Haftungsrisiken und Urheberrecht beim Einsatz von KI

Wissenschaftliche Ausarbeitung im Modul Master-Projekt:
Wirtschaftsrecht im Transfer

vorgelegt von

Nasin Akin 1261844

Nadine Möllenkamp 50131307

Britta Sirges 1187278

Angefertigt im Studiengang Wirtschaftsrecht (LL.M.)
an der Hochschule Bielefeld,
Fachbereich Wirtschaft

Sommersemester 2025

Erstprüferin: Prof. Dr. jur. Christiane Nitschke
Zweitprüfer: Prof. Dr. jur. Daniel Antonius Hötte

Inhaltsverzeichnis

Abkürzungsverzeichnis

DSFA	Datenschutz-Folgeabschätzung
KI	Künstliche Intelligenz
KI-System	System künstlicher Intelligenz
KI-VO	VO (EU) 2024/1689: Verordnung über künstliche Intelligenz
LLM	Large Language Models
ProdHaftRL	Richtlinie (EU) 2024/2853

Bezüglich der weiteren verwendeten Abkürzungen wird verwiesen auf:

Kirchner	Abkürzungsverzeichnis der Rechtssprache, 11. Aufl., Berlin 2024.

A. Einleitung

In Unternehmen können KI-basierte Systeme in unterschiedlichen betrieblichen Bereichen zum Einsatz kommen. Der zunehmende Einsatz bringt vielfältige rechtliche Herausforderungen mit sich. Im Fokus stehen dabei insbesondere Haftungsrisiken, Datenschutzverletzungen, Urheberrechtsverstöße sowie die Anforderungen der neuen KI-Verordnung (VO (EU) 2024/1689). Die folgende Ausarbeitung gibt einen Überblick über die praktischen Auswirkungen des Einsatzes von Bildverarbeitungssystemen zur automatisierten Sichtkontrolle in der Produktion, KI-Chatbots im Marketing sowie generativen KI-Tools zur automatisierten Codeerzeugung in der Softwareentwicklung. Zudem werden die gesetzlichen Anforderungen dargestellt und entsprechende Handlungsempfehlungen abgeleitet.

B. Anforderungen der KI-VO

Mit dem Inkrafttreten der KI-VO am 1. August 2024 wurde auf europäischer Ebene ein Rechtsrahmen für KI-Systemen geschaffen. Zentrales Element ist die Einteilung von KI-Systemen in vier Risikokategorien: unannehmbares, hohes, begrenztes und minimales Risiko.

I. Risikoklassifizierung und Pflichten

Für die betriebliche Anwendungspraxis sind vor allem die Hochrisiko- und begrenzt riskanten Systeme relevant. Eine Hochrisiko-KI i.S.d Art. 6 – 29a i.V.m. Anhang 1,3 KI-VO liegt dann vor, wenn Systeme in sicherheitskritischen Bereichen eingesetzt werden oder rechtliche Auswirkungen auf betroffene Personen haben, etwa im Bereich von Justiz, Bildung oder kritischer Infrastruktur. Demnach liegt exemplarisch bei KI-gestützten internen Sichtkontrollen in der Produktion kein Hochrisikosystem vor, wenn die Produkte nicht sicherheitskritisch sind und kein direkter Eingriff in sicherheitsrelevante Entscheidungen erfolgt. Ferner sind KI- Chatbots sowie generative KI-Tools zur Codeerzeugung nicht dem Anhang zuzuordnen. Dennoch ist bei Weiterentwicklungen der KI eine kontinuierliche Bewertung erforderlich. Schon eine wesentliche Modifikation eines KI-Systems kann eine erneute Risikoklassifizierung und Rollenver-

schiebung auslösen und damit zusätzliche regulatorische Pflichten begründen.[1] Denn die KI-VO differenziert zwischen Anbieter- und Betreiberpflichten. Anbieter unterliegen dem vollständigen Pflichtenkatalog nach Art. 8ff. KI-VO, u.a. mit Anforderungen an Risikomanagement, Transparenz, Qualitätssicherung und Nachverfolgbarkeit. Betreiber hingegen nutzen ein fertiges System im vorgegebenen Zweck und sind nach Art. 3 Nr. 4, Art. 26 KI-VO verpflichtet, dieses entsprechend den Anweisungen sicher zu verwenden. Liegt keine Hochrisiko-KI vor, könnte das KI-System ein begrenztes Risiko aufweisen. Begrenzte Risiken liegen bei Systemen vor, die zwar keine Grundrechte gefährden, aber direkt mit natürlichen Personen interagieren oder synthetische Inhalte erzeugen. Dies ist etwa bei einem Chatbot oder einer Codegenerierung in der Softwareentwicklung der Fall. Für diese Systeme gelten ab dem 2. August 2026 nach Art. 50 KI-VO Transparenzanforderungen: Nutzern ist verständlich mitzuteilen, dass sie mit einer KI-Anwendung interagieren. Ferner sind KI-generierte Inhalte eindeutig als solche zu kennzeichnen. Zur Einhaltung dieser Vorgaben ist eine Umsetzung entsprechender Hinweise z. B. über Hinweisfenster oder Wasserzeichen notwendig. Zusätzlich sollten Arbeitsanweisungen festlegen, in welchen Fällen menschliche Kontrolle verpflichtend ist.[2]

