Nomos PRAXIS

Determann | Paal

KI-Recht international

Compliance Field Guide

Nomos

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Nomos **PRAXIS**

Prof. Dr. Lothar Determann
Freie Universität Berlin, University of California

Prof. Dr. Boris P. Paal, M.Jur. (Oxford)
Technische Universität München

KI-Recht international

Compliance Field Guide

Nomos

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Zitiervorschlag: Determann/Paal KI-Recht international § ... Rn. ...

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7560-0989-3 (Print)
ISBN 978-3-7489-4648-9 (ePDF)

1. Auflage 2025
© Nomos Verlagsgesellschaft, Baden-Baden 2025. Gesamtverantwortung für Druck und Herstellung bei der Nomos Verlagsgesellschaft mbH & Co. KG. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten.

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Vorwort

In einer meiner frühesten Kindheitserinnerungen spiele ich zu Hause unter dem Schreibtisch meines Vaters mit rechteckigen Karten in den Farben Grün, Rot, Weiß und Blau, die in unterschiedlichen Abständen Dutzende von Zeilen mit ovalen Löchern enthalten. Mein Vater erklärte mir später, dass die Löcher in jenen Lochkarten die Anweisungen an einen riesigen Großrechner darstellten, und zwar in Form von Einsen und Nullen, Strom und kein Strom, den einzigen Signalen, die der Computer verarbeitete. In den 1960er und 1970er Jahren schrieb mein Vater frühe Computerprogramme zur Optimierung von Formen für optische Linsen und Spiegel in Mikroskopen der Ernst Leitz GmbH in Wetzlar, einem Familienunternehmen, das auch für seine Leica (kurz für „**Lei**tz-**Ca**mera") bekannt ist. Mein Vater las mir viele Science-Fiction-Bücher vor, darunter *I, Robot* von Isaac Asimov, und Robert Jungks Bücher über die Entwicklung der Atombombe und anderer gefahrträchtiger neuer Technologien, darunter „*Die Zukunft hat schon begonnen – The Future Has Already Begun*". Zudem schenkte mein Vater mir auch einen frühen Taschenrechner von Hewlett Packard, später einen Commodore-Heimcomputer und brachte mir grundlegende Programmierkenntnisse bei.

Ich bin in einem Land (Deutschland) aufgewachsen, welches viele technische Innovationen hervorgebracht hat, das aber zugleich häufig von einer tiefsitzenden Angst vor potenziellen negativen Auswirkungen neuer Technologien geprägt war und ist. Ungefähr zu der Zeit, als ich geboren wurde, verabschiedete mein Heimatland, das Bundesland Hessen, das weltweit erste Datenschutzgesetz, einen Vorläufer der Datenschutz-Grundverordnung (DS-GVO) der Europäischen Union, was auf die Betroffenheit von Grundrechten im Rahmen der Bekämpfung von Inlandsterrorismus zurückzuführen war. Im Jahr 1990 erließ ein Berufungsgericht in Kassel eine einstweilige Verfügung, die die Entwicklung der Gentechnik in Deutschland bis zu dem Zeitpunkt untersagte, in welchem der Bundestag ein Gesetz zur Bewältigung potenzieller Risiken erlassen haben würde. Mit ähnlicher Begründung haben deutsche Gerichte im Jahre 1993 begonnen, einstweilige Verfügungen gegen den Bau von Mobilfunkstationen zu erlassen, weil die Gerichte die Entstehung von „Elektrosmog" befürchteten, mit dem ich mich in meiner Dissertation von 1996 über „Neue gefahrträchtige Technologien als Rechtsproblem" befasst habe.

Im Jahr 1999 habilitierte ich mit meiner Habilitationsschrift über „Kommunikationsfreiheit im Internet – Freiheitsrechte und gesetzliche Beschränkungen" an der Freien Universität Berlin, an welcher ich seit 1994 lehre. Ich zog nach San Francisco, um bei der internationalen Anwaltskanzlei Baker McKenzie im Bereich Technologierecht zu arbeiten, und begann Computerrecht an der University of San Francisco School of Law und an der University of California, Berkeley School of Law zu lehren, wobei ich mich neben vielen anderen Themen im Zusammenhang mit Informationstechnologie auch mit Fragen der Künstlichen Intelligenz befasste.

In meiner Rechtspraxis habe ich zahlreiche Unternehmen – von Start-ups bis hin zu Tech-Giganten – bei der Entwicklung, Vermarktung und Nutzung neuer Technologien beraten, oft lange bevor spezifische Gesetze, Verordnungen oder Gerichtsentscheidungen klare Regeln für die Einhaltung von Vorschriften aufgestellt hatten. Seit den frühen

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

2000er Jahren habe ich Formulare für Datenschutz-Folgenabschätzungen, Richtlinien für die Verwendung von externem Code und Risikoprüfungsprozesse für Kunden entwickelt, Jahre bevor Unternehmen gesetzlich verpflichtet wurden, Datenschutz-Folgenabschätzungen im Rahmen der DS-GVO zu dokumentieren. Auch hier sind im Laufe der Jahre immer wieder Fragen im Zusammenhang mit KI aufgetaucht, die praktischen Auswirkungen von KI schienen den meisten Kunden jedoch bis vor Kurzem fern und futuristisch.

Als OpenAI Ende 2022 ChatGPT ins Leben rief und in weniger als zwei Monaten 100 Millionen Nutzer auf der ganzen Welt anlockte, rückte KI in den Mittelpunkt des Interesses sehr vieler Menschen, sprang auf die Titelseiten der Medien und wurde zu einem wichtigen Punkt auf der Agenda von Politik sowie Unternehmen. Sowohl öffentliche als auch private Organisationen erkundigten sich eilig nach den Chancen, Risiken und rechtlichen Anforderungen.

Mit diesem Handbuch zum Recht der KI hoffe ich, Anwälten, Compliance-Beauftragten, Ingenieuren, Datenschutzexperten und anderen Unternehmensvertretern einen praktischen Leitfaden an die Hand zu geben. Einen ähnlichen Ansatz verfolgte ich 2010, als ich meinen „Field Guide to Data Privacy Law“ verfasste, der nun in der 5. Auflage auf Englisch und in einem Dutzend weiterer Sprachen weltweit erhältlich ist. Ich habe in diesem Werk eine umfassende Anleitung zu datenschutzrelevanten Themen im Zusammenhang mit KI gegeben, bin aber der Meinung, dass KI noch viel dringendere Fragen zur Einhaltung von Rechtsvorschriften aufwirft, die in diesem Buch behandelt werden sollen. In diesem Sinne hoffe ich, dass Sie dieses Buch als einen Wegweiser für das Recht der KI hilfreich finden, um komplexe Probleme an der Schnittstelle von Technologie, Recht und internationaler Compliance zu bewältigen.

Eine Reihe von Wissenschaftlern, Kunden, Kollegen, Studenten, Freunden und Familienmitgliedern hat wertvolle Beiträge zu diesem Handbuch geleistet. Besonders dankbar bin ich Jessica Vapnek, Professor of Practice am University of California College of the Law, San Francisco; Ken Caldeira, Senior Scientist bei Breakthrough Energy und an der Carnegie Institution for Science; Ashley Pantuliano, Associate General Counsel, OpenAI; Dan Ralls, Global Legal Counsel, TikTok; Carla J. „CJ” Utter, Privacy Counsel, Xperi, Inc.; Pamela Church, Helena Engfeldt und Irina Shestakova, Partner bei Baker McKenzie; Ruth Hill Bro, Special Advisor, ABA Cybersecurity Legal Task Force und ehemalige Vorsitzende der ABA Science & Technology Law Section; Frances Say, Rechtsassistentin bei Baker McKenzie; Anne Determann; Martin Determann, Automobilingenieur; Dr. Hans Determann, Physiker; Garima Kedia, LLM-Kandidatin 2024, University of California, Berkeley School of Law; Yanshu Zhang, JD-Kandidatin 2024, The George Washington University Law School. Die in diesem Buch zum Ausdruck gebrachten Meinungen spiegeln die persönlichen Ansichten der Autoren wider und sollten nicht meinen Mitwirkenden, Universitäten, Anwaltskanzleien, Kunden oder anderen zugeschrieben werden.

Viel Spaß mit dem Buch,

Lothar Determann

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

In dem sich dynamisch rund um die KI-Themen, -Technologien und -Anwendungen entwickelnden Rechtsgebiet, das mit guten Gründen mittlerweile als „KI-Recht“ firmiert, nimmt das zunächst von Lothar Determann in englischer Sprache als "Field Guide to Artificial Intelligence Law" verfasste Werk eine herausragende Stellung ein. Das Werk präsentiert ein leicht zugängliches und handhabbares, zugleich aber auch umfassendes Navigationsinstrument zum Aufbruch in die neuen KI-Landschaften, sodass Nutzer sicher durch die komplizierten rechtlichen Anforderungen geleitet werden und zukunftssicher (auch) eigene Expertise zur Identifizierung sowie Lösung von neuen Fragestellungen aufbauen können. Das Werk identifiziert und behandelt nicht nur die aktuellen rechtlichen Herausforderungen, sondern antizipiert darüber hinaus vor allem auch künftige Entwicklungen.

KI ist längst deutlich mehr als eine technologische Innovation. KI prägt Gesellschaft, Wirtschaft und zunehmend auch unser Rechtsverständnis. Mit der Einführung und Verwendung von KI-Systemen in vielfältigen Lebensbereichen, von der Medizin und der Mobilität über das Finanzwesen bis hin zur öffentlichen Verwaltung, gewinnen die Fragen nach den rechtlichen Rahmenbedingungen und Folgenabschätzungen, der Ausgestaltung von Haftung und Verantwortlichkeit sowie der Einbeziehung von ethischen Grundsätzen immer mehr an Bedeutung. Die Rolle des Rechts ist dabei zumindest eine zweifache: Zunächst geht es darum, durch klare Normen und Richtlinien möglichst Sicherheit und Vertrauen in diese neuen Technologien zu schaffen. Darüber hinaus muss das Recht flexibel genug bleiben, um den schnellen technologischen Wandel und die neuen Herausforderungen, die mit KI-Systemen einhergehen, angemessen bewältigen zu können.

Dieser komplexe Anspruch erfordert eine intensive und interdisziplinäre Zusammenarbeit – auch und gerade – zwischen Juristen und Technikern. Denn während Juristen rechtliche Risiken identifizieren und Lösungen zur Einhaltung von Normen erarbeiten, verstehen Techniker die komplexen Mechanismen und Potenziale der KI-Systeme. Beide Perspektiven sind notwendig, um ein ganzheitliches Verständnis und verantwortungsvolle Regelungen für die Anwendung und Entwicklung von KI zu schaffen. So drohen Juristen ohne technisches Grundverständnis häufig Gefahr zu laufen, zu stark auf hypothetische Gefahren oder unwirksame Regulierungsansätze zu fokussieren. Technikexperten hingegen mögen demgegenüber dazu neigen, rechtliche Fragestellungen als eine Art Hemmschuh für ihre Entwicklungen zu sehen, statt diese rechtlichen Vorgaben als Rahmen für eine langfristige und gesellschaftlich akzeptierte Nutzung zu begreifen. Eine erfolgreiche disziplinenübergreifende Zusammenarbeit hilft daher nicht nur, rechtliche Grauzonen zu vermeiden, sondern auch die Chancen der KI effektiv und verantwortungsvoll zu nutzen.

Das vorliegende Buch zum KI-Recht will alle Interessierten gleichermaßen dazu anregen, ein Verständnis für die Schnittstellen von Recht und Technologie zu entwickeln. Dazu wird aufgezeigt, wie interdisziplinäre Zusammenarbeit eine tragende Rolle bei der Gestaltung rechtlicher und ethischer Normen für die Zukunft der KI spielt. Denn nur durch das Zusammenspiel von rechtlichem Fachwissen und technischer Expertise kann auf breiter Basis sichergestellt werden, dass KI sowohl innovativ als auch rechtssicher und menschenzentriert eingesetzt wird. Dieser Interdisziplinarität habe ich mich

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

mit meinem Wechsel an die Technische Universität München (TUM) als Wissenschaftler und Forscher, Berater und Gutachter noch stärker verschrieben und hoffe, dass dieses Buch von meinen hierdurch gewonnenen Erfahrungen profitiert.

Sie halten ein Werk in den Händen, dass von jahrzehntelanger Praxiserfahrung profitiert und sorgfältig konzipiert wurde, um sowohl Novizen als auch Experten ein belastbares Verständnis für die rechtlichen Herausforderungen und Verpflichtungen im Zusammenhang mit der Entwicklung und Implementierung von KI-Systemen zu vermitteln. Eine der besonderen Stärken des Werkes liegt in dem verlässlich schnellen Zugang zu komplexen rechtlichen Themen, weshalb juristischer Fachjargon konsequent vermieden wird. Insgesamt handelt es sich bei dem „International Compliance Guide" zum KI-Recht um einen wertvollen Leitfaden für Juristen und Rechtsanwender, KI-Entwickler und KI-Anwender, politische Entscheidungsträger und alle, die sich mit den komplexen rechtlichen Vorgaben im KI-Bereich befassen dürfen und müssen.

Vor diesem Hintergrund war es für mich eine besondere Ehre und Freude, gemeinsam mit meinem Freund Lothar Determann die deutschsprachige Fortschreibung von „Determann's Field Guide to Artificial Intelligence Law" verfassen zu dürfen.

In diesem Sinne schließe ich auch von meiner Seite mit den besten Wünschen für eine gewinnbringende Lektüre und viel Vergnügen mit dem Werk!

