall von DeepSeek bestehen hier Vorbehalte. Vgl. auch Empfehlung des niedersächsischen Landesdatenschutzbeauftragten unter https://www.lfd.niedersachsen.de/ki/empfehlung-des-lfd-niedersachsen-zum-einsatz-von-deepseek (Abruf: 21.10.2025).

91 Zu KI-Richtlinien und KI-Rahmenbetriebsvereinbarungen allg. *Pepping*, BB 2025, 1269 ff.

92 Kommission, unter https://digital-strategy.ec.europa.eu/de/faqs/ai-literacy-questions-answers (Abruf: 21.10.2025).

93 Insoweit auch Bundesnetzagentur, Hinweispapier, unter https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/_functions/Hinweispapier.pdf?__blob=publicationFile&v=2 (Abruf: 21.10.2025) S. 3.

94 Kommission, unter https://digital-strategy.ec.europa.eu/de/faqs/ai-literacy-questions-answers (Abruf: 21.10.2025); Bundesnetzagentur, Hinweispapier unter https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/_functions/Hinweispapier.pdf?__blob=publicationFile&v=2 (Abruf: 21.10.2025) S. 3 ff.

95 S. oben III. 2. b).

96 Kommission, unter https://digital-strategy.ec.europa.eu/de/faqs/ai-literacy-questions-answers (Abruf: 21.10.2025).

97 Kommission, unter https://digital-strategy.ec.europa.eu/de/faqs/ai-literacy-questions-answers (Abruf: 21.10.2025).

98 Kommission, Veröffentlichung vom 4.2.2025, unter https://digital-strategy.ec.europa.eu/de/library/living-repository-foster-learning-and-exchange-ai-literacy (Abruf: 21.10.2025).

regelmäßigen Auffrischung und Dokumentation der durchgeführten Maßnahmen.[99]

Im Lichte der gesetzgeberischen Entscheidung, formalisierte Governance- und Dokumentations-Strukturen allein für den Betrieb von Hochrisiko-KI-Systeme vorzusehen, sprechen gute Gründe dafür, keine allzu überzogenen Anforderungen für die Nutzung von ChatGPT zu stellen. Dies wird die Rechtsprechung bei der weiteren Konkretisierung der Anforderungen im Rahmen von Art. 4 KI-VO zu berücksichtigen haben.

2. Transparenz zur Qualifikation der Sicherheitserwartungen bei der Nutzung von ChatGPT

Welchen Einfluss der Einsatz von ChatGPT auf die erzeugten Inhalte hat, hängt vom jeweiligen Einsatzfeld ab: KI kann dabei sowohl zur Steigerung der Qualität wie zu deren Minderung, insbesondere infolge Halluzinierens, führen.

Im Lichte der höchstrichterlichen Rechtsprechung zu Aufklärungs- und Hinweispflichten beim Einsatz neuer und weitgehend unerprobter Technologien[100] stellt sich entsprechende Transparenz im Vertragsverhältnis als probates Mittel dar, das Vertrauen des Vertragspartners zu modifizieren, und so den Sorgfaltsmaßstab – in den Grenzen des Rechts der Allgemeinen Geschäftsbedingungen – zu modifizieren. Es kann also sinnvoll sein, ganz unabhängig von Transparenzpflichten gem. Art. 50 Abs. 4 KI-VO für Betreiber bei Veröffentlichung von mithilfe von KI erzeugten Deepfakes im Sinne des Art. 3 Nr. 60 KI-VO bzw. für den öffentlichen Diskurs bestimmte Informationen, auf die KI-Verwendung und die sich hieraus ergebenden Konsequenzen hinzuweisen.[101] Die mit dem KI-Einsatz verbundenen Chancen und Risiken wären so einem (potentiellen) Vertragspartner bekannt und im Falle deren Verwirklichung eine haftungsrechtlich relevante Sorgfaltspflichtverletzung damit letzlich schwer begründbar.

Im Fall der Erbringung (anwaltlicher) Beratungsleistungen könnte damit etwa darauf hingewiesen werden, dass bei der Sachverhaltsermittlung[102] auf ChatGPT zurückgegriffen wurde.[103] Dies kann bei der Verarbeitung großer Datenmengen, z. B. in M&A-Transaktionen oder komplexen Streitverfahren, einen (erheblichen) Effizienzgewinn darstellen und gleichzeitig mit einer Kostenreduktion verbunden sein. Allerdings besteht die Gefahr, dass die (anwaltliche) Beratung ggf. auf der Grundlage eines nicht zutreffend bzw. nicht vollständig ausermittelten Sachverhalts erbracht wird. Die (anwaltliche) Beratung wäre hier etwa als sog. Red Flag Due Dilligence auf Dealbreaker vertraglich zu beschränken, wo nur auf die die Transaktion gefährdende Risiken geprüft werden würde.[104]