II. Handlungsempfehlung zur operativen Umsetzung

Unabhängig von der Risikoklassifizierung verpflichtet Art. 4 KI-VO Unternehmen dazu, sicherzustellen, dass eine KI-Kompetenz entwickelt wird. Zielgerichtete Schulungen sind hierfür geeignete präventive Maßnahmen.[3] Zur operativen Umsetzung empfiehlt sich die Einführung eines KI-Compliance-Systems, das zentrale Anforderungen wie Risikobewertung, Dokumentationspflichten, Zuständigkeiten und technische Prüfungen systematisch abbildet und Schnittstellen zu anderen Rechtsgebieten integriert. Bestehende Strukturen, etwa Compliance- oder Datenschutzmanagementsysteme, können erweitert werden. Zudem sollten alle eingesetzten KI-Systeme in einem zentralen Verzeichnis erfasst und hinsichtlich Rolle und Risikokategorie geprüft werden. Eine frühzeitige Dokumentation sowie laufendes Monitoring sind entscheidend, um rechtliche Anforderungen dauerhaft zu erfüllen und Projektrisiken zu

1 Förster/Gehrmann SPA 2024, 113 (114).

2 Ebers, in: SWK Legal Tech, 80. Regulierung (EU), KI VO Rn. 17; Kumkar/Griesel, KIR 2024, 117.

3 Klos/Taylan, CCZ 2024, 205 (210).

vermeiden.[4] Zwar können aus der KI-VO Bußgelder folgen, jedoch ergeben sich daraus nicht unmittelbar Haftungstatbestände. Diese richten sich weiterhin nach den bestehenden gesetzlichen Regelungen, insbesondere der Produkthaftung, sowie der zivil- und deliktischen Haftung.[5]

C. Haftungsrisiken in der Produktion

Insbesondere im Bereich der Produktion ergeben sich beim Einsatz von KI-Systemen verschiedene Haftungsrisiken, die berücksichtigt werden müssen. Kommt eine automatisierte Sichtkontrolle durch ein KI-System zu einem falschen Ergebnis und bewertet ein fehlerhaftes Produkt als einwandfrei, könnten Schadensersatzansprüche entstehen, wenn durch das fehlerhafte Produkt ein Schaden entsteht.

I. Produkthaftung

Die Produkthaftung regelt die Haftung bei fehlerhaften Produkten. Zu beachten ist, dass kein Verschulden erforderlich ist. Das deutsche ProdHaftG basiert auf der europäischen Richtlinie 85/374/EWG. Diese Richtlinie wurde mit Veröffentlichung am 23. Oktober 2024 von der neuen Richtlinie (EU) 2024/2853 abgelöst. Die Vorgaben dieser neuen Richtlinie muss der deutsche Gesetzgeber bis zum 9. Dezember 2026 in das nationale Recht umgesetzt haben. Davon betroffen sind vor allem der Produktbegriff und die Definition eines Fehlers.

1. Produkt

Die neue Produkthaftungsrichtlinie erweitert den Produktbegriff. Neben den beweglichen Sachen gem. § 2 ProdHaftG, also allen körperlichen Gegenständen, nennt die ProdHaftRL in Art. 4 Nr. 1 nun digitale Konstruktionsunterlagen und Software als Produkte.[6] „Digitale Konstruktionsunterlage" meint gem. Art. 4 Nr. 2 ProdHaftRL eine digitale Darstellung oder Vorlage einer beweglichen Sache, die die für die Produktion eines körperlichen Gegenstandes notwendigen funktionalen Informationen enthält, indem sie eine automatische Steuerung von Maschinen oder Werkzeugen ermöglicht. Beispiele für Software sind in Erwägungsgrund 13 ProdHaftRL genannt: Betriebssysteme, Computerprogramme und auch KI-Systeme.

---

4 Chibanguza/Steege NJW 2024, 1769 (1773).

5 Klos/Taylan, CCZ 2024, 205 (209).

6 *Wagner*, in: MüKo BGB § 2 ProdHaftG Rn. 4.