Boris Paal

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Inhaltsübersicht

Vorwort 5

Inhaltsverzeichnis 11

Abkürzungsverzeichnis 17

Vorbemerkungen 19

§ 1 Überblick 23

§ 2 Recht der Künstlichen Intelligenz 35

§ 3 Start eines Compliance-Programms zu KI-Gesetzen 67

§ 4 Erstellung der Dokumentation 87

§ 5 Folgenabschätzung und Risikominimierung 119

§ 6 KI-Vereinbarungen 155

§ 7 Leitlinien 173

§ 8 Aufrechterhaltung und Prüfung der Einhaltung der Rechtsvorschriften 183

Anhang: KI-Compliance Checkliste 191

Recherche und Quellen 195

Stichwortverzeichnis 197

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Inhaltsverzeichnis

Vorwort 5

Inhaltsübersicht 9

Abkürzungsverzeichnis 17

Vorbemerkungen 19

I. Orientierung 19

II. Schlüsselbegriffe 20

§ 1 Überblick 23

I. Ausgangspunkt 23

II. Taxonomie 23

III. Anwendungsbereich 29

IV. Beobachtungen 33

V. Aufsichtsinstitutionen 33

§ 2 Recht der Künstlichen Intelligenz 35

I. KI-spezifische Gesetze 35

1. USA 35
2. EU 37
3. VR China 40

II. Produktsicherheit, Delikts- und Strafrecht 40

III. Eigentumsrechte 43

1. Eigentum an KI, Eingaben (Input) und Ausgaben (Output) 44
2. Rechtsverletzungen 46
3. Lizenzbedingungen für Open Source-Code 47
4. Computereingriff 49
5. Datenrechte 50

IV. Geschäftsgeheimnisse, Vertraulichkeit und Sicherheit 52

V. Diskriminierungsschutz 53

VI. Datenschutz und Diffamierung 54

VII. Öffentlichkeit 56

VIII. DS-GVO und andere Datenverarbeitungsvorschriften 56

1. Personenbezogene Daten 57
2. Anonymisierung und synthetische Daten 57
3. Öffentlich verfügbare Daten 58
4. Verarbeitung 59
5. Einschränkungen bei der Verarbeitung personenbezogener Daten 59

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

6. Datenminimierung/Zweckbindung/Fairness 59
7. Rechte der betroffenen Personen 60
8. Datenschutz-Folgenabschätzungen 60
9. Territoriale Anwendbarkeit der DS-GVO 61
10. DS-GVO-Konformitätsmaßnahmen 61

IX. Aufbewahrung und Speicherung von Daten 62

X. Verträge und Industriestandards 64

§ 3 Start eines Compliance-Programms zu KI-Gesetzen 67

I. Verantwortung übernehmen 67
1. Datenschutzbeauftragte und Experten für den Schutz der Privatsphäre (Privacy Professionals) 68
2. Rechtsanwälte 68
3. IT-Experten 68
4. Produktentwickler 68
5. Rechnungsprüfer und Compliance-Beauftragte 69
6. KI-Nutzer 69
7. Neue Abteilungen und Institutionen oder Aufgabenträger 69

II. Gremien/Leitung/Verwaltung/Regulierung 69

III. Zuweisung der Verantwortlichkeit 70

IV. Effektive Zusammenarbeit mit internen Interessengruppen und externen Beratern 71

V. Tools und Automatisierung 72

VI. Vorbereitung einer Aufgabenliste 74

VII. Bestandsaufnahme von KI und Gesetzen 75

VIII. Prioritäten setzen 77

IX. Ermittlung der wichtigsten rechtlichen Anforderungen 80
1. Welche Gesetze sind für KI und Ihr Unternehmen besonders relevant? 80
2. Welche Gesetze gelten für Ihr Unternehmen unter Zugrundelegung sachlicher Anwendbarkeitsbeschränkungen? 81
3. Welche Gesetze gelten für Ihr Unternehmen aufgrund von territorialen Begrenzungen? 81
4. Welche Gesetze können gegen Ihr Unternehmen durchgesetzt werden? 83

X. Ausführung 84

§ 4 Erstellung der Dokumentation 87

I. Warum erstellen Sie das Dokument? 87
1. Rechtliche Gründe 88

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

2. Geschäftliche Gründe 89
3. Organisatorische Gründe 90

II. Wer und was ist Ihre Zielgruppe? 91

III. Unterscheiden Sie Dokumentationskategorien 93

IV. Rechtsberatung, Risiken und Compliance-Bemühungen 99
1. Anwaltsgeheimnis 99
2. Dokumentation zum Compliance-Nachweis 100

V. Bekanntmachungen 103

VI. Warnungen 104

VII. Einwilligung 105

VIII. Wie man eine rechtswirksame Einwilligung erhält 107
1. Opt-In, Opt-Out und alles dazwischen 109
2. Über das Opt-In hinausgehende Einwilligungen 113
3. Sonstige Überlegungen zur Erteilung von Einwilligungen 115

IX. Verzeichnisse von Verarbeitungstätigkeiten, Datenkarten und Flussdiagrammen 116

X. Vereinbarungen 117

XI. Leitlinien 117

§ 5 Folgenabschätzung und Risikominimierung 119

I. Auswirkungen, Schaden und Risiko 119

II. Quantifizierung und Qualifizierung von Risiko und Schaden 120

III. Bewertung der Auswirkungen und Risiken von KI 121

IV. Schadens- und Haftungsrisiken 121

V. Versicherung 122

VI. Risiken besonderer Sanktionen und Abhilfemaßnahmen 122

VII. Schutz von Privilegien und Vertraulichkeit bei der Erstellung von Folgenabschätzungen 126

VIII. Speziell erforderliche Folgen- und Risikoabschätzungen 127
1. Voreingenommenheitsprüfungen nach NYC-Recht 127
2. Datenschutz-Folgenabschätzungen nach der DS-GVO 128
3. Altersgerechtes Design 128

IX. KI-Risiken von A bis Z 129
1. Automatisierte Entscheidungsfindung 129
2. Bias – Voreingenommenheit 130
3. Control – Kontrolle 131
4. Desinformationen/Fälschungen/Verleumdungen 133
5. Ethik und ESG 134

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

6. Facial recognition: Gesichtserkennung und Verarbeitung biometrischer Daten 135
7. Government procurement – Öffentliche Beschaffungsbedingungen und Steuern 135
8. „Halluzinationen“ 136
9. IP – Rechte an geistigem Eigentum, Verletzung und Eingriffe in Computer 137
10. Jailbreaking 140
11. Kontrakte – Verträge 141
12. Labour – Arbeit und Beschäftigung 141
13. Manipulation 142
14. Non-Disclosure-Agreements (NDAs)/ Geheimhaltungsverpflichtungen 143
15. Open-Source-Code-Lizenzbestimmungen 143
16. Persönlichkeitsrechte und Datenschutz 144
17. Qualitätskontrolle 145
18. Residenz und Aufbewahrung von Daten 145
19. Sicherheit und Schutz 146
20. Transparenz 147
21. Unerbetene Nachrichten (Spam) 148
22. Verkäufer/Lieferanten/Anbieter 149
23. Waffen/Ausfuhrkontrollen/Handelsembargos 151
24. X-rated Content – nicht jugendfreie Inhalte/Deepfakes 151
25. Youth Protection – Jugendschutz 152
26. „Zero Hour“- Bedrohungen 154
27. Zudem: Risiken der Nichtentwicklung, Bereitstellung und Nutzung von KI 154

§ 6 KI-Vereinbarungen 155

I. Organisation von Vereinbarungen (insbesondere Verträge, Klauseln und Anhänge) 155
II. Was bietet der Verkäufer? 157
III. Was sind die Hauptpflichten des Käufers? 158
IV. Welche Nebenpflichten übernimmt jede Partei oder übernehmen beide Parteien? 161
V. Wer sollte welche Rechte besitzen? 162
VI. Welche Informationen sind vertraulich und sollten wie von den Parteien geschützt werden? 163
VII. Was wird jede Partei für die andere tun, wenn etwas schief geht? 164

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

VIII. Wie sollten die einzelnen Parteien haften? Welche Haftungsbeschränkungen sollten gelten? 171
IX. Rechtswahl und Streitbeilegung 172
X. Höhere Gewalt (force majeure) 172

§ 7 Leitlinien 173

I. Zulässige Nutzung von generativer KI 174
II. Verwendung von KI-generiertem und Open-Source-Code 175
III. Datenerfassung und -nutzung für die KI-Entwicklung 180

§ 8 Aufrechterhaltung und Prüfung der Einhaltung der Rechtsvorschriften 183

I. Wiederkehrende Verpflichtungen und Änderungsmanagement 183
II. Dokumentation und Prozesse ausmustern und auslaufen lassen 184
III. Übernahme oder Prüfung eines bestehenden Compliance-Programms 184
IV. Entwicklung von Audit-Kontrollen 185
V. Technische KI-Leistungs-, Qualitäts- und Sicherheitsprüfungen 186
VI. Compliance-Tools und Automatisierung 186
VII. Due-Diligence-Prüfung bei Zusammenschlüssen und Übernahmen (M&A) 187
VIII. Due Diligence bei Lieferanten 188
IX. Fortbildung der Mitarbeiter 189
X. Überwachung neuer Entwicklungen 189

Anhang: KI-Compliance Checkliste 191

1. Wer ist in Ihrer Organisation für die Einhaltung der KI-relevanten Rechtsvorschriften zuständig? 191
2. Kennen Sie Ihre KI? 191
3. Haben Sie Folgenabschätzungen und Maßnahmen zur Risikominimierung dokumentiert? 192
4. Behandeln Sie Systeme und Daten vertraulich und sicher? 192
5. Haben Sie angemessene Datenverarbeitungs- und Vertraulichkeitsvereinbarungen mit KI-Anbietern? 192
6. Haben Sie die erforderlichen Warnungen und Hinweise erteilt sowie ggf. die erforderliche Zustimmung eingeholt? 192

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

7. Verfügen Sie über Verfahren und Ressourcen, um auf Sicherheitsvorfälle, behördliche Anforderungen, Nutzeranfragen, Verbraucherbeschwerden und Anträge von Betroffenen, insbesondere auf Auskunft, Korrektur und Löschung zu reagieren? 193

8. Wird KI an der richtigen Stelle entwickelt, bereitgestellt und eingesetzt? 193

9. Sind Ihre kommerziellen Verträge in Bezug auf KI angemessen? 193

10. Haben Sie Ihre Compliance-Maßnahmen dokumentiert? 193

Recherche und Quellen 195

Stichwortverzeichnis 197

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Vorbemerkungen

I. Orientierung

Dieses Handbuch soll Ihnen helfen, sich in einem komplexen Feld von für Künstliche Intelligenz (KI) relevanten Gesetzen, Pflichten und Rechten, Risiken und Chancen, Anwendungsbereichen und Technologien zurechtzufinden. Generalisten in Rechtsabteilungen von Unternehmen und in der privaten Praxis, Produktberater, Compliance-Beauftragte, Programmierer, Datenschutzbeauftragte, Datenwissenschaftler, Informationssicherheitsspezialisten, Marketingmanager, Personalverantwortliche, Personalspezialisten (Human Resources) und andere werden immer häufiger mit dem Thema KI sowie den damit verbundenen rechtlichen Compliance-Fragen und -Herausforderungen konfrontiert. Zahlreiche Informationen zu den relevanten Themenkomplexen sind öffentlich zugänglich, ein Großteil dieser Informationen ist sogar kostenlos verfügbar. Gleichwohl wird es häufig schwierig sein, ein praktisches Problem schnell und zuverlässig in den Griff zu bekommen, ohne sich im Spannungsverhältnis von Komplexität und Details zu verheddern oder sogar zu verlieren. 1

An dieser Stelle kommt das vorliegende Werk als international angelegter Compliance Guide mit der Funktion eines qualifizierten Leitfadens ins Spiel. Das Handbuch soll helfen, Probleme zu erkennen, einen belastbaren praktischen Überblick zu geben, Fragen zu formulieren und Lösungen zu finden. Gleichwohl geht es nicht darum, sich bei dem Thema KI-Compliance lediglich „durchzuschlagen", obgleich auch dies vielfach bereits eine beachtliche Leistung darstellen mag. Vielmehr finden sich, wo das Werk konzeptionell (noch) keine hinreichend detaillierte Antwort geben kann, stets Hinweise auf weitere, leicht zugängliche Ressourcen und Quellen – so konkret etwa durch die Angabe von Schlüsselbegriffen, die eine weitere Vertiefung ermöglichen und erleichtern. Allerdings werden Sie in diesem Handbuch keine Fußnoten mit überbordenden Zitatenapparaten finden. Denn das Werk, das Sie in den Händen halten, ist für den nutzbringenden Einsatz in der Praxis gedacht. 2

Der Begriff „Compliance" stammt aus dem angloamerikanischen Rechtskreis und leitet sich vom englischen Verb „to comply" ab, das übersetzt etwa „befolgen" oder „sich anpassen" bedeutet. Im Kontext der Unternehmensführung beschreibt Compliance die Verpflichtung von Unternehmen, sich an geltende Gesetze, Richtlinien und ethische Standards zu halten. Besonders in internationalen Unternehmen, die in mehreren Rechtskreisen tätig sind, hat sich der englische Begriff etabliert und findet mittlerweile auch im deutschsprachigen Raum breite Verwendung. Man mag beklagen, dass es sprachlich und rechtlich wünschenswert gewesen wäre, deutsche Begriffe wie „Rechtseinhaltung" oder „Rechtsbefolgung" hätten sich anstelle des Anglizismus „Compliance" durchgesetzt. Denn diese Begriffe würden die eigentliche Bedeutung klarer und verständlicher transportieren, insbesondere im Hinblick auf die zentrale Rolle der Gesetzestreue. Gleichwohl werden wir in diesem Buch der etablierten Compliance-Terminologie folgen, um die Handhabung und Anschlussfähigkeit zu erleichtern. 3

Das Handbuch enthält umfangreiche Check- und Aufgabenlisten mit den wichtigsten Compliance-Anforderungen. Hierauf aufbauend finden Sie praktische Vorschläge, wie Sie diesen Compliance-Anforderungen effizient und belastbar begegnen können. 4

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Außerdem finden Sie immer wieder Beispiele und Hinweise zu länderspezifischen rechtlichen Einzelheiten und Unterschieden, auf die international tätige Unternehmen in der Praxis mit großer Wahrscheinlichkeit stoßen werden. Die hierauf bezogenen Ausführungen wurden zur Veranschaulichung ausgewählt, wollen aber keinesfalls eine abschließende weltweite Geltung beanspruchen. In diesem Sinne werden Ihnen die präsentierten Fallbeispiele die Herangehensweise erleichtern, wenn Sie sich erst einmal in der KI-Landschaft belastbar orientiert haben sowie sodann nach rechtlichen Details für eine bestimmte Jurisdiktion und eine konkrete Situation suchen wollen.