Grenzen der Vertragsgestaltung ergeben sich jedenfalls dort, wo Drittinteressen betroffen sind, da die Verwendung von ChatGPT die allgemein geltende haftungsrechtliche Verantwortung des Betreibers unberührt lässt.[105] Nutzt ein Betreiber ChatGPT etwa beim Verfassen von Werbetexten,[106] kann sich dies zwar als eine kostenoptimierte Option für einen Kunden darstellen. Gleichzeitig gehen damit (rechtliche) Risiken, etwa aus dem Urheberrecht, dem Verbraucherschutzrecht oder dem Wettbewerbsrecht[107] einher, die im Außenverhältnis nicht zulasten der hierdurch geschützten Personenkreise ausgeschlossen werden können.[108] Im Innenverhältnis könnte hier zwar mit Freistellungsansprüchen bzw. der Beschränkung des Leistungsversprechens – jeweils im Rahmen des AGB-rechtlich Zulässigen – das Haftungsrisiko des Betreibers gegenüber dem jeweiligen Kunden minimiert werden; Ansprüche geschützter Dritter können so jedoch nicht wirksam modifiziert werden oder diese gänzlich ausschließen.

V. Fazit und Ausblick

Die Nutzung von ChatGPT birgt Chancen und Risiken. Die KI-VO hat sich insoweit zum Ziel gesetzt, einen Rechtsrahmen für die verantwortungsvolle Nutzung vertrauenswürdiger KI zu schaffen, ohne dabei einen allgemein gültigen Sorgfaltsmaßstab zu statuieren. Schutzwürdiges Vertrauen der von KI-Einsatz Betroffenen und Bestimmung des anwendbaren Sorgfaltsmaßstabes stehen insoweit in einer Wechselwirkung: Die Allgemeinheit darf dabei einerseits auf die gesetzeskonforme Nutzung von ChatGPT vertrauen, andererseits besteht die Möglichkeit dieses Vertrauen im Vertragsverhältnis zu modifizieren.

Daher sollten Betreiber, um ihr mit der Nutzung von ChatGPT einhergehendes Haftungsrisiko zu minimieren, einerseits ausreichende KI-Kompetenz ihres Personals und der von ihnen Beauftragten aufbauen und andererseits die Möglichkeiten der Vertragsgestaltung – innerhalb des AGB-rechtlich Zulässigen – nutzen.

Es gilt daher schon jetzt

- Entscheidungen bezüglich des Einsatzes und der Nutzung von LLMs nachvollziehbar und dokumentiert zu treffen,
- allgemeine KI-Kompetenzen im Unternehmen strukturiert aufzubauen und
- bestehende Verträge und Vertragsmuster für Leistungen, bei denen ChatGPT zum Einsatz gelangt, zu überprüfen und ggf. zu überarbeiten.

Dr. Christian Pisani, LL.M. (London), RA, in München tätig, Dozent im Versicherungsrecht an der Hagen Law School und lehrt u. a. KI-Themen im Masterstudiengang Medizinethik der Johannes Gutenberg-Universität Mainz.

Hinweis der Redaktion:
Lesen Sie zum Thema KI auch den Beitrag *Risse/Weiß*, Der Robo-Judge und Fluggastfälle: Mehr als eine Utopie?, BB 2025, 1731 ff.

99 Bundesnetzagentur, Hinweispapier, unter https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/_functions/Hinweispapier.pdf?__blob=publicationFile&v=2 (Abruf: 21.10.2025) S. 4 f.
100 BGH, 24.9.1992 – VII ZR 213/91, BB 1993, 26, NJW-RR 1993, 26 m. w. N. aus der höchstrichterlichen Rechtsprechung.
101 Für die Rechtsberatung etwa *Gasteyer*, AnwBl Online 2024, unter https://anwaltsblatt.anwaltverein.de/files/anwaltsblatt.de/Dokumente/2024/anwbl-online-2024-270-gasteyer.pdf (Abruf: 21.10.2025), 270, 274.
102 *Schnabl*, RDi 2025, 8, 11 unter Hinweis auf die Rspr.; *Thole/Rolff*, Anwaltsblatt 2025, 13, 14.
103 *Thole/Rolff*, Anwaltsblatt 2025, 13, 14.
104 *Schnabl*, RDi 2025, 8, 11.
105 S. oben III. 2. a.
106 Kommission, unter https://digital-strategy.ec.europa.eu/de/faqs/ai-literacy-questions-answers (Abruf: 21.10.2025).
107 Erwägungsgrund 45 der KI-VO.
108 S. oben III. 1.