2. Fehler

Bei der Beurteilung, ob ein Produkt fehlerhaft ist, kommt es gemäß § 3 Abs. 1 ProdHaftG darauf an, ob die berechtigten Sicherheitserwartungen erfüllt werden. Dabei müssen alle Umstände berücksichtigt werden. Im Einzelnen bedeutet das: Unter der Darbietung nach lit. a) ist neben der äußeren Gestaltung eines Produkts auch jede Produktbeschreibung und -werbung und die Gebrauchsanweisung zu verstehen.[7] Die Produktsicherheit kann nur für den Gebrauch sichergestellt werden, mit dem billigerweise gerechnet werden kann (§ 2 Abs. 1 lit. b)). Das bedeutet, dass nur solche Verwendungen umfasst sind, die bei vernünftiger Betrachtung typischerweise zu erwarten sind. Dazu zählt u.a. auch ein vorhersehbarer Fehlgebrauch des Produkts.[8] Zeitpunkt der Beurteilung ist gemäß lit. c) derjenige, in dem das Produkt in den Verkehr gebracht wurde. Ein Produkt, das einmal fehlerfrei war, kann nicht nachträglich als fehlerhaft gelten.[9] Art. 7 Abs. 2 ProdHaftRL entspricht weitgehend § 3 Abs. 1 ProdHaftG und stellt ebenfalls auf die berechtigten Sicherheitserwartungen ab. Allerdings erweitert die Richtlinie den Katalog der Umstände, die bei der Bewertung eines Produktfehlers zu berücksichtigen sind. In Art. 7 Abs. 2 lit. c) ProdHaftRL explizit erwähnt ist nun die Fähigkeit des Produkts, nach seinem Inverkehrbringen oder seiner Inbetriebnahme weiter zu lernen oder neue Funktionen zu erwerben. Mit dieser Regelung wird nun speziell auf KI-Systeme in Form von Software Bezug genommen.[10] Darüber hinaus kann nach Art. 7 Abs. 2 lit. f) ProdHaftRL auch das Nichteinhalten von Anforderungen an die Produktsicherheit, einschließlich Cybersicherheitsanforderungen, zur Fehlerhaftigkeit führen. Das Produkthaftungsgesetz unterscheidet zwischen drei Fehlerkategorien: Konstruktions-, Fabrikations- und Instruktionsfehler.[11]

3. Schaden

Die Haftung nach § 1 Abs. 1 S. 1 ProdHaftG ist auf Personen- und Sachschäden begrenzt. Im Fall der Sachbeschädigung ist ein Ersatz nur möglich, wenn nicht das fehlerhafte Produkt selbst, sondern eine andere Sache beschädigt wurde und diese andere Sache üblicherweise für den privaten Gebrauch bestimmt und tatsächlich überwiegend privat genutzt worden ist. Die ProdHaftRL

---

7 *Wagner*, in: MüKo BGB § 3 ProdHaftG Rn. 16.

8 *Wagner*, in: MüKo BGB § 3 ProdHaftG Rn. 24, 26.

9 *Wagner*, in: MüKo BGB § 3 ProdHaftG Rn. 38.

10 *Hess*, in: Handbuch des Vertriebsrechts, § 11 Rn. 16.

11 *Förster,* in: BeckOK BGB § 3 ProdhaftG Rn. 30, 33, 38.

erweitert die Haftung in Art. 6 Abs. 1 lit. c) auf Schäden aus der Vernichtung oder Beschädigung von Daten, die nicht für berufliche Zwecke verwendet werden. Der Schaden muss zusätzlich kausal sein.[12]

4. Beweislast

Gemäß § 1 Abs. 4 S. 1 ProdHaftG liegt die Beweislast für den Produktfehler, den Schaden und die Kausalität beim Geschädigten. Die ProdHaftRL belässt es dabei, sieht jedoch in Art. 10 verschiedene Beweiserleichterungen vor.