5 Hier ein paar Vorschläge, wie Sie diesen „KI-Recht – International Compliance Guide" besonders gewinnbringend verwenden können: Wenn Sie dieses Buch erworben haben, weil Sie ein Handlungsprogramm zur Einhaltung der maßgeblichen Rechtsvorschriften zu KI entwerfen oder einführen sollen, werden Ihnen die nachfolgende Übersicht über „Schlüsselbegriffe" (→ Rn. 7 ff.) und der „allgemeine Überblick" (→ § 1 Rn. 1 ff.) eine wertvolle Orientierungsgrundlage geben, aufgrund derer Sie in einem nächsten Schritt die sieben Hauptkapitel des Buchs (§§ 2–8) zur weiteren Navigation verwenden können. Falls Sie sich (nur) schnell über ein bestimmtes Thema informieren wollen, können Sie im Stichwortverzeichnis nachschlagen, um direkt zu der von Ihnen gesuchten Fragestellung zu gelangen. Wie auch immer Sie dieses Handbuch verwenden mögen, wir hoffen, Sie finden das Werk hilfreich, um sich in dem komplexen, neuen und sich dynamisch entwickelnden Bereich des KI-Rechts und bei der Auseinandersetzung mit den hiermit verbundenen Compliance-Herausforderungen zurechtzufinden.

6 Zur besseren Lesbarkeit wird in diesem Buch durchgehend das generische Maskulinum verwendet. Die verwendeten Personenbezeichnungen beziehen sich – sofern nicht anders kenntlich gemacht – auf alle Geschlechter.

II. Schlüsselbegriffe

7 Wir haben die folgenden Begriffe und Definitionen für dieses Buch genutzt, um rechtlich relevante Konzepte und Unterscheidungen einfach und intuitiv zu vermitteln, während Informatiker, Philosophen, Juristen und politische Entscheidungsträger weiterhin über Grundsätze, Definitionen und Terminologie diskutieren sowie diese näher auskonturieren mögen.

8 Weitere Definitionen, Begriffe und Überlegungen finden Sie in dem unmittelbar folgenden Abschnitt, der einen Überblick zu den in diesem Buch behandelten Themen gibt.

9 **Anbieter** ist eine Person oder ein Unternehmen, die bzw. das KI hostet und pflegt sowie Nutzern den Zugang zu den Funktionen dieser KI eröffnet, zB über eine Webseite oder eine mobile App, die Online-Chats, computergenerierte Bilder oder Suchergebnisse liefert.

10 **Anthropomorphismus** bedeutet, dass Tieren, Pflanzen oder Maschinen menschliche Eigenschaften oder Verhaltensweisen zugeschrieben werden, zB in Bezug auf „maschinelles Lernen" oder „Halluzinationen" im Zusammenhang mit KI. In diesem Buch bemühen wir uns, solche Anthropomorphismen zu vermeiden. Zwar können Menschen neue technologische Konzepte oft schneller verstehen, wenn Metaphern verwendet wer-

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

den. Auch und gerade Juristen sowie politische Entscheidungsträger sollten in dieser Hinsicht aber vorsichtig sein. Um die Menschlichkeit zu erhalten und zu schützen, sollten wir Menschen generell zwischen uns und den Maschinen unterscheiden. Wir müssen unsere Fähigkeit bewahren, Maschinen abschalten zu können, ohne uns weitere Gedanken darüber machen zu müssen, ob dies einen „Mord" darstellt oder andere Verwicklungen aufwerfen mag. Dies gilt insbesondere mit dem Blick auf KI, die wir nicht vollständig vorhersagen, verstehen oder kontrollieren können. Wir drohen ansonsten unsere einzigartigen Fähigkeiten zu verlieren oder jedenfalls in ungünstiger Weise einzuschränken, falls wir (zu sehr) anthropomorphisieren.

Compliance meint die Einführung eines systematischen Programms und vieler Einzelmaßnahmen zur Rechtseinhaltung – von unternehmensinternen Richtlinien bzw. Kodizes bis hin zu gesetzlichen Vorgaben – im Unternehmen. Die deutschen Begriffe, wie Rechtseinhaltung oder Rechtsbefolgung haben sich nicht durchsetzen können und beinhalten weniger als das englische Lehnwort „Compliance" ausdrückt. Denn die Einhaltung von zB ethischen oder moralischen Standards wird nicht erfasst. Auch passendere Begriffe, wie Regeltreue und Regelkonformität, mussten im deutschen Sprachgebrauch letztlich dem englischen Wort den Vortritt lassen. Ziele der Compliance liegen in der Risikominimierung, der Effizienzsteigerung und der Effektivitätssteigerung. Der Begriff der Compliance umfasst insbesondere auch Hinweisgebersysteme (u.a. auch sog. Whistleblower-Hotlines), die in den USA nach der Aufdeckung von Missbräuchen im Bereich der Dotcom-Blase etabliert wurden. 11

Deterministische Systeme sind Computersysteme, die mit spezifischen Schritt-für-Schritt-Anweisungen programmiert werden („wenn dies passiert, dann mach das"), um Ergebnisse zu erzeugen, die die Entwickler vorhersagen, erklären und kontrollieren können. In diesem Buch wird der Begriff „deterministisch" für Systeme verwendet, die nicht als KI iSd vorstehenden Definition eingestuft werden. Alternativ könnte diese Art von Computersystemen als „regelbasiert", „statisch" oder „traditionell" bezeichnet werden. Jede Software ist anfällig für Fehlfunktionen aufgrund von Bugs und anderen Fehlern; Entwickler können Fehler in deterministischen Systemen finden und durch Patches, Updates und Upgrades beheben. 12

Entwickler ist eine Einzelperson oder ein Unternehmen, die bzw. das KI entwickelt, indem es bzw. sie idR von Dritten gelieferte Hardware konfiguriert, den Programmcode schreibt oder ändert, Trainingsdaten verwendet (und ggf. auch sammelt) sowie insbesondere Techniken des maschinellen und verstärkenden Lernens anwendet. 13

Input (**Eingaben**) sind Aufforderungen und andere Informationen, die Menschen eingeben oder die KI über Sensoren erfasst, zB Zahlen, die auf einem Taschenrechner eingegeben werden, Aufforderungen an Chatbots, Sprachbefehle an intelligente Lautsprecher und Lenkradbewegungen in Autos. 14

Künstliche Intelligenz (**KI**) bezeichnet Computersysteme, die Texte, Bilder, Problemlösungen und andere Ergebnisse generieren, wobei diese Computersysteme in hohem Maße autonom und in einer Weise arbeiten, die ihre Entwickler nicht mit Sicherheit vorhersagen, erklären oder kontrollieren können. 15

Nutzer ist eine Einzelperson oder ein Unternehmen, die bzw. das Output von KI bezieht. Der Begriff des Nutzers ist weit zu verstehen und zu unterscheiden vom 16

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Begriff des Betreibers iSd Art. 3 Nr. 4 der Europäischen KI-Verordnung. Letzterer Begriff bezieht sich, in Abgrenzung zum Nutzer, ausschließlich auf solche Personen, die KI nicht im Rahmen einer persönlichen sondern vielmehr für eine berufliche Tätigkeit verwenden.

17 **Output** (**Ausgaben**) sind die Ergebnisse von Rechenoperationen, die Systeme für menschliche Bediener oder andere Systeme bereitstellen, einschließlich Zahlen, die von Taschenrechnern zurückgegeben werden, Antworten von Chatbots, Musik, die von intelligenten Lautsprechern abgespielt wird, und Wegbeschreibungen, die von Autos befolgt werden.

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

§ 2 Recht der Künstlichen Intelligenz

I. KI-spezifische Gesetze 2
1. USA 4
2. EU 10
3. VR China 20

II. Produktsicherheit, Delikts- und Strafrecht 23

III. Eigentumsrechte 29
1. Eigentum an KI, Eingaben (Input) und Ausgaben (Output) 31
2. Rechtsverletzungen 36
3. Lizenzbedingungen für Open Source-Code 39
4. Computereingriff 45
5. Datenrechte 50

IV. Geschäftsgeheimnisse, Vertraulichkeit und Sicherheit 53

V. Diskriminierungsschutz 58

VI. Datenschutz und Diffamierung 61

VII. Öffentlichkeit 65

VIII. DS-GVO und andere Datenverarbeitungsvorschriften 66
1. Personenbezogene Daten 67
2. Anonymisierung und synthetische Daten 68
3. Öffentlich verfügbare Daten 72
4. Verarbeitung 74
5. Einschränkungen bei der Verarbeitung personenbezogener Daten ... 75
6. Datenminimierung/Zweckbindung/Fairness 76
7. Rechte der betroffenen Personen 77
8. Datenschutz-Folgenabschätzungen 78
9. Territoriale Anwendbarkeit der DS-GVO 80
10. DS-GVO-Konformitätsmaßnahmen 81

IX. Aufbewahrung und Speicherung von Daten 82

X. Verträge und Industriestandards 87

Unternehmen müssen eine Vielzahl von Gesetzen einhalten, die sich auf geschäftliche Aktivitäten beziehen. Im KI-Kontext werfen mehrere dieser Gesetze spezifische **neue Herausforderungen und Auslegungsprobleme** auf. Hiermit müssen sich Unternehmen auseinandersetzen, wenn sie KI-Systeme entwickeln, bereitstellen oder nutzen, da die Systeme autonom arbeiten und ihre Entwickler ihre Ergebnisse nicht mit Sicherheit vorhersagen, erklären oder kontrollieren können. Solche Gesetze können als „**KI-Gesetze**" bezeichnet werden. Einen ersten und ausgewählten Überblick über diese Gesetze finden Sie in diesem ersten Kapitel des Handbuchs. 1

I. KI-spezifische Gesetze

Führende KI-Unternehmen haben die Öffentlichkeit vor **schwerwiegenden Risiken** im Zusammenhang mit der KI-Entwicklung gewarnt, darunter sogar auch vor dem Aussterben der Menschheit. CEOs und Forscher haben sich zusammengetan, um zu fordern, dass Unternehmen die weitere Entwicklung stoppen, Forscher die Entwicklung einstellen und Regierungen den KI-Sektor regulieren. 2

Im Mai 2024 erließen der **US-Bundesstaat Colorado** und die **Europäische Union** jeweils **Gesetze zur KI**, die 2026 vollständig in Kraft treten und bestimmte Risiken im Zusammenhang mit KI adressieren. Keines der beiden Gesetze zielt darauf ab, alle rechtlichen Erwägungen im KI-Zusammenhang zu berücksichtigen, zB in Bezug auf den Datenschutz oder das geistige Eigentum. 3

1. USA

Im Jahr 2018 fügte **Kalifornien** dem **Business & Professions Code** eine Section 17941 hinzu, wonach niemand einen **Bot** verwenden darf, um mit einer Person in Kalifornien online zu kommunizieren und die andere Person absichtlich über die Verwendung einer künstlichen Identität zu kommerziellen Zwecken oder zur Beeinflussung einer 4

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Wahl zu täuschen. Unternehmen können sich der Haftung entziehen, wenn sie ihre Bots offenlegen, die als automatisierte Online-Konten definiert sind und alle oder jedenfalls im Wesentlichen alle Aktionen oder Beiträge dieses Kontos künstlich erzeugen. Unternehmen sind zwar verpflichtet, auch deterministisch programmierte Bots offenzulegen. In der Praxis ist es aber viel wahrscheinlicher, dass Menschen von KI-gesteuerten Bots getäuscht werden. Daher betrachten Juristen dieses kalifornische Gesetz zu Recht als eines der **ersten KI-spezifischen Gesetze**.

5 Die **USA** erließen 2020 ein **Gesetz zur nationalen KI-Initiative**, um Programme zwischen den Bundesbehörden zu koordinieren sowie dadurch die KI-Forschung und Anwendung für den Wohlstand und die nationale Sicherheit zu beschleunigen. Organisationen des privaten Sektors unterliegen diesem Gesetz zwar nicht direkt, können aber indirekt als Auftragnehmer oder Zulieferer der Regierung betroffen sein. Einzelne Bundesstaaten folgten diesem Beispiel. So erließ **Connecticut** das **Gesetz Nr. 23–16 über KI**, automatisierte Entscheidungsfindung und den Schutz personenbezogener Daten, das am 1.7.2023 in Kraft trat. Nach diesem Gesetz muss das Connecticut Department of Administrative Services bis zum 31.12.2023 ein Inventar aller Systeme veröffentlichen, die KI einsetzen und von einer staatlichen Behörde verwendet werden, wobei anzugeben sind (1) der Name des Systems und ggf. des Anbieters, (2) eine Beschreibung der allgemeinen Fähigkeiten und Verwendungszwecke eines solchen Systems, (3) ob ein solches System verwendet wurde, um unabhängig eine Schlussfolgerung, eine Entscheidung oder ein Urteil zu treffen, zu informieren oder wesentlich zu unterstützen, und (4) ob ein solches System vor der Implementierung einer Folgenabschätzung unterzogen wurde.

6 Seit dem 1.1.2023 müssen Arbeitgeber in **New York City** automatisierte Entscheidungshilfen für die Beschäftigung (**automated employment decision tools, AEDTs**) auswerten, um die Wahrscheinlichkeit von ungleichen Auswirkungen (disparate impacts) und Diskriminierungen aufgrund von Geschlecht, Herkunft oder ethnischer Zugehörigkeit zu beurteilen. Arbeitgeber müssen die Vorschriften auch in Bezug auf deterministische Entscheidungshilfen einhalten. KI stellt in dieser Hinsicht sogar noch viel größere Herausforderungen und Risiken dar, da die Entwickler die Ergebnisse nicht mit Sicherheit vorhersagen, erklären oder kontrollieren können. Daher kann dieses New York City-Gesetz als ein frühes KI-spezifisches Gesetz verstanden werden.

