

*Band
5*

Lucas Jürss / Hans-Jörg Fischer (Hrsg.)

*Künstliche Intelligenz und Corporate
Governance – eine kritische Analyse der
Anforderungen für Unternehmen vor dem
Hintergrund der KI-Verordnung*

~
Lisa Marie Pinno

KCW Schriftenreihe



KCW KompetenzCentrum
für Wirtschaftsrecht
der FOM Hochschule für Oekonomie & Management

Lisa Marie Pinno

*Künstliche Intelligenz und Corporate Governance – eine kritische Analyse
der Anforderungen für Unternehmen vor dem Hintergrund der KI-Verordnung*

KCW Schriftenreihe der FOM, Band 5

Essen 2026

ISBN (Print) 978-3-89275-427-5 ISSN (Print) 2748-6869
ISBN (eBook) 978-3-89275-428-2 ISSN (eBook) 2748-6877

Dieses Werk wird herausgegeben vom KCW KompetenzCentrum für Wirtschaftsrecht
der FOM Hochschule für Oekonomie & Management gGmbH

Verlag:
MA Akademie Verlags- und Druck-Gesellschaft mbH, Leimkugelstraße 6, 45141 Essen
info@mav-verlag.de

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



Dieses Werk ist lizenziert unter CC BY 4.0:
Creative Commons Namensnennung 4.0 International.

Diese Lizenz erlaubt unter den Voraussetzungen der Lizenzbedingungen, u. A. der Namensnennung der Urheberin oder des Urhebers, der Angabe der CC-Lizenz (inkl. Link) und der ggf. vorgenommenen Änderungen die Bearbeitung, Vervielfältigung und Verbreitung des Materials in jedem Format oder Medium für beliebige Zwecke. Die Rechte und Pflichten in Zusammenhang mit der Lizenz ergeben sich ausschließlich aus dem Lizenzinhalt: CC BY 4.0 Deed | Namensnennung 4.0 International | Creative Commons | <https://creativecommons.org/licenses/by/4.0/legalcode.de>.

Die Bedingungen der Creative-Commons-Lizenz gelten nur für Originalmaterial. Die Wiederverwendung von Material aus anderen Quellen (gekennzeichnet mit Quellenangabe) wie z. B. von Schaubildern, Abbildungen, Fotos und Textauszügen erfordert ggf. weitere Nutzungsgenehmigungen durch den jeweiligen Rechteinhaber.

Lisa Marie Pinno

***Künstliche Intelligenz und Corporate Governance –
eine kritische Analyse der Anforderungen für
Unternehmen vor dem Hintergrund der KI-Verordnung***

Kontakt zur Autorin

Lisa Marie Pinno, LL.M.
lisa.pinno.lp@gmail.com

Vorwort

Die Schriftenreihe des KompetenzCentrums für Wirtschaftsrecht (KCW) an der FOM Hochschule für Oekonomie & Management bietet seit jeher ein Forum für herausragende wissenschaftliche Arbeiten, die sich aktuellen und praxisrelevanten Fragestellungen des Wirtschaftsrechts widmen. Mit der vorliegenden Masterthesis von Lisa Marie Pinno wird diese Reihe mit Band 5 um einen ebenso fundierten wie wegweisenden Beitrag erweitert.

Die Autorin analysiert kritisch die Anforderungen der „KI-Verordnung“ ((EU) 2024/1689) und deren praktische Auswirkungen auf die Corporate Governance von Unternehmen.

Sie stellt sich damit keinem leichten Unterfangen: Zwar sind die in der Fachliteratur erschienenen Beiträge zur rechtlichen Würdigung der Verordnung (inzwischen) zahlreich, jedoch mangelt es noch an konkreten Vorschlägen zur Implementierung der bisweilen sperrigen rechtlichen Vorgaben der Verordnung in Unternehmen.

Vor diesem Hintergrund überzeugt die Autorin, indem sie sich der Implementierungsdebatte um die KI-Verordnung nicht nur im Rahmen abstrakter Rechtsausführungen, sondern per Entwurf eines konkreten Umsetzungsleitfadens stellt. Die Arbeit wurde als Masterarbeit im Frühjahr 2025 vorgelegt und ist – dies gilt erst recht zum Zeitpunkt der Vorlage – in dieser Konkretheit in der Fachliteratur insgesamt herausragend.

Dass die Autorin sich bereiterklärt hat, ihre Arbeit zu veröffentlichen und in den wissenschaftlichen Diskurs einzuführen, ist ein akademischer Gewinn; dass auf diese Weise mehr Leserinnen und Leser Gelegenheit erhalten, die hervorragende Leistung der Autorin zur Kenntnis zu nehmen, ein schöner Nebeneffekt.