II. Haftung nach dem BGB

Neben der Produkthaftung kommen auch Schadensersatzansprüche nach § 280 Abs. 1 BGB bei Verletzungen von vertraglichen Pflichten und die Deliktshaftung nach § 823 Abs. 1 BGB in Betracht. Besonderheiten im Zusammenhang mit KI-Systemen ergeben sich vor allem bei der Frage nach dem Verschulden, welches für beide Ansprüche Voraussetzung ist. Der Maßstab richtet sich nach § 276 Abs. 1. S. 1 BGB: Vorsatz und Fahrlässigkeit. Fahrlässig handelt gemäß § 276 Abs. 2 BGB, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt. Bei dieser Beurteilung sind auch die Anforderungen der KI-VO zu berücksichtigen. Insbesondere die von der Risikoklasse abhängigen Pflichten geben die erforderliche Sorgfalt bei Einsatz und Inverkehrbringen von KI-Systemen vor. Auch die nach Art. 4 KI-VO geforderte KI-Kompetenz bei den Mitarbeitenden kann eine Rolle spielen.[13] Nach § 280 Abs. 1 S. 2 BGB wird das Verschulden des Schuldners allerdings vermutet, sodass der Schuldner sich im Schadensfall entlasten muss. Für den Anspruch nach § 280 Abs. 1 BGB müssen zudem ein Schuldverhältnis und eine Pflichtverletzung vorliegen sowie ein Schaden entstanden sein. Dieser Schaden müsste kausal zur Pflichtverletzung sein.[14] Ersatzfähig sind Personen-, Sach- und Vermögensschäden.[15] Der Anspruch nach § 823 Abs. 1 BGB erfordert eine Verletzung von Leben, Körper, Gesundheit, Freiheit, Eigentum oder sonstiger Rechte und ebenfalls einen kausalen Schaden. Zusätzlich müsste die Rechtsgutverletzung rechtswidrig sein, d.h. es darf kein Rechtfertigungsgrund vorliegen.[16] Von

12 *Förster,* in: BeckOK BGB § 1 ProdhaftG Rn. 29.

13 Handbuch KI-VO, S. 223f.

14 Schuldrecht I – AT, Rn. 986ff.

15 *Ernst*, in: MüKo BGB § 280 Rn. 36; Schuldrecht I – AT, Rn. 1047ff.

16 *Förster,* in: BeckOK BGB § 823 BGB Rn. 16.

§ 823 Abs. 1 BGB umfasst ist die Produzentenhaftung, die beim Inverkehrbringen eines fehlerhaften Produkts greift. Dabei wird zwischen den verschiedene Arten Konstruktions-, Fabrikations-, Instruktions- und Produktbeobachtungsfehler unterschieden.[17] Ob einzelne Regelungen der KI-VO als Schutznorm einer einzelnen Person i.S.d. § 823 Abs. 2 BGB zu bewerten sind, ist noch offen. Die Nennung des Schutzes natürlicher Personen als Ziel der Verordnung in Erwägungsgrund 2 könnte dafürsprechen.[18]

D. Datenschutzrecht im Marketing

Im Bereich des Marketings ist der Einsatz KI-gestützter Chatbots zunehmend verbreitet. Datenschutzrechtlich sind solche Anwendungen mit erheblichen Anforderungen verbunden, da regelmäßig personenbezogene Daten verarbeitet werden, sodass die Anwendbarkeit der DSGVO nach Art. 2, 3 DSGVO eröffnet ist. Hierbei liegt die Verantwortlichkeit nach Art. 4 Nr. 7 DSGVO bei dem Unternehmen, welches die Chat-Funktion bereitstellt und über die Zwecke und Mittel der Verarbeitung entscheidet. Eine Einbindung externer Anbieter erfordert den Abschluss eines Auftragsverarbeitungsvertrags gem. Art. 28 DSGVO, in dem insbesondere die Zwecke, der Umfang und die technischen Schutzmaßnahmen der Datenverarbeitung festgelegt werden.

I. Rechtmäßigkeit und Datengrundsätze

Die Verarbeitung personenbezogener Daten bedarf zunächst einer spezifischen Rechtsgrundlage nach Art. 6 DSGVO. Zu differenzieren ist dabei zwischen der Verarbeitung von Nutzungsdaten während der Interaktion und einer etwaigen weiteren Verarbeitung der Daten zu Trainingszwecken. In vielen Fällen kann für die Verarbeitung der Nutzerinteraktion die Einwilligung der betroffenen Person gem. Art. 6 Abs. 1 lit. a DSGVO als legitime Grundlage dienen. Diese Einwilligung muss jedoch freiwillig, spezifisch, informiert und unmissverständlich erfolgen. In der Praxis wird sie häufig über die konkludente Nutzung des Chatbots i.V.m. einem vorgelagerten Datenschutzhinweis eingeholt. Für eine nachweisbare und belastbare Einwilligung empfiehlt sich jedoch ein explizites Opt-in-Verfahren, bei dem der Nutzer aktiv und ausdrücklich zustimmen muss, insbesondere wenn personenbezogene Daten im Rahmen der