7 In den USA ist **Colorado** der erste US-Bundesstaat, der ein umfassendes KI-Gesetz in Kraft gesetzt hat. Das KI-Gesetz von Colorado ist ein **sektorübergreifendes KI-Governance-Gesetz**, das für Entwickler gilt, die in Colorado geschäftlich tätig sind und ein KI-System entwickeln oder absichtlich und in erheblichem Umfang verändern, sowie für Nutzer, die in Colorado geschäftlich tätig sind und ein KI-System mit hohem Risiko einsetzen. **KI-Systeme mit hohem Risiko** sind definiert als KI-Systeme, die eine folgenschwere Entscheidung treffen oder ein wesentlicher Faktor bei der Entscheidungsfindung sind, zB bei Entscheidungen über die Einschreibung in ein Bildungssystem, die Beschäftigung oder Finanzdienstleistungen. Das KI-Gesetz von Colorado erlegt Entwicklern und Anwendern die Pflicht zur angemessenen Sorgfalt auf, um **algorithmische Diskriminierung in KI-Systemen mit hohem Risiko** zu vermeiden. Wenn ein Entwickler oder Betreiber bestimmte Bestimmungen des Gesetzes einhält, besteht

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

die widerlegbare Vermutung, dass der Entwickler oder Betreiber angemessene Sorgfalt walten ließ, um algorithmische Diskriminierung zu vermeiden.

Betreiber von **KI-Systemen mit hohem Risiko** müssen eine **Risikomanagementpolitik** und ein **Risikomanagementprogramm** einführen, eine **Folgenabschätzung** für das KI-System mit hohem Risiko durchführen und Verbraucher **benachrichtigen**, wenn das KI-System mit hohem Risiko eine Verbraucher betreffende Folgeentscheidung trifft. Entwickler und Betreiber sind außerdem verpflichtet, dem Generalstaatsanwalt innerhalb von 90 Tagen nach Entdeckung zu melden, wenn ein risikoreiches KI-System eine algorithmische Diskriminierung verursacht hat. 8

Das KI-Gesetz von **Colorado** betrachtet **General Purpose AI-(GPAI-)Systeme** nicht als Hochrisikosysteme. Die Entwickler von GPAI-Systemen sind allerdings verpflichtet, eine detaillierte Zusammenfassung der für das Training des Allzweckmodells verwendeten Inhalte zu erstellen und aufzubewahren und den Betreibern eine Beschreibung der für das Training, die Tests und die Validierung verwendeten Daten zur Verfügung zu stellen. 9

2. EU

Die europäische Verordnung über Künstliche Intelligenz (**EU-KI-VO** = AI Act) ist die erste weltweit umfassende Regulierung zur Steuerung des Einsatzes von KI. Die EU-KI-VO zielt darauf ab, das Funktionieren des europäischen Binnenmarkts zu verbessern und die Einführung einer menschenzentrierten und vertrauenswürdigen KI zu fördern. Zugleich soll ein hohes Schutzniveau hinsichtlich Gesundheit, Sicherheit und der in der Europäischen Grundrechtecharta verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, vor den schädlichen Auswirkungen von KI-Systemen in der Union gewährleistet und die Innovation unterstützt werden (**Art. 1 EU-KI-VO**). 10

Die **EU-KI-VO** als das KI-Gesetz der EU, das am 1.8.2024 in Kraft getreten ist, führt Verpflichtungen ein, die für alle Akteure im KI-Ökosystem gelten, so insbesondere für Anbieter und Betreiber. Es handelt sich um ein umfangreiches und detailliertes Regelungsregime, das auf der Grundlage und nach der Konzeption der EU-Rechtsvorschriften zur Produkthaftung und zum Verbraucherschutz ausgearbeitet wurde; das Gesetzeswerk besteht aus 113 Artikeln und 180 Erwägungsgründen. Aufgrund seines extraterritorialen Geltungsbereichs fällt voraussichtlich (nahezu) jedes Unternehmen, das auf den EU-Markt abzielt, unter das EU-KI-Gesetz. 11

Die **EU-KI-VO** regelt umfassend und sektorübergreifend den Einsatz und die Entwicklung von KI-Systemen über den gesamten Lebenszyklus hinweg. Die EU-KI-VO findet nicht nur in Bezug auf europäische Unternehmen Anwendung, sondern uU auch auf Unternehmen außerhalb der EU (sog. **Marktortprinzip**), so insbesondere auf (1) Unternehmen mit Sitz in der EU, die KI-Systeme verwenden, (2) Importeure, Händler oder Hersteller von KI-Systemen in der EU, (3) Anbieter, sowohl innerhalb als auch außerhalb der EU, die KI-Systeme in den Binnenmarktverkehr bringen, und (4) auf Anbieter und Nutzer von KI-Systemen, deren Ausgaben (Output) in der EU genutzt werden, unabhängig davon, wo diese ansässig sind. 12

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

13 Im Zentrum des **sachlichen Anwendungsbereichs** stehen das „**KI-System**" (Art. 3 lit. 1 EU-KI-VO) und „**KI-Modelle mit allgemeinem Verwendungszweck**" (Art. 3 lit. 63 EU-KI-VO). Ein KI-System ist legaldefiniert als: „ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können". Prominente Beispiele für solche KI-Systeme sind medizinische Diagnose-Systeme oder autonomes Fahren. KI-Modelle mit allgemeinem Verwendungszweck (**General Purpose AI, GPAI**) zeichnen sich dadurch aus, dass sie eine erhebliche allgemeine Verwendbarkeit aufweisen und in eine Vielzahl von nachgelagerten Systemen oder Anwendungen integriert werden können. Nach der Legaldefinition der EU-KI-VO ist ein KI-Modell „mit allgemeinem Verwendungszweck" „ein KI-Modell – einschließlich der Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird –, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden". Aktuelle Beispiele für solche GPAIs sind **GPT-4, DALL-E, Google BERT, Midjourney 5.1**.

14 **Ausgenommen vom sachlichen Anwendungsbereich der EU-KI-VO** sind private und nicht kommerzielle Anwendungen, militärische oder verteidigungsbezogene Systeme sowie Systeme, die ausschließlich zu Forschungs- und Entwicklungszwecken genutzt werden. Die Regeln der EU-KI-VO wirken über die Grenzen der EU hinaus, weshalb auch Unternehmen betroffen sein können, die sich zwar in Drittstaaten befinden, ihre KI-Systeme aber in Europa anbieten. Insbesondere Anbieter und Betreiber sind für die Einhaltung der zahlreichen Pflichten verantwortlich. Die EU-KI-VO stellt vielfältige Anforderungen, sowohl an die einzelnen KI-Systeme als auch an die verschiedenen Stakeholder **entlang des gesamten KI-Produkt- und Lebenszyklus**.

15 Die **EU-KI-VO** verfolgt einen **risikobasierten Ansatz**, um den unterschiedlichen Gefahrenpotenzialen und Anwendungsmöglichkeiten von KI gerecht zu werden. Dieser Ansatz berücksichtigt das jeweilige Risiko, das ein KI-System für die Gesundheit, Sicherheit und Grundrechte der Menschen aus Sicht des Gesetzgebers darstellen kann. Ziel ist es, durch abgestufte Anforderungen und Maßnahmen einen angemessenen Schutz zu gewährleisten, ohne die Innovationskraft und Entwicklung von KI-Systemen unnötig zu behindern. Die EU-KI-VO legt hierzu dem Grunde nach **vier Risikostufen** fest, die von der Verwendung von KI-Systemen abhängen: unannehmbares, hohes, begrenztes und minimales Risiko. Je nach Risikostufe gelten unterschiedliche Anforderungen. Bei den im Zentrum der Regelungen stehenden **KI-Systemen mit hohem Risiko** handelt es sich um KI-Systeme, die sich negativ auf die Gesundheit und Sicherheit von Menschen, ihre Grundrechte oder die Umwelt auswirken könnten. Biometrische Identifizierungssysteme, Bildung und Personalbeschaffung sind Bereiche,

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

in denen der Einsatz von KI nach der EU-KI-VO ein hohes Risiko darstellen würde. Die Pflichten der Anbieter zielen ab auf die Schaffung und Aufrechterhaltung eines sicheren KI-Systems, während sich die Pflichten der Nutzer auf die verantwortungsvolle und sichere Nutzung des Systems beziehen. Zu den Verpflichtungen, die die Betreiber von KI-Systemen mit hohem Risiko erfüllen müssen, gehören angemessene Systeme zur Risikobewertung und -minderung, eine hohe Qualität der verwendeten Datensätze, um Risiken und diskriminierende Ergebnisse zu minimieren, sowie angemessene menschliche Kontrollmaßnahmen. So wäre bspw. ein Tool zum Scannen von Lebensläufen, das eine Rangfolge der Bewerber erstellt, ein KI-System mit hohem Risiko, da es Einstellungsentscheidungen treffen könnte, die die Grundrechte der Bewerber beeinträchtigen. Der Anbieter und der Entwickler eines solchen Tools müssen hiernach sicherstellen, dass sie bei der Entwicklung und Nutzung des Tools ihren jeweiligen Verpflichtungen nachgekommen sind.

16 Für **KI-Modelle mit allgemeinem Verwendungszweck** (**GPAI**) gibt es einen eigenen Regelungskomplex, der diese Systeme in **drei Kategorien** unterteilt, nämlich **GPAI-Modelle mit systemischem Risiko**, **einfache GPAI-Modelle, die proprietär sind**, und **einfache GPAI-Modelle, die im Rahmen von freien und quelloffenen Lizenzen** (**Open Source**) **bereitgestellt werden**. Open-Source-Modelle profitieren von einer weniger strengen Regulierung. Zu den Verpflichtungen der GPAI-Anbieter gehören das Erstellen einer einschlägigen technischen Dokumentation, einer Zusammenfassung der Schulungsinhalte sowie eines Handlungsprogramms zur Beachtung von Urheber- und Vorbehaltsrechten.

17 Die **EU-KI-VO** überlässt es den Unternehmen, die erforderlichen Maßnahmen selbst zu implementieren, legt jedoch zugleich **empfindliche Sanktionen mit hohen Geldstrafen** für die Verletzung der gesetzlichen Vorgaben fest. Ähnlich wie bei der DS-GVO wird ein Selbstkontrollmechanismus etabliert, der entsprechende Risiken und Unsicherheiten für Unternehmen mit sich bringt. Die möglichen **Geldstrafen nach der EU-KI-VO** übertreffen mit bis zu 35 Mio. EUR oder – im Falle von Unternehmen – von bis zu 7 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres sogar die der DS-GVO.

18 Es bleibt abzuwarten, ob Rechtsordnungen auf der ganzen Welt die **EU-KI-VO** in ihren **eigenen Regelungsregimen nachbilden** werden. Es könnte noch zu früh sein, dies belastbar zu beurteilen, aber angesichts der Tatsache, dass die EU-KI-VO extraterritoriale Wirkung hat sowie einige Länder wie Brasilien, Chile und die Türkei erste umfassende KI-Gesetzesentwürfe auf der Grundlage der EU-KI-VO vorbereitet haben, sind die Auswirkungen jedenfalls bereits zu spüren.

19 Betroffene Unternehmen sollten sich fortlaufend der **EU-KI-VO-Compliance** annehmen, um weitreichende Haftungsthemen und Bußgelder zu vermeiden. Dabei wird es jeweils im Einzelfall nötig sein, einzelne Systeme – ggf. unter Zuhilfenahme externer Rechtsberater – zu untersuchen und entsprechende Leitlinien zu entwickeln. Deshalb sollten alle zur Einhaltung der EU-KI-VO ergriffenen Maßnahmen dokumentiert werden, um bei Prüfungen und Anfragen der Behörden Nachweise erbringen zu können. Zudem sollten möglichst detaillierte Aufzeichnungen über alle Risikobewertungen, Konformitätsprüfungen und Überwachungsmaßnahmen geführt werden.

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

3. VR China

20 Mit Wirkung vom 15.8.2023 hat die **Volksrepublik China** (**VR China**) „**Interim Measures for the Management of Generative Artificial Intelligence Services**" („Vorläufige Maßnahmen für die Verwaltung von Diensten der generativen künstlichen Intelligenz") erlassen, die auf einer Reihe bestehender Gesetze basieren. In diesen vorläufigen Maßnahmen erklärt die VR China, dass Anbieter und Nutzer von generativen KI-Diensten die bestehenden Gesetze in Bezug auf „**generative KI-Technologien**" einhalten müssen, die definiert sind als „Modelle und relevante Technologien, die in der Lage sind, Inhalte wie Texte, Bilder, Audio oder Video zu erzeugen". Anbieter von KI-Systemen sind verpflichtet, die Integrität der Staatsgewalt zu wahren. Diese Verpflichtung umfasst insbesondere die Pflicht, die nationale Einheit zu bewahren sowie die soziale und wirtschaftliche Ordnung sicherzustellen. Entsprechend sind Anbieter verpflichtet, Sicherheitschecks für ihre KI-Modelle durchzuführen, sofern diese KI-Modelle dazu geeignet sind, die öffentliche Meinung zu beeinflussen.

21 **Pauschale Verbote**, ähnlich den in der EU-KI-VO vorgesehenen, wie zB betreffend Systeme für Social-Scoring oder Echtzeitüberwachung, bestehen derzeit nicht. Betreiber müssen lediglich die o.g. Einschränkungen beachten, vor allem also die Wahrung der öffentlichen Ordnung und der Staatsmacht.

22 Darüber hinaus werden KI-Tools von der **VR China** als eine Chance für ökonomisches Wachstum wahrgenommen sowie als Möglichkeit, eine Vorreiterrolle in diesem neu wachsenden Technologiesektor einzunehmen.