Düsseldorf & Mannheim im Februar 2026

Dr. Lucas Jürss

Lehrbeauftragter im Bereich Compliance
FOM Hochschule in Düsseldorf (bis 2025)
Rechtsanwalt und Fachanwalt für Strafrecht

Prof. Dr. Hans-Jörg Fischer

Professor für Wirtschafts- und Steuerrecht
FOM Hochschule in Mannheim
Wissenschaftlicher Leiter des KCW

Inhalt

Vorwort.....	IV
Abbildungsverzeichnis	VII
Abkürzungsverzeichnis	VIII
Über die Autorin	IX
1 Einleitung.....	1
1.1 Problemstellung, Zielsetzung und Forschungsfrage	1
1.2 Vorgehensweise	3
2 Rechtlicher Rahmen und theoretische Grundlagen.....	5
2.1 Wesentliche Rechtsgrundlagen.....	5
2.1.1 Historische Entwicklung	5
2.1.2 KI-Verordnung	7
2.1.3 Weitere relevante Gesetze	12
2.2 Künstliche Intelligenz	13
2.2.1 Definitionen	13
2.2.2 Konzepte und Technologien	17
2.3 Corporate Governance	21
2.3.1 Definitionen und Kernaspekte	22
2.3.2 Bedeutung für Unternehmen.....	23
2.4 Schnittstelle Corporate Governance und Künstliche Intelligenz	26
3 Umsetzungsleitfaden – Anforderungen KI-Verordnung	30
3.1 Vorabprüfung.....	30
3.2 Vorbereitende Maßnahmen	30
3.2.1 Identifizierung Rollen und Verantwortlichkeiten	31
3.2.2 Einbindung Betriebsrat	32
3.2.3 Identifizierung bestehender Governance-Strukturen und Prozessschritte.....	33
3.2.4 Einführung Meldewege und Überwachungsmaßnahmen.....	34

3.3	Umsetzungsmaßnahmen.....	38
3.3.1	Erstellung KI-Verzeichnis.....	38
3.3.2	Identifizierung Rollen und System-Verantwortliche.....	39
3.3.3	Einteilung Risikoklassen	43
3.3.4	Erstellung Pflichtenkatalog.....	60
3.3.5	Mapping: KI-Verzeichnis und Pflichtenkatalog.....	65
4	Kritische Analyse der Anforderungen	66
4.1	Chancen.....	66
4.1.1	Rechtssicherheit durch einheitliche Regulierung	66
4.1.2	Gewährleistung eines hohen Schutzniveaus	67
4.2	Risikobasierte Regulierung	67
4.2.1	Zunehmendes Vertrauen in KI-Technologien	68
4.2.2	Förderung der Innovation.....	69
4.2.3	Ausgestaltungsmöglichkeiten für Unternehmen.....	69
4.3	Herausforderungen.....	70
4.3.1	Risikobasierter Ansatz.....	70
4.3.2	Diskriminierung.....	71
4.3.3	Umsetzungsfristen.....	72
4.3.4	Ungenaue Beschreibungen	73
4.3.5	Kosten- und Ressourcenaufwand	75
5	Handlungsempfehlungen und Ausblick.....	76
6	Fazit	78
	Literatur	81

Abbildungsverzeichnis

Abbildung 1:	Corporate Governance als Schutzmechanismus	27
Abbildung 2:	Prüfungsschema Risikokategorien	44

Abkürzungsverzeichnis

AI	Artificial Intelligence
AI HLEG	High-Level Expert Group on Artificial Intelligence
AktG	Aktiengesetz
BetrVG	Betriebsverfassungsgesetz
BR	Betriebsrat
ChatGPT	Chatbot Generative Pre-trained Transformer
DCGK	Deutsche Corporate Governance Kodex
DORA	Digital Operational Resilience Act
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
Erwgr.	Erwägungsgrund
GFA	Grundrechts-Folgenabschätzung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GPAI-Modell	General Purpose AI-Modell
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V.
IDW PS	IDW-Prüfungsstandards
IEC	Internationalen Elektronische Kommission
IKS	Internes Kontrollsystem
ISO	International Organization for Standardization
KI	Künstliche Intelligenz
KI-VO	KI-Verordnung
KMU	Kleine und mittlere Unternehmen
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
ProdHaftRL	Produkthaftungsrichtlinie
TOMs	Technische und organisatorische Maßnahmen

Über die Autorin

Lisa Marie Pinno ist seit mehreren Jahren im Bereich Compliance tätig und arbeitet bei einem international agierenden Versicherungsunternehmen. In dieser Position verantwortet sie unter anderem die Identifikation, Bewertung und Überwachung von Compliance-Risiken in den Bereichen IT und KI. Dabei befasst sie sich insbesondere mit regulatorischen Anforderungen, internen Kontrollsystemen sowie der Weiterentwicklung entsprechender Compliance-Strukturen im Unternehmensumfeld.