17 Handbuch KI-VO, S. 224.

18 Handbuch KI-VO, S. 224.

Chat-Kommunikation weiterverarbeitet oder gespeichert werden sollen. Alternativ oder ergänzend kann die Datenverarbeitung auch auf Art. 6 Abs. 1 lit. b DSGVO gestützt werden, sofern die Chat-Interaktion der Durchführung eines Vertrages oder vorvertraglicher Maßnahmen dient. Dies ist etwa bei Bestandskunden der Fall, die sich mit konkreten Support-Anliegen an das Unternehmen wenden.[19] Für allgemein gehaltene Anfragen kann die Verarbeitung auch auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden, sofern ein berechtigtes Interesse des Unternehmens besteht und keine überwiegenden schutzwürdigen Interessen der betroffenen Person entgegenstehen. Eine Interessenabwägung ist daher stets erforderlich.[20] Komplexer ist die Frage der Zulässigkeit der Verarbeitung zu Trainingszwecken, etwa zur Verbesserung des KI-Systems. Dabei handelt es sich regelmäßig um eine Zweckänderung i.S.d. Art. 6 Abs. 4 DSGVO. Eine Einwilligung wäre zwar möglich, ist aufgrund ihrer Widerrufbarkeit jedoch in der Praxis kaum tragfähig. Möglich erscheint eine Stützung auf Art. 6 Abs. 1 lit. f DSGVO, sofern das berechtigte Interesse, etwa an der Weiterentwicklung des Systems, das Interesse der betroffenen Person überwiegt. Dabei sind insbesondere Risiken durch Profilbildung oder mangelnde Transparenz zu berücksichtigen.[21] Unabhängig von der gewählten Rechtsgrundlage sind zudem die Grundsätze des Art. 5 DSGVO einzuhalten. Insbesondere sind Daten nur zweckgebunden und nur so lange wie nötig zu verarbeiten. Dies erfordert ein Datenschutzkonzept, das u.a. Zugriffsbeschränkungen, Löschroutinen und eine begrenzte Speicherdauer vorsieht.[22]

II. Pflichten und Sicherheitsmaßnahmen

Darüber hinaus sind die Informationspflichten nach Art. 12 ff. DSGVO zu beachten. Die betroffene Person ist transparent über Art, Umfang und Zweck der Datenverarbeitung zu informieren. Ebenso sind die Betroffenenrechte, insbesondere auf Auskunft (Art. 15), Berichtigung (Art. 16) und Löschung (Art. 17), zu gewährleisten, etwa bei Widerruf einer Einwilligung oder Wegfall der Verarbeitungsgrundlage. Zusätzlich verpflichtet Art. 32 DSGVO zur Umsetzung technischer und organisatorischer Maßnahmen. Neben der Verschlüsselung von Daten bei der Übertragung und Pseudoanonymisierungsverfahren ist

19 EuGH GRUR 2023, 1131 Rn. 90ff; Hardan ZD 2024, 663 (664); Paal ZfDR 2024, 129 (154).

20 Golland EuZW 2024, 846 (849ff.); Hardan ZD 2024, 663 (665).

21 Hüger ZfDR 2024, 263 (271ff.); Paal ZfDR 2024, 129 (148ff.).

22 Willecke, Hdb- Multimedia Recht, Teil 29.3 Rn. 30ff.

auch eine strenge Zugriffsbeschränkung auf personenbezogene Inhalte sicherzustellen. Organisatorisch empfiehlt sich die Durchführung regelmäßiger Mitarbeiterschulungen im Umgang mit sensiblen Daten sowie die Etablierung einer unternehmensweiten Datenschutzrichtlinie, um das Bewusstsein für datenschutzrechtliche Risiken nachhaltig zu fördern.[23] Bei selbstlernenden Systemen, die etwa automatisierte Entscheidungen oder Profilbildungen ermöglichen, ist zudem zu prüfen, ob eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich ist. Dies ist dann der Fall, wenn ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Eine solche DSFA muss auf einer strukturierten Risikoanalyse basieren und die Maßnahmen zur Risikominderung dokumentieren.[24]

Verstöße gegen zentrale Vorschriften können nach Art. 83 DSGVO mit Bußgeldern von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes geahndet werden. Daneben besteht nach Art. 82 DSGVO ein Schadensersatzanspruch der betroffenen Person, sofern ihr durch unrechtmäßige Verarbeitung ein Schaden entstanden ist. Die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO verlangt daher eine lückenlose und aktuelle Dokumentation aller datenschutzrelevanten Prozesse.

E. Urheberrecht in der Softwareentwicklung

Im Bereich der Softwareentwicklung werden nicht nur neue KI-Programme z.B. im Kundenauftrag erstellt bzw. verwendet, sondern auch bei der Entwicklung von Computerprogrammen eingesetzt. Die Einsatzmöglichkeiten von KI sind vielfältig, denn sie kann beispielsweise einen Code erstellen oder verändern, vervollständigen oder auf Fehler analysieren. Im Hinblick auf die Erstellung und Nutzung generativer KI ergeben sich urheberrechtliche Herausforderungen. Hierbei stellen sich vor allem Fragen zum Input der KI, welche das Training einer KI-Anwendung betreffen sowie zum Output der KI, insbesondere zur Schutzfähigkeit von mittels KI-erstellten Codes.