II. Produktsicherheit, Delikts- und Strafrecht

23 Regierungen schützen ihre Bürger vor Gefahren für Leben und Gesundheit mit zahlreichen Gesetzen, die es verbieten, Personen vorsätzlich oder fahrlässig zu verletzen, sich an bestimmten riskanten Aktivitäten zu beteiligen und Produkte zu verkaufen oder zu verwenden, die bekanntermaßen oder wahrscheinlich Schaden verursachen. Einzelpersonen und Unternehmen, die gegen diese Verbote verstoßen, können von bestimmten Aktivitäten abgehalten und mit einer Vielzahl von Sanktionen belegt werden, darunter Freiheitsstrafen für Einzelpersonen, Geldstrafen, Strafzahlungen und Entschädigungszahlungen. Wenn ein Opfer getötet oder verletzt wird, entscheiden Strafverfolgungsbehörden und Gerichte auf der Grundlage einer komplexen Analyse der objektiven Verursachung, der Verhaltenspflichten und des Grads des subjektiven Verschuldens, wer zur Verantwortung gezogen wird sowie welche Strafmaßnahmen und Haftungen damit einhergehen.

24 So tragen bei jedem Verkehrsunfall Fahrzeughalter, Fahrzeugführer, Autohersteller und verschiedene andere Personen oder Organisationen in gewissem Maße zu einer Kette von Ereignissen bei, zB ein Fahrzeugführer, der die zulässige Höchstgeschwindigkeit überschritten hat, ein Beifahrer, der den Fahrzeugführer mit einer Frage abgelenkt hat, ein Autohersteller, der sich für billige Bremsbeläge entschieden hat, ein Fahrzeughalter, der es versäumt hat, regelmäßige Wartungstermine einzuhalten, ein Kneipenwirt, der dem Fahrzeugführer zu viel Alkohol ausgeschenkt hat, ein Hundebesitzer, dessen Tier auf die Straße gelaufen ist, oder ein Geschäftsinhaber, dessen grelle Neonreklame die Sicht des Fahrzeugführers beeinträchtigt hat. Im Laufe der Zeit hat der Gesetzgeber

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

zahlreiche Vorschriften über die Pflichten und Verantwortlichkeiten des Einzelnen in Bezug auf die Sicherheitsmerkmale von Kraftfahrzeugen, die Fahrzeugwartung, das Fahrverhalten, den Verkauf und Konsum von Alkohol, die Tierkontrolle und die Werbung am Straßenrand entwickelt. Auch die Gerichte haben Regeln dafür entwickelt, wie die individuelle Verantwortung für Schäden, die durch mehrere menschliche Akteure und Faktoren verursacht wurden, zuzuordnen ist. Der Autohersteller wird idR nicht zur Verantwortung gezogen, wenn die Bremsen den Spezifikationen und geltenden Vorschriften entsprechen und kein Konstruktionsfehler vorliegt. Der Fahrzeughalter kann zivilrechtlich für Schäden haftbar gemacht werden, die Dritten durch das Fahrzeug zugefügt werden. In den meisten Ländern ist der Fahrzeughalter verpflichtet, eine Kfz-Haftpflichtversicherung abzuschließen, die Sach- und Personenschäden Dritter abdeckt, sodass die Opfer eines Unfalls, in den das Auto des Halters verwickelt ist, ein Mindestmaß an Schadensersatz erhalten. Ein Kneipenwirt wird idR nicht für einen Unfall verantwortlich gemacht, der von einem betrunkenen Fahrzeugführer verursacht wurde, es sei denn, der Kneipenwirt hat den Fahrzeugführer dazu veranlasst, nach dem Trinken zu fahren, oder der Kneipenwirt hatte triftige Gründe, die Trunkenheit am Steuer vorherzusehen und aufgrund einer Handlungspflicht zu verhindern. Ein Tierhalter haftet verschuldensunabhängig für die von seinem Tier verursachten Schäden, wird aber idR nicht strafrechtlich belangt.

Um zu bestimmen, wie diese **Regeln in KI-Sachverhalten** anzuwenden und zu interpretieren sind, können die Gerichte allfällige **Analogien** und eine Vielzahl von Argumenten berücksichtigen, die im Laufe der Zeit akzeptiert oder abgelehnt werden. So ist bspw. eine Person auf dem Fahrersitz eines autonomen oder teilautonomen Autos möglicherweise nicht als Fahrzeugführer verantwortlich. Wenn eine KI ein Auto gegen eine weiße Wand steuert, die das KI-System nicht von weißen Wolken am Horizont unterscheiden konnte, mag der Hersteller anstelle oder zusätzlich zu der Verantwortung des Fahrzeughalters verschuldensunabhängig haftbar gemacht werden können. Womöglich sollten Hersteller verpflichtet werden, eine Kfz-Haftpflichtversicherung abzuschließen, und nicht mehr die Fahrzeughalter, denn der relative Grad des Risikos hängt nicht mehr so sehr vom Fahrzeughalter oder menschlichen Fahrzeugführer, sondern weitgehend von der KI im Auto ab. Ob ein Geschädigter beweisen kann, dass der Autohersteller für einen Unfall verantwortlich ist, bei dem zahlreiche Faktoren eine Rolle spielen, wird jedoch jedenfalls neue Untersuchungen erfordern. Nach unserer in diesem Handbuch verwendeten Definition kann niemand die Funktionsweise der KI mit demselben Grad an Sicherheit vorhersagen, erklären oder kontrollieren, wie ein Ermittler einen Programmierfehler in deterministischen Automobilsystemen finden oder, wenn kein Programmierfehler gefunden wird, stattdessen entscheiden könnte, dass externe Faktoren hauptsächlich sind. 25

In Ermangelung einer neuen Gesetzgebung könnten die Gerichte dazu neigen, **KI-Eigentümer und -Besitzer** auf der Grundlage ähnlicher Grundsätze und politischer Erwägungen wie bei der Haftung von Auto- und Tierbesitzern für physische Schäden an Menschen und Sachwerten **strikt haftbar** zu machen. Eine natürliche oder juristische Person, die ein **autonomes Auto**, einen **Roboter** oder eine andere KI besitzt und diese KI für den eigenen Gebrauch oder zur Erbringung von Dienstleistungen für andere 26

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

betreibt oder die KI von anderen betreiben lässt, sollte sich daher darauf einstellen, dass sie für durch die KI verursachte Schäden womöglich streng haftet. Der Eigentümer eines KI-gesteuerten Produkts sollte in Erwägung ziehen, eine **Versicherung für die Haftung gegenüber Dritten** abzuschließen oder sich vom KI-Anbieter entschädigen zu lassen, wie in Kapitel 5 dieses Handbuchs näher erläutert. Der Gesetzgeber könnte in Erwägung ziehen, eine verpflichtende Grund(haftpflicht)versicherung nicht nur für Autos vorzuschreiben, sondern ggf. auch KI-Anbieter zu verpflichten, eine Versicherung für Produkte abzuschließen, bei denen der einzelne Eigentümer oder Betreiber nicht wesentlich zu den von der KI ausgehenden Risiken beiträgt. Im Jahr 2022 veröffentlichte die EU-Kommission den Entwurf einer Richtlinie zur Anpassung der außervertraglichen zivilrechtlichen Haftungsvorschriften an die Künstliche Intelligenz (KI-Haftungsrichtlinie), die die im August 2024 in Kraft getretene EU-KI-VO ergänzen und widerlegbare Vermutungen für Verstöße und Kausalzusammenhänge vorsehen soll.

27 In Bezug auf die **strafrechtliche Verantwortlichkeit** und die **Haftung auf Schadensersatz** verhängen Gerichte idR Strafen, um Schuldige zur Rechenschaft zu ziehen, Kriminelle davon abzuhalten, erneut gegen Gesetze zu verstoßen, sowie die Öffentlichkeit von ähnlichen Straftaten abzuschrecken, Straftäter zu inhaftieren und Verurteilte zu resozialisieren. Menschen können durch die Androhung von Strafen in ihrem Verhalten beeinflusst werden, KI hingegen nicht. Wenn Unternehmen Menschen durch KI ersetzen, könnten sich Strafgesetze und strafrechtliche Haftung als unwirksam erweisen, es sei denn, Gerichte machen Menschen für den bloßen Einsatz von KI oder für Schäden strafrechtlich verantwortlich, die durch unzureichend getestete oder überwachte KI verursacht wurden. In der Praxis hat KI bereits in Strafprozessen eine Rolle gespielt: Im Jahr 2015 erhob das US-Justizministerium Anklage gegen Unternehmen und einzelne Beschuldigte wegen Verstößen gegen das Kartellrecht in einem Fall, in dem es um Preisabsprachen durch Algorithmen ging. Während Mitarbeiter aus Angst vor einer Gefängnisstrafe nach dem Kartellrecht möglicherweise zögerten, sich mit Wettbewerbern auf Mindestpreise zu einigen, stimmte die KI die Preise unmittelbar mit der von Wettbewerbern eingesetzten KI ab, um die wirtschaftliche Rendite zu optimieren.

28 Unternehmen sollten **KI-Risikobewertungen** durchführen, um potenzielle Schäden und **Maßnahmen zur Risikominderung** zu ermitteln, mit dem primären Ziel, Schäden zu verhindern, und dem sekundären Ziel, sich gegen Anschuldigungen und Haftungsansprüche zu schützen. Genauso wie ein Unternehmen das Risiko der Haftung für Handlungen und Unterlassungen von kriminellen Mitarbeitern verringern kann, können Unternehmen die von KI ausgehenden Risiken verringern, indem sie robuste **Compliance-Programme** einführen, wie in den Kapiteln 2 und 3 dieses Handbuchs vorgeschlagen. Wenn Unternehmen erkennbare Risiken identifizieren und abmildern, können sie sich besser gegen den Vorwurf der Verursachung und des individuellen Verschuldens verteidigen. Auf der Grundlage von Risikobewertungen, die in Kapitel 4 dieses Handbuchs vorgeschlagen werden, können Unternehmen entsprechende Leitlinien verfassen, um das Risiko bestimmter Schäden zu verringern. Außerdem können Unternehmen KI-Nutzer und Dritte warnen, um eine riskante KI-Nutzung zu verhindern oder zumindest die Verantwortung für eine riskante KI-Nutzung von den Entwicklern und Anbietern auf die KI-Nutzer zu verlagern, wie in den Kapiteln 5 und 6 dieses Handbuchs vorgeschlagen.

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

III. Eigentumsrechte

In den meisten Gesellschaften und Rechtssystemen können Grundbesitz, Tiere, materielle Güter und geistiges Eigentum erworben werden. Die Rechtsordnungen weisen Einzelpersonen solche **Eigentumsrechte** auch und gerade zu, um Verhaltensweisen zu fördern, die der Allgemeinheit zugutekommen. Ein Landwirt wird bspw. eher Zeit und Ressourcen in den Anbau und die Aufzucht von Tieren investieren, wenn er ein Eigentumsrecht geltend machen kann, um andere davon abzuhalten, sein Grundstück zu betreten und die Früchte seiner Arbeit zu ernten. Hersteller und Händler werden eher motiviert sein, in die Herstellung und den Vertrieb von Werkzeugen und anderen Produkten zu investieren, wenn sie verhindern können, dass andere ihre Produkte und Markenzeichen kopieren und diese Duplikate verkaufen. Autoren und Erfinder investieren in Werke und Erfindungen, wenn sie andere davon abhalten können, ihre Werke zu kopieren oder ihre Erfindungen ohne Entschädigung zu nutzen. Die Öffentlichkeit profitiert von der Verfügbarkeit von Lebensmitteln, Produkten, kreativen Werken und Erfindungen. Mit zahlreichen Regeln und Ausnahmen wägt der Gesetzgeber deshalb ab zwischen den Interessen der Öffentlichkeit und individuellen Ausschlussrechten, um sicherzustellen, dass die Eigentümer ihre Ausschlussrechte nicht unangemessen zum Nachteil anderer nutzen; dabei kommt es zB zu folgenden **Einschränkungen von Eigentumsrechten**: 29

- **Enteignungsverfahren**, die es dem Staat erlauben, Land gegen Entschädigung zu enteignen, um bspw. Straßen, Eisenbahnen, Dämme und andere öffentliche Bauwerke zu bauen.
- Wegerechte und Zugang für benachbarte Grundstückseigentümer.
- Erschöpfungsgrundsätze (sog. „**Erstverkaufsdoktrin**“), die es den Käufern erlauben, rechtmäßige Kopien von Werken, markenrechtlich geschützten Waren oder patentierten Produkten im Interesse des Handels und des Wettbewerbs weiterzuverkaufen.
- Einräumung einer fairen Nutzung im angloamerikanischen Rechtsraum (sog. **Fair-Use-Doktrin**), die es der Öffentlichkeit erlaubt, urheberrechtlich geschützte Werke zum Zwecke der Schaffung neuer, umgestaltender Werke zu vervielfältigen, wenn dies den Markt für die kopierten Werke nicht übermäßig beeinträchtigt.
- **Obligatorische Zulassungsregelungen**, zB zur Sicherstellung bezahlbar erhältlicher Arzneimittel, um Krisen im Bereich der öffentlichen Gesundheit zu verhindern.

Gesetzgeber, Gerichte und Anwälte werden diese **Abwägungsentscheidungen** in KI-bezogenen Sachverhalten nunmehr vielfach neu überdenken müssen. Aufgrund der großen **Autonomie**, in der KI operiert, und des Umstandes, dass KI-Entwickler die Funktionalität oder die Ausgaben (Output) der KI nicht mit Sicherheit vorhersagen, erklären oder kontrollieren können, wird es für Gesetzgeber oder Gerichte in Abhängigkeit von der jeweils betroffenen Rechtsordnung herausfordernd sein, zu bestimmen, ob der KI-Output eine verletzende Kopie des KI-Trainingsmaterials darstellt, ein abgeleitetes Werk, das auf der Grundlage der Grundsätze der fairen Nutzung verteidigt werden kann, ein lizenziertes abgeleitetes Werk, das auf der Grundlage von Nutzereingaben erstellt wurde, oder ein neues Originalwerk, das auf der Kreativität des Entwicklers oder Nutzers beruht. Open-Source-Programmierer, Schriftsteller, Künstler, Comedians und andere Kreative sowie Betreiber von Online- Plattformen haben zahlreiche Klagen 30

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

gegen KI-Entwickler angestrengt, weil die KI-Entwickler Daten und Inhalte ohne Genehmigung abgreifen und dadurch eine Verletzung von Eigentumsrechten in Betracht kommt, wenn KI trainiert wird, die zunehmend in der Lage ist, Kreative zu ersetzen und mit Online-Diensten zu konkurrieren. Daher müssen Unternehmen bei der Entwicklung, Bereitstellung und Nutzung von KI die Risiken der **Verletzungen von Eigentumsrechten** und von sonstigen **Rechtsverletzungen** sorgfältig berücksichtigen.

1. Eigentum an KI, Eingaben (Input) und Ausgaben (Output)

31 Wie bei jeder anderen Technologie können **KI-Entwickler Urheberrechte, Patente und andere geistige Eigentumsrechte an originellen oder neuartigen Systemen** erwerben. KI-Entwickler werden jedoch idR keine Ausschließlichkeitsrechte an den von den Systemen erzeugten Ergebnissen erwerben. Etwas anderes mag gelten, wenn sie nachweisen können, dass die menschlichen Entwickler selbst die Ergebnisse erfunden oder verfasst haben. Im Ausgangspunkt dürften menschliche Entwickler aufgrund der **Autonomie und Unvorhersehbarkeit** der KI-Systeme keine Erfindung oder Urheberschaft an Ergebnissen der KI geltend machen können. Im Gegensatz dazu können Entwickler bei **deterministisch programmierten Systemen** eine engere Verbindung zu den Ergebnissen des Systems nachweisen als bei KI, da Entwickler die Ergebnisse vorhersagen, erklären und kontrollieren können.

32 Manche Ergebnisse sind zu funktional, um urheberrechtlich geschützt zu werden, oder gemeinfrei und ggf. nicht neu genug, um patentrechtlich geschützt zu werden. Bspw. legt der Entwickler eines deterministischen Taschenrechners zwar die Zahl, die der Rechner als Antwort auf eine Eingabeaufforderung liefert, im Voraus fest; diese Zahl kann aber nicht urheberrechtlich geschützt werden, weil sie durch die Mathematik vorgegeben ist. Entwickler von Videospielen hingegen erstellen Grafiken für Figuren und Hintergründe, die urheberrechtlich schützbare Werke darstellen. Bei Textverarbeitungsprogrammen fügen Entwickler einige vorgegebene kreative Elemente in die Nutzeroberflächen ein, die die Systeme auf den Bildschirmen der Nutzer erzeugen und die dem Urheberrecht des Entwicklers unterliegen. Entwickler von Textverarbeitungsprogrammen überlassen es jedoch vollständig den Nutzern, Text mithilfe der Software zu erstellen, sodass der Entwickler keine Grundlage für die Geltendmachung von Urheberrechten an der vom Nutzer erzeugten **Ausgabe** hat. Bei deterministischen Systemen kann die Ausgabe idR entweder durch Handlungen des Entwicklers oder des Nutzers erklärt werden, was die Zuweisung von Urheberrechten an der Ausgabe relativ einfach macht.

33 **Nutzer von KI** können **Urheberrechte** an kreativen Beiträgen und möglicherweise **Patente** auf Erfindungen innehaben, indem sie neuartige Eingabeaufforderungen oder andere Eingaben an das KI-System aufbauen. Ebenso wie die Entwickler von KI-Systemen können aber auch die Nutzer von KI-Systemen idR keine Urheberrechte oder Patente für die Ergebnisse des KI-Systems erwerben. Das Maß an Kreativität oder erfinderischer Innovation, das ein Nutzer in die Entwicklung von Eingabeaufforderungen oder in andere Eingaben investieren kann, wird idR zu geringfügig sein im Vergleich zu der Menge an wertvollen Informationen und Problemlösungsfortschritten in der KI-Ausgabe. Darüber hinaus kann ein KI-Nutzer die Ausgabe nicht in vergleichbarer Weise

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

vorhersagen, erklären oder kontrollieren, wie demgegenüber ein Nutzer die Ausgabe eines deterministischen Systems vorhersagen, erklären oder kontrollieren kann, zB die Ausgabe in Form eines Textes, den ein Nutzer mit einem Textverarbeitungsdokument schreibt. In den meisten Fällen wird man daher davon ausgehen müssen, dass die Ausgabeergebnisse (Output) von KI-Systemen nicht durch Urheberrechte, Patente oder andere Rechte an geistigem Eigentum geschützt ist.

34 Gerichte werden voraussichtlich zu dem Schluss kommen, dass es mit dem Telos der Gesetze zum Schutz des geistigen Eigentums durchaus vereinbar ist, dass **KI-Output** idR **nicht für den Schutz des geistigen Eigentums in Frage kommt**, weil der Gesetzgeber solche Rechte des geistigen Eigentums vor allem zu dem Zweck gewährt hat, Menschen zu Innovationen im öffentlichen Interesse zu ermutigen. Gerichte, Urheberrechts- und Patentämter in den USA haben idS bereits den Urheberrechtsschutz für Fotos verweigert, die von einem Affen mit einer Kamera erstellt wurden, sowie Anträge auf Urheberrechte und Patente für Werke und Erfindungen zurückgewiesen, die von KI erzeugt wurden. Nach den Gesetzen zum Schutz des geistigen Eigentums werden menschliche Erfinder mit Patenten, Urheberrechten und anderen Rechten am geistigen Eigentum belohnt, wenn sie Erfindungen machen und künstlerische Werke schaffen. Inhaber von Rechten an geistigem Eigentum können ihre Innovationen zu Geld machen, indem sie von anderen Lizenzgebühren für die Nutzung oder den Verkauf ihrer Erfindungen oder die Anfertigung von Kopien ihrer Werke verlangen oder indem sie andere vom Markt ausschließen und selbst höhere Preise für Kopien und Produkte verlangen – wobei dies stets unter dem Vorbehalt der Vorgaben des Kartellrechts steht. Der Gesetzgeber gewährt solche Anreize, um Innovation und Fortschritt im öffentlichen Interesse zu fördern, so wie Grundeigentümer durch Eigentumsrechte ermutigt werden, ihr Land zu bebauen oder zu bewirtschaften, und Eigentümer von beweglichen Gütern durch Eigentumsrechte ermutigt werden, Werkzeuge und andere nützliche Produkte herzustellen. Zu diesem Zweck erhalten KI-Entwickler geistige Eigentumsrechte an der Entwicklung von KI.

35 Hat ein Entwickler aber erst einmal KI geschaffen, besteht zumeist gerade keine Notwendigkeit, für Anbieter oder Nutzer allfällige Anreize zu schaffen, um KI-Ausgaben (Output) zu erzeugen. Maschinen brauchen keine rechtlichen Anreize und profitieren auch nicht davon. KI-Anbieter sorgen hauptsächlich dafür, dass die Systeme mit Strom versorgt, angeschlossen und sicher sind. Nutzer können etwas kreative Energie investieren, wenn sie innovative Aufforderungen (**Prompts**) für die KI-Anwendungen entwickeln, aber ihr Beitrag zum KI-generierten Output ist gleichwohl oft relativ gering. Daher dürften die Nutzer zumeist nicht als diejenigen anzusehen sein, die in erster Linie für Innovationen verantwortlich sind, wenn KI eine Ausgabe erzeugt. Dementsprechend wird der Gesetzgeber möglicherweise keine Notwendigkeit sehen, die Gesetze zum geistigen Eigentum zu ändern, um Eigentumsrechte an den von KI erzeugten Ergebnissen zu gewähren. Gesetzgeber könnten es vielmehr für ausreichend halten, dass KI-Entwickler mit Eigentumsrechten an den von ihnen entwickelten Systemen belohnt werden.

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Stichwortverzeichnis

Die **fetten** Zahlen verweisen auf den Paragrafen (das Kapitel), die mageren auf die Randnummer.

Abhilfemaßnahmen **3** 37, **5** 13, **6** 31 f.
AEDT **1** 27, **2** 6, **3** 18, **4** 32, **5** 28 f., 80, **8** 2
– Anwendungsbereich **5** 28 f.
Affero GPL **7** 6
Age-Appropriate Design Code **5** 33, 115
Aggregation **2** 69
Algorithmus **7** 7
Allgemeine KI (AGI) **1** 7
Anbieter **1** 2, 10, 23, 29, 35, 37, **2** 11 f., 14 ff., 20, 26, 35 f., 38, 42, 63 f., 66 f., 70 f., 77, 86, **3** 6, 17 f., 40, 42, 49 f., **4** 8, 13 f., 21, 24, 41 ff., 45, 52, 60, 62, 67, **5** 29 f., 44, 49 ff., 58, 60 ff., 67, 69 f., 72, 84, 86, 88 f., 91, 99, 102, 105, 107 ff., 114, 121, **6** 1, 4, 10 ff., 14 ff., 23 ff., 30, 33 ff., 42 ff., 46, **7** 5 f., **8** 14, 21, 23
– Begriff **Vor** 9
– Geschäftsgeheimnis **2** 53
Anonymisierung **2** 68, 70 f., **5** 89, 91, **8** 22
Anthropomorphismus **5** 60, 73
– Begriff **Vor** 10
Anwaltsgeheimnis **4** 24, 27 ff., 34, **5** 27, 98
Anwendungsprogrammschnittstellen (API) **4** 21, **6** 10
Arbeitnehmer **3** 40, **4** 50 f., 54, 56, **5** 79
Audit **4** 31, 34, 42, **5** 98, 103, 106 f., 110, **6** 25, 35 ff., **8** 3 f., 9, 13, 23
Auditkontrollen **8** 10 ff.
Aufgabenliste **3** 1, 26 ff., 36, 38
Aufsichtsinstitutionen **1** 39
– Durchsetzung **3** 7, 50, **5** 18, 21, 95, **6** 5, 44
– Equal Employment Opportunity Commission (EEOC) **2** 59
– Ermittlungen **3** 28
– Federal Trade Commission **5** 20, 118 f.
– Governance **2** 7, **3** 12, **4** 67, **5** 25, 52 f., **8** 3
– Überwachung **1** 39, **3** 7, 16, 26, **4** 48, 52, 54, **5** 53, 79 f., 83, 93, 102, 105 f., 114, **6** 10, **8** 24 f.
Aufzeichnungen über Datenverarbeitungstätigkeiten **3** 33
Ausfuhrkontrollen **5** 110
Ausgabe **1** 10, 12, 15, **2** 32 f., 36 f., 42, 62 ff., 67, 77, **3** 6, 42, **4** 15, 43, 59 f., **5** 1, 43, 49, 70, 80, 88 f., **6** 24, 26 f., 30, 35 ff., **7** 5
Auslagerung **5** 104
Ausrichtung **5** 44
Automated employment decision tools (AEDTs) **1** 27, **2** 6, **3** 18, **4** 32, **5** 28 f., 80, **8** 2
– Anwendungsbereich **5** 28 f.
Automatisierung **1** 3, **3** 22 ff., **4** 10, **5** 95, **8** 15 ff.
Autonome Replikation **5** 45
Autonomes Auto **2** 26
Autonomie **1** 4, 9, 11, 13 f., 17, **2** 30 f., 59, **4** 66, **5** 34, 37, 44 ff.
Autovervollständigung **2** 63 f., **5** 62

Berechtigtes Interesse (Ausnahme) **4** 28, 47
Bescheinigungen **5** 110, **6** 35 ff.
Besitzer, Haftung **2** 26
Best Practices **4** 1, 13, **5** 122
Bias **5** 40 ff., 106, **6** 25
Big Data **2** 71
Binding Corporate Rules (BCR) **2** 81
Biometric Information Privacy Act (BIPA) **5** 54
Biometrische Daten **5** 54, 57
Black Duck **2** 43
Bot **2** 4, 45, **5** 65, 99
Botnet **5** 45
Bug-Bounty **5** 98
Bug-Bounty-Programm **5** 74
Bürokratie **8** 5

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Business & Professions Code **2** 4

California Age-Appropriate Design Code Act (CAADCA) **4** 26, **5** 5, 33, 115
California Consumer Privacy Act (CCPA) **1** 34, **2** 52, 72, 76, **4** 8, 34, 66, **6** 4, 17, 19 f., **8** 2
California Online Privacy Protection Act of 2003 (CalOPPA) **4** 8
CAPTCHA **2** 47, **5** 82, **7** 7
CDA (Communications Decency Act) **5** 49, 69
Central Processing Unit/Zentrale Recheneinheit (CPU) **1** 12
ChatGPT **1** 16, **5** 23
Children's Online Privacy Protection Act (COPPA) **5** 118 f.
Click-Through-Vereinbarungen **5** 22
CMIA (Confidentiality of Medical Information Act) **4** 50
Colorado **1** 2, **2** 7 ff.
Colorado Act für KI, artificial intelligence system **1** 21
Commerce Clause **3** 50
Common Rules **4** 26, 46
Communications Decency Act (CDA) **5** 49, 69
Compliance **Vor** 1 ff., 11 ff., **2** 19, 28, 81, **3** 1 ff., **4** 1, 26 ff., **5** 14, 16, 18, 24 ff., 105 ff., **6** 1 f., 20, **8** 2 ff.
– Begriff **Vor** 3, 11
– Lückenbewertung **4** 34
– Nachweis **4** 31 ff.
Compliance-Beauftragter **3** 2, 7, 14, **8** 9, 13
Compliance-Dossier, Aufzeichnungen **4** 33
Compliance-Manager **3** 16
Compliance-Programm **2** 28, **3** 1 ff.
Confidentiality of Medical Information Act (CMIA) **4** 50
Connecticut **2** 5
COPPA (Children's Online Privacy Protection Act) **5** 118 f.
Copyleft **2** 41
CPU *siehe* Central Processing Unit/Zentrale Recheneinheit (CPU)
Crawler **2** 45, **4** 26, **7** 7
Customer Relationship Management (CRM) **5** 105
Cybersicherheit **2** 55, **5** 73, 96, 98