---

23 Mantz, in: Sydow/Marsch DSGVO BDSG, Art. 32 DSGVO Rn. 25.

24 Baumgartner, in: Ehmann/Selmayr DSGVO, Art. 35 DSGVO Rn. 50ff; Recktenwald DSRITB 2023, 387 (395).

I. Training generativer KI

Hinsichtlich des Inputs einer KI ist fraglich, ob und in welchem Umfang ein Training generativer KI auf Grundlage öffentlich verfügbarer Daten eine Urheberrechtsverletzung darstellt. Sowohl das Speichern von Trainingsdaten als auch das Einlesen dieser Daten in die KI im Rahmen des Trainings könnten einen Eingriff in das Vervielfältigungsrecht des Urhebers gem. § 16 UrhG darstellen. Grundsätzlich müssen vor der Verwertungshandlung Nutzungsrechte der Rechteinhaber in Form von Lizenzen gem. § 31 UrhG eingeholt werden. Eine Urheberrechtsverletzung liegt dann vor, wenn Daten ohne Einwilligung des Urhebers verwendet werden und keine Schranke, d.h. ein gesetzlicher Erlaubnistatbestand, greift. Als praxisrelevante Schranken kommen vor allem die §§ 44a, 44b UrhG in Betracht. § 44a UrhG erlaubt vorübergehende Vervielfältigungshandlungen, die flüchtig oder begleitend sind und einen integralen und wesentlichen Teil eines technischen Verfahrens darstellen. Sie dürfen keine eigenständige wirtschaftliche Bedeutung haben. Es ist davon auszugehen, dass die Daten beim Training generativer KI für die gesamte Dauer des Trainings gespeichert und verwendet werden. Das Speichern und Einlesen der Trainingsdaten sind damit als längerfristig anzusehen und daher nicht vorübergehend. Beide Handlungen sind für den gesamten Trainingsprozess der KI bedeutsam.[25] Die Schranke des § 44a UrhG ist demnach nicht auf das Training der KI anwendbar. Bislang ist jedoch noch unklar, wie lange Trainingsdaten i.S.d. Vorschrift gespeichert werden dürfen.[26]

Ob das Training der KI gem. § 44b Abs. 2 S. 1 UrhG erlaubt ist, ist umstritten. Nach dieser Norm sind Vervielfältigungen von rechtmäßig zugänglichen Werken für das Text und Data Mining zulässig. Rechtmäßig zugänglich ist ein Werk dann, wenn es für den Nutzer frei im Internet verfügbar ist, beispielsweise durch eine Open-Access-Veröffentlichung oder wenn der Nutzer eine Lizenz für den Zugriff auf die Inhalte hat.[27] Für die Anwendbarkeit dieser Schranke spricht, dass die KI-VO in den Erwägungsgründen 105 und 106 das Data Mining gem. § 44b UrhG berücksichtigt. Dagegen wird eingewendet,

25 Kunitz LTZ 2025, 10 (13).

26 Käde MMR 2024, 142 (148).

27 BT-Drucks. 19/27426, 88.

dass der Gesetzgeber KI-Systeme bei Einführung des § 44b UrhG nicht bedacht hat.[28] Es bleibt abzuwarten, wie sich die Rechtsprechung dahingehend positioniert.

II. Schutzfähigkeit von KI-erstelltem Code

Fraglich ist in Bezug auf den Output einer KI, ob auch Erzeugnisse wie Programmcodes dem urheberrechtlichen Schutz unterliegen, welche unter dem Einsatz von generativen KI-Systemen entstanden sind. Ein durch KI erstellter (menschenlesbarer) Programmcode in Form eines Quellcodes oder Objektcodes könnte als Computerprogramm i.S.d. §§ 69a Abs. 1, Abs. 3 UrhG schutzfähig sein. Gem. § 69a Abs. 3 S. 1 UrhG werden Computerprogramme geschützt, wenn sie individuelle Werke in dem Sinne darstellen, dass sie das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers sind. Ein urheberrechtlicher Schutz setzt gem. § 2 Abs. 2 UrhG i.V.m. § 7 UrhG eine persönliche geistige Schöpfung eines Menschen voraus (sog. Schöpferprinzip). Wird ein solcher Code ausschließlich durch KI erstellt, liegt keine menschlich-gestalterische Tätigkeit vor. Vollständig durch KI generierte Codes sind in Ermangelung eines menschlichen Schöpfers nach geltendem Recht also nicht vom Urheberrechtsschutz umfasst.[29] Allerdings gibt es vom Schöpferprinzip eine Ausnahme: Die KI kann dem Schöpfer beim Schöpfungsprozess als Hilfsmittel bzw. Werkzeug dienen, wodurch das durch KI erstellte Ergebnis eine persönliche geistige Schöpfung darstellen kann. In diesem Zusammenhang ist für die Schöpfung entscheidend, dass die KI beim Entstehungsprozess lediglich eine untergeordnete Rolle spielen darf und die Steuerung des Schöpfungsvorgangs durch den Menschen erfolgt. Die KI führt dann nur die gestalterischen Entscheidungen des Menschen aus. Andernfalls handelt es sich beim Ergebnis nicht um eine persönliche geistige Schöpfung.[30] Hierbei ist allerdings regelmäßig eine Einzelfallbetrachtung dahingehend vorzunehmen, für welche Tätigkeiten die KI konkret zum Einsatz kommt.[31] Teile eines Codes können bei entsprechender Schöpfungshöhe ebenfalls einen Schutz i.S.d. Urheberrechts erlangen.[32] Bei Bewertung der Schutzfähigkeit ist nur auf den Teil des Codes