DALL-E **2** 13
Dark Patterns **4** 48, 57, 66
Data Controller **2** 81
Datenaufbewahrung **2** 82 ff., **4** 26, **5** 95
Datenbroker **7** 7
Datenlokalisierung **2** 83
Datenminimierung **2** 76, 81, **4** 76
Datenraum **8** 21
Datenrechte **2** 50 ff.
Datenresidenz (Data Residency) **2** 82 f., **5** 95
Datenschutzbeauftragter **1** 40, **2** 81, **3** 2 f., 14, 33, **4** 15, 26, 35, 39, **5** 18 f., **6** 28
– Verzeichnisse über Verarbeitungstätigkeiten (VVZs) **4** 69
Datenschutzbehörde **5** 18, 20, 23, 32
Datenschutzerklärung **4** 8, 41, 52, 65, **5** 118
Datenschutz-Folgenabschätzung (DSFA) **2** 78, 81, **3** 24, **4** 35 ff., 39, **5** 4, 30 ff., 80, 91, 106, 122, 125, **6** 25
– Age-Appropriate Design Code **5** 33
– CAADCA **5** 33
– DS-GVO **3** 34
– Legal Tech **3** 23
Datenschutzgesetz **1** 33, **2** 79, **4** 50
Datenschutz-Grundverordnung (DS-GVO) **1** 24, **2** 66, **4** 10, 32 ff., 40, **5** 5, 38, **6** 8, 17, 19 ff., **8** 3
– Aufbewahrungsfristen **5** 94
– Bußgelder **5** 18
– Compliance Anforderungen **2** 81
– Datenschutz-Folgenabschätzung (DSFA) **2** 78, 81, **3** 34, **4** 35, **5** 4, 30 ff., 80, 106
– Datenschutzhinweise **2** 81, **4** 8
– Datenverarbeitungsverträge (DVV) **4** 24

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

– Einwilligung **4** 49
– Löschung **2** 77
– Minderjährige **5** 121
– personenbezogene Daten **2** 67 ff.
– Verarbeitung **2** 74
– Verzeichnisse über Verarbeitungstätigkeiten (VVZs) **4** 69
– Zweckbindung **2** 76
Datenschutzhinweis, DS-GVO **2** 81, **4** 8
Datensicherheit **2** 53 ff., 85, **3** 50
Datensouveränität **2** 83
Datenspeicherort **2** 83
Datenspeicherung **2** 84, **4** 67, **5** 94 f.
Datenverarbeitungsverträge (DVV) **2** 81, **4** 17, 24, **7** 5, **8** 12
Datenverarbeitungsvorschriften **2** 55 f., 65 f., **5** 91
– EU und Japan **1** 25
Dawn Raids **4** 24
Deepfakes **5** 47 f., 113
Deep-Linking **2** 46
De-Identifizierung, De-Anonymisierung **2** 70
Deliktsrecht **2** 23 ff.
Deterministische Systeme **1** 4, 10, 13, **6** 35 ff.
– Begriff **Vor** 12
– Urheberrechte **2** 32
Deutschland **1** 31 f.
– Minderjährige **5** 121
Dienstleister, Anwendungsbereich **1** 29, **2** 47, 55, **3** 43, **4** 60, **5** 66, 68, 106, **6** 4, 15, 27, 30 f., **8** 23
Digital Millennium Copyright Act (DMCA) **5** 69
Diskriminierungsschutz **2** 58 ff.
Dokumentation **2** 16, **3** 23, 27 f., 33, 42, 57, **4** 1 ff., 5 ff., 10, 14, 25 ff., 30, 33, 36 f., 51, **5** 1, 80, 95, 122, **6** 35 ff., **7** 6, **8** 3 ff.
– Erstellung **4** 1 ff.
– geschäftliche Gründe **4** 13 ff.
– Nachweis der Compliance **4** 31
– organisatorische Gründe **4** 16
– rechtliche Grundlage **4** 8 ff.
– Zielgruppe **4** 19 ff.
Dossier **4** 34
DS-GVO (Datenschutz-Grundverordnung) **1** 24, **2** 66, **4** 10, 32 ff., 40, **5** 5, 38, **6** 8, 17, 19 ff., **8** 3
– Aufbewahrungsfristen **5** 94
– Bußgelder **5** 18
– Compliance Anforderungen **2** 81
– Datenschutz-Folgenabschätzung (DSFA) **2** 78, 81, **3** 34, **4** 35, **5** 4, 30 ff., 80, 106
– Datenschutzhinweise **2** 81, **4** 8
– Datenverarbeitungsverträge (DVV) **4** 24
– Einwilligung **4** 49
– Löschung **2** 77
– Minderjährige **5** 121
– personenbezogene Daten **2** 67 ff.
– Verarbeitung **2** 74
– Verzeichnisse über Verarbeitungstätigkeiten (VVZs) **4** 69
– Zweckbindung **2** 76
Due-Diligence **4** 32, **5** 87
– Lieferanten **8** 23
– Prüfung **5** 107 f., **8** 7, 18 ff.
Durchsetzung, Aufsichtsinstitutionen **3** 7, 50, **5** 18, 21, 95, **6** 5, 44
DVV (Datenverarbeitungsverträge) **2** 81, **4** 17, 24, **7** 5, **8** 12

Eigentum **2** 29, **3** 42, **5** 2, 17, 70, **7** 7
– Daten **2** 50 ff., **6** 27
– Datenbank **2** 51
Eigentum, geistiges **1** 2, 29 f., **2** 3, 29 ff., 33 ff., **5** 9, 71 f., 79, 104, **6** 24, **7** 6
– Rechtsverletzungen **2** 36 ff.
Eingabe **1** 12, **5** 77, **6** 14, 16 f., 26, 30, 35 ff., **7** 5
Einwilligung **2** 52, 65, 81, **3** 1, 51, **4** 24, 45 ff., 52, 56 f., 60, **5** 51, 53, 115, 118, 120 f., **6** 7 f., 17, 22, 24, **7** 6
– Auffälligkeit **4** 55
– Einbeziehung von Hinweisen **4** 63
– gebündelte Einwilligung **4** 58
– Rechtswirksamkeit **4** 49 ff.
– Schweigen **4** 56

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

– Standard-Einwilligungserklärungen **4** 51 ff.
– Zeitpunkt **4** 54
Entschädigung **2** 29, 48, 52
Entwickler **1** 35 f., **2** 66, 71, 77, **3** 6, 25, 40, 42, **4** 26, **5** 37, 51, 65, 72, 84, 91, **6** 1, 12, 25, 35 ff.
– Begriff **Vor** 13
– Bot **2** 45
– Eigentum an KI, Input und Output **2** 31 ff.
– Geschäftsgeheimnis **2** 53
– Open-Source-Code **2** 39 ff.
– Rechte der Datenbankbesitzer **2** 51
– Scraping-Technologien **2** 45
– Verarbeitung **2** 74 f.
– Web-Crawler **2** 45
Equal Employment Opportunity Commission (EEOC), Aufsichtsinstitutionen **1** 39, **2** 59
Ermittlungen, Aufsichtsinstitutionen **3** 28
ERP (Unternehmensressourcenplanung) **5** 105
ESG (Environmental, Social and Governance) **5** 25, 51 ff.
Ethik **5** 50
Ethikkommission **4** 46
EU-KI-VO **2** 10 ff., 14 f., 17 ff., 26, **5** 5
– General Purpose AI (GPAI) **2** 13
– KI-System **1** 20
– risikobasierter Ansatz **2** 15
– sachlicher Anwendungsbereich **2** 13 f.
– Sanktionen **2** 17
Europäischer Datenschutzausschuss, gebündelte Einwilligung **4** 58
Europäische Union (EU) **1** 2, **2** 3
– Aufgabenliste **3** 28
– Einwilligung, Datenschutzrecht **4** 47
– Standardvertragsklauseln (Standard Contractual Clauses/SCCs, auch Musterklauseln genannt) **3** 53
EU-U.S. Data Privacy Framework **2** 81
EWR+ (Europäischer Wirtschaftsraum+) **2** 66, 81, **6** 4, 17, 22
– Niederlassung **2** 80
EWR (Europäischer Wirtschaftsraum) **3** 49 f., **6** 4, 17
– Durchsetzbarkeit der Gesetze **3** 51
– Minderjährige **5** 121
– Niederlassung **2** 80

Fair Credit Reporting Act (FCRA) **4** 50
Fair use **2** 42
– -Test **3** 24
– -Verteidigung **2** 38
FAQs **7** 6
FCRA (Fair Credit Reporting Act) **4** 50
Federal Trade Commission (FTC) **5** 23
– Aufsichtsinstitutionen **1** 39, **5** 20, 118 f.
Filter **5** 89, 114
Folgenabschätzung **1** 19, **5** 1 ff., 53, 79
– Vertraulichkeit **5** 27
Force majeure (höhere Gewalt) **6** 46
Forschung am Menschen **5** 51
Fragebögen **5** 107
Free Software Foundation (FSF) **2** 41, **7** 6
FTC (Federal Trade Commission) **5** 23
– Aufsichtsinstitutionen **5** 20, 118 f.
Fusionen und Übernahmen (M&A) **4** 11, 32, **8** 18 ff.

Garante, ChatGPT **5** 23
Garantien **4** 38, **5** 21, 100, **6** 32, 34 ff., **7** 6
Geistiges Eigentum **1** 2, 29 f., **2** 3, 29 ff., 33 ff., **5** 9, 71 f., 79, 104, **6** 24, **7** 6
– Rechtsverletzungen **2** 36 ff.
Genehmigung **3** 53 f., **4** 46, **5** 30, **7** 7
General Public License (GPL) **2** 40, **7** 6
General Purpose AI (GPAI), EU-KI-VO **2** 13, 16
Geschäftsgeheimnis **2** 53 ff., **5** 84 f., 104
Geschäftspartner **3** 43 f., 53, **4** 12, 33, 48, **5** 15, 76, 109
Gesetze über Computereingriffe, Anwendungsbereich **3** 6, 37

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Gesetz über Computerbetrug und -missbrauch *siehe* United States Computer Fraud and Abuse Act (CFAA)
Gesetz zum Schutz der Privatsphäre von Kindern im Internet *siehe* Children's Online Privacy Protection Act (COPPA)
Gesichtserkennung **5** 38, 53 ff.
Gesundheitsinformationen **5** 5
Github/Gitlab **2** 39, 43
Google BERT **2** 13
Governance **3** 28
– Aufsichtsinstitutionen **2** 7, **3** 12, **4** 67, **5** 25, 52 f., **8** 3
GPAI-Systeme (General Purpose AI), Colorado **2** 9
GPL (General Public License) **2** 40, **7** 6
GPT-4 **2** 13
Grundrechtecharta **2** 10

Haftung **1** 10, 35, **2** 4, 26 ff., 63, **3** 17, 42, **4** 18, 24, 36, 41, 43, **5** 10 f., 13 f., 21, 49, **6** 1, 32, 35 ff., 42, 44
– Schaden durch KI **6** 23
Halluzination **5** 60, **6** 35 ff.
Health Insurance Portability and Accountability Act (HIPAA) **2** 70, **3** 43, **4** 24, 26, 46, 50, **5** 5, 98, 109, **6** 4, 19, 21
Herkunftslandprinzip **3** 50
Hessen **1** 33, **2** 79
Hintergrundüberprüfungen **5** 103
HIPAA (Health Insurance Portability and Accountability Act) **2** 70, **3** 43, **4** 24, 26, 46, 50, **5** 5, 98, 109, **6** 4, 19, 21
Höhere Gewalt **6** 46

ICO (UK Information Commissioner's Office) **8** 2
Illinois
– Biometric Information Privacy Act (BIPA) **5** 54
Indonesien, Datenresidenz **2** 82
Industriestandards **2** 87
Input (Eingaben), Begriff **Vor** 14
Intelligenz **1** 6
– Maschine **1** 8
Interim Measures for the Management of Generative Artificial Intelligence Services **2** 20
Internet Service Provider/Internetdienstanbieter (ISP) **3** 48, **5** 49, 69
IP-Adresse (Internet Protocol-Address) **7** 7
ISO (Internationale Organisation für Normung) **5** 98
ISP (Internet Service Provider) **3** 48, **5** 49, 69
Italien, ChatGPT **5** 23

Jailbreak **5** 73, 82
Japan **1** 25, **2** 38, **5** 67
– Aufgabenliste **3** 28

Kalifornien **1** 27, **4** 25, 40, **5** 33
– Bot **2** 4
– Business & Professions Code **2** 4
– CAADCA (Gesetz zur altersgerechten Gestaltung) **4** 26, **5** 5, 33, 115
– California Consumer Privacy Act/ Kalifornisches Gesetz zum Schutz der Privatsphäre der Verbraucher (CCPA) **1** 34, **2** 52, 72, 76, **4** 8, 34, 66, **6** 4, 17, 19 f., **8** 2
– CalOPPA Kalifornisches Gesetz zum Schutz der Privatsphäre im Internet **4** 8
– CCPA (California Consumer Privacy Act) **1** 34, **2** 52, 72, 76, **4** 8, 34, 66, **6** 4, 17, 19 f., **8** 2
– CMIA (Confidentiality of Medical Information Act/Gesetz über die Vertraulichkeit medizinischer Informationen) **4** 50
– Daten **2** 52
– Datenschutzbehörde **5** 20
– Kalifornisches Gesetz zum Schutz der Privatsphäre im Internet (CalOPPA) **4** 8
– Meldung von Datenschutzverletzungen **2** 57
– Minderjährige **5** 120
– Privacy by Design **4** 62

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Kalifornisches Gesetz zum Schutz der Privatsphäre im Internet (CalOPPA) **4** 8
Kalifornisches Gesetz zur altersgerechten Gestaltung (CAADCA) **4** 26, **5** 5, 33, 115
Kanada, Datenschutz-Folgenabschätzungen **4** 36
Kartellrecht **2** 27
KI-Gesetze **1** 2, **2** 1 ff.
KI-Haftungsrichtlinie **2** 26
KI-System mit hohem Risiko, Colorado **2** 7 f.
Klinische Studien **4** 46, **5** 51
Kommerzielle Risikoverteilung **6** 6, 32
Kontrolle **1** 4, 9, 11, 14, 17, 22, **2** 79, **4** 59, **5** 43 ff., 49, 68 f., **6** 17, 35 ff., **7** 6
Konzerninterne Vereinbarungen **3** 28
Künstliche Intelligenz (KI) **1** 20
– Begriff **Vor** 15
– Definition **1** 4 ff., 9 f., 17 f., 20 ff.