28 Schneider MMR 2024, 724 (725).

29 Maamar ZUM 2023, 481 (490).

30 Baumann NJW 2023, 3673 (3676); Maamar ZUM 2023, 481 (490).

31 Ory/Sorge NJW 2019, 710 (711).

32 Siglmüller/Gassner RDi 2023, 124 (125).

abzustellen, für den die Urheberrechtsverletzung geltend gemacht wird. Wird hingegen der gesamte Code übernommen, kommt es auf das Computerprogramm im Ganzen an, nicht auf einzelne Teile.[33] Unternehmen ist im Hinblick auf einen Urheberrechtsstreit anzuraten, genau zu dokumentieren, in welchem Stadium der Codeentwicklung technische Hilfsmittel eingesetzt wurden und welche konkreten Tätigkeiten der Gestaltung durch die KI übernommen worden sind.[34]

F. Best Practices – Aufbau einer KI- Governance

Ein zentraler Erfolgsfaktor bei der Einführung von KI in Unternehmen ist der Aufbau einer strukturierten KI-Governance. Dies schafft Transparenz über technische und organisatorische Prozesse, fördert das Vertrauen der Mitarbeitenden und ermöglicht eine fundierte Kontrolle der eingesetzten Systeme. Die Verankerung von Governance-Strukturen sollte dabei auf strategischer Ebene erfolgen. Hierzu gehört u.a. die Festlegung klarer Verantwortlichkeiten. Ein bewährter Ansatz ist dabei das sogenannte Drei-Linien-Modell der Verteidigung (3 Lines of Defense), das die Aufgabenverteilung im Unternehmen strukturiert und klare Schnittstellen definiert: Die erste Linie umfasst operative Einheiten wie Produktentwickler, Geschäftsbereichsleiter sowie die jeweilige Fachabteilung, die für die Implementierung von KI-Systemen und deren Dokumentation verantwortlich sind. Die zweite Linie übernimmt eine überwachende und unterstützende Funktion, etwa durch einen zentralen KI- Beauftragten, der die Umsetzung begleitet oder durch ein interdisziplinäres KI-Gremium aus Mitgliedern der Fachbereiche Recht, Compliance, Datenschutz, IT, Risikomanagement und HR. Diese Einheiten sind für unternehmensweite Richtlinien, Risikoanalysen und Maßnahmen zur Risikominderung zuständig. Die dritte Linie stellt schließlich eine unabhängige Überwachungsinstanz dar, z. B. die interne Revision oder externe Prüfer, die die Einhaltung regulatorischer Anforderungen objektiv bewerten.[35] Im Rahmen der dritten Linie sollte für jedes KI-System auch eine verantwortliche Person benannt werden, ein sog. Systemverantwortlicher, der die Einhaltung der Governance-Vorgaben für das jeweilige Sys-

33 Käde MMR 2024, 142 (144).

34 Baumann NJW 2023, 3673 (3676).

35 Pötsch/Bernnat, Regulierung von KI in der EU, S.161ff.

tem sicherstellt und als direkter Ansprechpartner fungiert. Dieser könnte beispielsweise der Projektleiter sein. Der regelmäßige Austausch zwischen diesen Linien ist unerlässlich. Da sich technologische und regulatorische Rahmenbedingungen laufend ändern, darf KI-Governance nicht statisch sein. Vielmehr bedarf es einer kontinuierlichen Überprüfung und Anpassung der bestehenden Strukturen. Regelmäßige Audits, Transparenz über KI-gestützte Entscheidungen sowie die Einhaltung ethischer Leitlinien sind dabei zentrale Instrumente.[36]

[36] Determann/Paal, KI-Recht International, S.70f.

Literaturverzeichnis

Baumann	Generative KI und Urheberrecht – Urheber und Anwender im Spannungsfeld, NJW 2023, 3673.
Beck‘scher Onlinekommentar Bürgerliches Gesetzbuch	Hau/Poseck (Hrsg.), 74. Edition, Stand 01.05.2025 (zit. *Bearbeiter*, in: BeckOK BGB).
Chibanguza/Steege	Die KI-Verordnung – Überblick über den neuen Rechtsrahmen, NJW 2024, 1769.
Determann/Paal	KI-Recht International: Praxisbezogene Lösungsansätze für die Sicherheit von KI-Anwendungen, 2025 (zit. *Bearbeiter*, KI-Recht International).
Ebers (Hrsg.)	Legal Tech, 1. Auflage 2023 (zit. Bearbeiter, in: SWK Legal Tech).
Ehmann/Selmayr (Hrsg.)	DSGVO, 3. Aufl. 2024 (zit. *Bearbeiter*, in: Ehmann/Selmayr DSGVO).
Förster/Gehrmann	Die KI-Verordnung aus HR-Sicht, SPA 2024, 113.
Golland	KI und KI-Verordnung aus daten schutzrechtlicher Sicht, EuZW 2024, 846.
Handbuch KI-VO	Handbuch KI-Verordnung – FAQ zum EU AI Act, Hullen/Voigt, 2024 (zit. Handbuch KI-VO).
Hardan	Datenschutzkonforme Nutzung von KI-basierten Chatbots, ZD 2024, 663.
Hoeren/Sieber/Holznagel (Hrsg.)	Handbuch Multimedia-Recht, 62. EL 2024 (zit. *Bearbeiter*, Hdb- Multimedia Recht).

Hüger	Die Rechtmäßigkeit von Datenverarbeitungen im Lebenszyklus von KI-Systemen, ZfDR 2024, 263.
Joussen	Schuldrecht I – Allgemeiner Teil, Boecken/Wilms (Hrsg.), 7. Aufl. 2023 (zit. Schuldrecht I – AT).
Käde	Next-Level Software Development, Computerprogrammschutz und weitere rechtliche Stolpersteine beim Einsatz von Code-generierender KI in der Praxis, MMR 2024, 142.
Klos/Taylan	Von der Theorie zur Praxis: Die KI-Verordnung effektiv umsetzen, CCZ 2024, 205.
Kumkar/Griesel	Transparenzpflichten für Deepfakes und synthetische Medieninhalte in der KI-VO, KIR 2024, 117.
Kunitz	Urheberrechtliche Herausforderungen bei KI-generierten Werken, LTZ 2025, 10.
Maamar	Urheberrechtliche Fragen beim Einsatz von generativen KI-Systemen, ZUM 2023, 481.
Martinek/Semler/Flohr (Hrsg.)	Handbuch des Vertriebsrechts, 5. Aufl. 2025 (zit. *Bearbeiter*, in: Handbuch des Vertriebsrechts).
Münchener Kommentar zum Bürgerlichen Gesetzbuch	Säcker/Rixecker/Oetker/Limperg/Schubert (Hrsg.), Band 2, 9. Aufl. 2022 Band 7, 9. Aufl. 2024 (zit. *Bearbeiter*, in: MüKo BGB).
Ory/Sorge	Schöpfung durch Künstliche Intelligenz? NJW 2019, 710.

Paal	KI-Training mit öffentlich frei zugänglichen Daten im Lichte der DS-GVO Vorgaben, ZfDR 2024, 129.
Pötsch/Bernnat	Regulierung von Künstlicher Intelligenz in der EU: Compliance Field Guide, 2025 (zit. *Bearbeiter*, Regulierung von KI in der EU).
Recktenwald	Datenschutzrechtliche Herausforderungen beim Einsatz Künstlicher Intelligenz im Unternehmenskontext, DSRITB 2023, 387.
Schneider	KI-unterstütztes Coding in der Spieleentwicklung, MMR 2024, 724.
Siglmüller/Gassner	Softwareentwicklung durch Open-Source-trainierte KI – Schutz und Haftung, RDi 2023, 124.
Sydow/Marsch (Hrsg.)	Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Auflage 2022 (zit. *Bearbeiter*, in: Sydow/Marsch DSGVO BDSG).

Rechtsprechungsverzeichnis

Quellenverzeichnis

Deutscher Bundestag — Entwurf eines Gesetzes zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes, 09.03.2021, Drucksache 19/27426, abrufbar unter: https://dserver.bundestag.de/btd/19/274/1927426.pdf (zuletzt abgerufen am 22.06.2025).

Zuordnung der Bearbeitung

Nasin Akin: Kapitel A, B, D, F

Nadine Möllenkamp: Kapitel E

Britta Sirges: Kapitel C