Large Language Model (LLM) **1** 15 f., **2** 67, 77, **5** 60 ff., 86, 88, **6** 18, 29, 35 ff.
Latenzzeit **6** 35 ff.
Legal Tech **3** 23
Leistungsbeschreibungen **4** 9, **5** 100, **6** 21
Leitlinie **3** 39, **4** 72, **7** 1, 5 ff.
– Erstellung **7** 4
Lesser GPL **7** 6
Litigation Hold **2** 84
Löschung **2** 76 f., 81, 84, 86, **3** 33, **4** 67, **5** 23, 45, 89, 91, 95, 98, **7** 7
Lückenbewertung **4** 34

M&A (Fusionen und Übernahmen) **4** 11, 32, **8** 18 ff.
Marktortprinzip **2** 12
Meldung von Datenschutzverletzungen **2** 57
Midjourney 5.1 **2** 13
Minderjährige **5** 33, 115 ff., 122, 125, **7** 7
– Deutschland **5** 121
– DS-GVO (Datenschutz-Grundverordnung) **5** 121
– EWR (Europäischer Wirtschaftsraum) **5** 121
– Kalifornien **5** 120
– Österreich **5** 121
– Vereinigte Staaten von Amerika **5** 118
Mining **1** 29
Mitteilung über finanzielle Anreize **2** 52
Modellkarten **5** 100, **6** 25
Monetarisierung **4** 67

National Institute of Standards and Technology (NIST) **5** 98
NDA (Non-disclosure agreement/Vertraulichkeitsvereinbarung) **2** 55
New York City **1** 27
– automated employment decision tools (AEDTs) **2** 6, **3** 18, **4** 32, **5** 28 f., 80, **8** 2
– BIAS-Audits **5** 106
– Local Law 144 aus 2021 **4** 32, **5** 28 f., 80, **8** 2
NIST (National Institute of Standards and Technology) **5** 98
Non-disclosure agreement/Vertraulichkeitsvereinbarung (NDA) **2** 55
Nutzer, Begriff **Vor** 16

Occupational Safety and Health Administrations (OSHAs) **5** 80
Offener Quellcode **2** 37, 39 ff., **5** 86 f., **7** 6
Offenlegung **4** 67, **5** 94, 98 ff., **7** 6, **8** 22
Ökologische und soziale Governance (ESG) **5** 25, 50, 52 f.
Open-Source-Code **2** 39 ff.
Open-Source-Software (OSS) **7** 6
Opt-In **4** 51 ff., 58, **5** 38
– darüber hinausgehende Einwilligung **4** 59
Opt-Out **2** 75, **3** 28, **4** 51 ff., **5** 38, **6** 4, 17
Ordre public **6** 44
Orientierung für Datenschutzbeauftragte **3** 2 f.
– Aufsichtsinstitutionen **3** 33, **4** 39, **5** 18
OSHAs (Occupational Safety and Health Administrations) **5** 80

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

OSS (Open Source Software) **7** 6
Österreich, Minderjährige **5** 121
Output (Ausgaben), Begriff **Vor** 17

Pandemie **5** 48, **6** 46
Parameter **3** 11
Pareto-Prinzip **3** 40
Payment Card Industry/Zahlungskartenindustrie (PCI) **4** 26, **5** 98
PCI-Normen (Payment Card Industry-Normen) **5** 98
Personenbezogene Daten **3** 39, **4** 68, **5** 88, **6** 4, 8, 17, 22, 27, 35 ff.
– CCPA (California Consumer Privacy Act) **2** 72
– DS-GVO **2** 67 ff.
– Einwilligung **4** 49
– Kinder **2** 81
– Verarbeitung **2** 75
Persönliche Daten
– Anwendungsbereich **2** 52, **4** 45, **5** 61, **6** 21
– Aufsichtsinstitutionen **2** 52, **4** 45, **5** 61, **6** 21
Plattform **5** 49, 69, 125
Privacy by Design **4** 37, 62
Privacyville **4** 61
Privatsphäre **2** 83
Produktsicherheit **2** 23 ff.
Profiling **5** 20
Prompt **2** 35, **4** 26, **5** 70, 77 f., **6** 10
Pseudonymisierung **2** 68 f.

Quick wins **3** 36, 56

Rechenschaftspflicht **3** 14
Rechtsverletzung **1** 10, **2** 30, 35 f., **5** 12, 49, 72, **6** 35 ff., **7** 6
Records of processing activities/Aufzeichnungen über Verarbeitungstätigkeiten (RoPA) **2** 81
Reinforcement learning **1** 14, 36
Rights of Publicity **2** 65
Risiken, KI-Entwicklung **2** 2
Risikobewertung **2** 28, **6** 25, **8** 12
Risikomanagementpolitik, Colorado **2** 8
Risikomanagementprogramm, Colorado **2** 8
Risikominimierung **2** 28, **5** 1 ff., 39, 43
Risikoverteilung **6** 32
Risikozuweisungsklauseln **6** 6
RL 95/46/EG **2** 79
Roboter **2** 26, 46 f., **6** 23
Rotes Team/red team **3** 11, **5** 74, 98, 112, 114
Russland, Datenresidenz **2** 82

SaaS (Software-as-a-Service) **4** 41, **7** 6
San Francisco, Gesichtserkennung **5** 55
SCCs (Standard Contractual Clauses/Standardvertragsklauseln, auch Musterklauseln genannt) **3** 53, **5** 75, 109, **6** 5, 35 ff., **8** 12
Schwärzung **2** 68 f., 71, **8** 22
Scraping **4** 24, 26, 46
– Anwendungsbereich **1** 29, **2** 45 ff., 49, 52, 73, 81, **4** 46, 48, **5** 64 ff., 76, **7** 7
Selbstbeurteilung **5** 107
Sensible Daten **5** 67
Service Level **6** 35 ff.
Service Level Agreements/Zusatzvereinbarung über die Dienstgüte (SLA) **6** 35 ff.
Service Organization Controls (SOC) **5** 98
Siegel **8** 14
SLA Service Level Addendum **6** 35 ff.
Social Engineering **5** 96, 98
Software-as-a-Service (SaaS) **4** 41, **7** 6
Sorgfaltspflicht **4** 18, 24
Soziale Medien **6** 22
Spam **3** 43, **5** 100, 102
Standardvertragsklauseln (Standard Contractual Clauses/SCCs, auch Musterklauseln genannt) **3** 53, **5** 75, 109, **6** 5, 35 ff., **8** 12
Steuer **2** 84
Steward **3** 11
Strafrecht **2** 23 ff., **5** 16
Suchmaschine **2** 63
Supervised learning **1** 14
Synthetisch **2** 68, **5** 47, 64, 72, 90

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

Systemverantwortlicher **3** 28
Systemverwalter **1** 18, **3** 15 f., **8** 3, 12

Technical, administrative, and organizational data security measures (TOMs) **2** 57, **3** 33, **4** 26, 67, **5** 98, 110, **6** 30
Technische Spezifikationen **6** 11, 34 f.
Technische Unterstützung **2** 45
Territorialitätsprinzip **1** 23
Territorialprinzip **3** 47
TOMs *siehe* Technical, administrative, and organizational data security measures (TOMs)
Trainingsdaten **5** 65, 72, 90, **6** 10, 35 ff.
– Aufbewahrung **5** 94
Turing, Alan **1** 8

U.S. Computer Fraud and Abuse Act **3** 37, 42, 47
Überwachung, Aufsichtsinstitutionen **1** 39, **3** 7, 16, 26, **4** 48, 52, 54, **5** 53, 79 f., 83, 93, 102, 105 f., 114, **6** 10, **8** 24 f.
UK Age Appropriate Design Code **5** 33, 115
UK ICO (UK Information Commissioner's) **8** 2
United States Computer Fraud and Abuse Act (CFAA) **2** 45, 47 f., **4** 46, **5** 65, 72
Unterauftragnehmer **5** 110
Upload-Filter **3** 23
Urheberrecht **2** 32, 36 ff., **3** 24, **4** 48, **5** 16, 64, 67, 69, 71, **6** 10, 16, 35 ff., **7** 6
– Open-Source-Code **2** 40
USA **1** 27, 30, **5** 67
– AEDT **5** 28 f., 80, **8** 2
– Aufgabenliste **3** 28
– Automated employment decision tools (AEDTs) **5** 28 f., 80, **8** 2
– Biometric Information Privacy Act (BIPA) **5** 54
– BIPA **5** 54
– CAADCA **4** 26, **5** 5, 33, 115
– California Consumer Privacy Act/ Kalifornisches Gesetz zum Schutz der Privatsphäre der Verbraucher (CCPA) **1** 34, **2** 52, 72, 76, **4** 8, **6** 4, 17, 19 f., **8** 2
– CalOPPA Kalifornisches Gesetz zum Schutz der Privatsphäre im Internet **4** 8
– CCPA (California Consumer Privacy Act) **1** 34, **2** 52, 72, 76, **4** 8, **6** 4, 17, 19 f., **8** 2
– CDA (Communications Decency Act) **5** 49, 69
– CFAA (United States Computer Fraud and Abuse Act) **2** 45, 47 f., **4** 46, **5** 65, 72
– Children's Online Privacy Protection Act (COPPA) **5** 118 f.
– Click-Through-Vereinbarungen **5** 22
– CMIA (Confidentiality of Medical Information Act/Gesetz über die Vertraulichkeit medizinischer Informationen) **4** 50
– Commerce Clause **3** 50
– Communications Decency Act (CDA) **5** 49, 69
– Confidentiality of Medical Information Act/Gesetz über die Vertraulichkeit medizinischer Informationen (CMIA) **4** 50
– Datenbanken **2** 51
– Datenschutz-Folgenabschätzungen **4** 36
– Equal Employment Opportunity Commission (EEOC) **1** 39, **2** 59
– Fair Credit Reporting Act (FCRA) **4** 50
– Fair use-Test **3** 24
– Fair use-Verteidigung **2** 38
– FCRA (Fair Credit Reporting Act) **4** 50
– Federal Trade Commission (FTC) **1** 39, **5** 20, 23, 118 f.
– Formularverträge **5** 22
– Health Insurance Portability and Accountability Act (HIPAA) **2** 70, **3** 43, **4** 24, 26, 46, 50, **5** 5, 98, 109, **6** 4, 19, 21

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.

https://www.nomos-shop.de/isbn/978-3-7560-0989-3

– Kalifornisches Gesetz zum Schutz der Privatsphäre im Internet (CalOPPA) **4** 8
– Kalifornisches Gesetz zur altersgerechten Gestaltung (CAADCA) **4** 26, **5** 5, 33, 115
– KI-Gesetze **2** 4 ff.
– National Institute of Standards and Technology (NIST) **5** 98
– Occupational Safety and Health Administrations (OSHAs) **5** 80
– private Rechtsstreitigkeiten **5** 21
– Rights of Publicity **2** 65
– U.S. Computer Fraud and Abuse Act **3** 37, 42, 47

Validierung durch Dritte **5** 93
Verarbeitung, DS-GVO **2** 74 f.
Verbindlich **7** 6
Verbraucherzentrale Bundesverband **5** 19
Vereinbarungen **4** 24, 48, 67, 70 f., **5** 11, 22, 59, 75, 125, **6** 1 ff., 5, 7 ff., 27
– zur Datenübermittlung **4** 67
Vereinigtes Königreich
– Age-Appropriate Design Code **5** 33, 115
– Data Controller **2** 81
– ICO (UK Information Commissioner's Office) **8** 2
Vereinigte Staaten von Amerika *siehe* USA
Verfolgung **2** 55, **3** 52
Verhaltenskodizes **5** 25, 52 f.
Vermont **2** 52
Verrechnungspreise **3** 28, **4** 67
Verschlüsselung **2** 68, **5** 97 f.
Versicherung **2** 26, **5** 11 ff.
Verstoß **5** 25, 99, **6** 30, 44, **8** 21
Verträge **2** 86 f., **4** 42, 47, **5** 65, 74, 76, 117 f., 121, **6** 1 f., 13, 35 ff., **7** 1 ff., **8** 21
– force majeure (höhere Gewalt) **6** 46
– Rechtswahl **6** 45
– Streitbeilegung **6** 45
Vertraulichkeit **2** 53 ff.
– Vertraulichkeitsklauseln **6** 30
Verursachung **2** 28, **5** 21
Verzeichnisse über Verarbeitungstätigkeiten (VVZs), DS-GVO **4** 69
Vorratsdatenspeicherung **2** 83 f.
VR China **1** 26, **2** 22, **6** 4
– Aufgabenliste **3** 28
– Datenresidenz **2** 82
– Interim Measures for the Management of Generative Artificial Intelligence Services **2** 20 f.

Wartung **3** 5, **8** 3
Werbung **2** 46, 65, **4** 33, **5** 38, **6** 18, 35 ff.
Wettbewerbsrecht **6** 35 ff.
Wikimedia-Foundation, Scraping **2** 45
Wikipedia **2** 45

Zero hour-Bedrohungen **5** 123
Zugangskontrolle **7** 7
Zugangsrecht **5** 115
Zustimmung **4** 46 ff.
Zweckbindung **2** 76
Zynga, Privacyville **4** 61

© NOMOS Verlagsgesellschaft. Alle Rechte vorbehalten.