1 Einleitung

Die fortschreitende Digitalisierung und damit einhergehend auch eine ihrer bedeutsamsten Entwicklungen – die „Künstliche Intelligenz“ (KI) – beschäftigt die Unternehmen in so einem erheblichen Maß wie kaum ein anderes gesellschaftliches Thema.¹

Die neuen Technologien führen zu einer Veränderung der Wirtschaft und Arbeitswelt. Während sie Unternehmen erhebliche Chancen bieten und völlig neue, innovative Möglichkeiten aufzeigen, wirft ihr Einsatz gleichzeitig weitreichende Fragen auf. Diese sind sowohl organisatorischer als auch rechtlicher und ethischer Natur. Insbesondere der Einsatz von KI erfordert eine einheitliche Rechtsgrundlage in der Europäischen Union (EU). Mit der am 12.07.2024 im Amtsblatt der EU veröffentlichten KI-Verordnung (KI-VO)² wird der voranschreitenden Entwicklung hinreichend Bedeutung zugemessen und das weltweit erste umfassende Regelwerk für KI geschaffen, welches eine Basis für die Regulierung bildet, aber auch das Vertrauen in die Technologie sowie Innovation stärkt.³

1.1 Problemstellung, Zielsetzung und Forschungsfrage

Mit der Verabschiedung der KI-VO sind die Unternehmen nun dazu angehalten, zu prüfen, ob sie der KI-VO unterliegen und welche Aspekte für sie im Umkehrschluss zu beachten sind.⁴

Bereits zum jetzigen Zeitpunkt werden die aus der KI-VO resultierenden Pflichten in der Literatur vereinzelt als schwer kontrollierbar beschrieben.⁵ Da die KI-VO das weltweit erste Regelwerk zur Regulierung von KI darstellt, kann davon aus-

¹ Vgl. *Bundesregierung*, AI Act verabschiedet, 2024, o.S.; *Kreutzer*, Künstliche Intelligenz verstehen, S. 499-501.

² Vgl. Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnung (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/ 858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. Nr. L 144 v. 12.7.2024.

³ Vgl. *Bundesregierung*, AI Act verabschiedet, 2024, o.S.; *Bülchmann*, Der KI-Act als komplexe Governance-Herausforderung, S. 408-409; *Müller-Peltzer/Schneider*, REL 2022, 9.

⁴ Vgl. *Bülchmann*, Der KI-Act als komplexe Governance-Herausforderung, S. 409.

⁵ Vgl. *Chibanguza/Steege*, NJW 2024, 1769; *Krönke*, NVwZ 2024, 529; *Seyffarth*, GWR 2024, 173.

gegangen werden, dass die praktische Umsetzung der Verordnung, insbesondere im Rahmen der Governance-Strukturen, einige Herausforderungen mit sich bringen wird.⁶

Vor welche Herausforderungen die KI-VO die Unternehmen stellt und welche Chancen sich ergeben, soll in dieser Arbeit genauer untersucht werden.

Ziel dieser Arbeit ist es auf Basis der bestehenden Literatur und der KI-VO herauszuarbeiten, welchen Anforderungen die Unternehmen zukünftig begegnen und welche Anpassungen der bisherigen Governance-Strukturen mit der Einführung der KI-VO notwendig sind.

Hierzu sollen zum einen die wesentlichen Regelungen der Verordnung aufgezeigt und zum anderen eine kritische Analyse ebendieser durchgeführt werden. Abschließend soll der Umfang und die Umsetzbarkeit der Anforderungen bewertet werden können. Im Rahmen dessen werden die folgenden Forschungsfragen beantwortet:

- Welche Anforderungen ergeben sich für Unternehmen vor dem Hintergrund der KI-Verordnung und wie sind diese zu bewerten?
- Erfordern die Entwicklungen der Künstlichen Intelligenz eine eigene Governance oder können die Anforderungen in die bereits bestehenden Strukturen integriert werden?

Im Gesamtergebnis soll die Arbeit die Auswirkungen der KI-VO auf die Governance-Strukturen darstellen und Auslegungshinweise der Verordnung aufzeigen. Die Arbeit kann sodann eine ergänzende Entscheidungsgrundlage und Handlungsempfehlung für Unternehmen bieten, um den Anforderungen der KI-VO gerecht zu werden.

Diese Arbeit kann von allen Unternehmen zu Orientierungszwecken gleichermaßen genutzt werden. Berücksichtigt werden sollte, dass vereinzelt branchenspezifische Bezüge hergestellt werden. Aufgrund des Umfangs der Verordnung erhebt die Arbeit keinen Anspruch auf Vollständigkeit und entfaltet daher ausschließlich unterstützende Wirkung.

Es sei darauf hingewiesen, dass im Rahmen der Arbeit Rechtsprechung, Literatur und Gesetzesänderung bis Mitte Dezember 2024 berücksichtigt wurden.

⁶ Vgl. *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 267; *Steinrötter/Markert*, RD 2024, 400.

1.2 Vorgehensweise

Die Arbeit setzt sich aus insgesamt sechs Teilen zusammen, wobei die angewandte Methodik überwiegend theoretisch ist.

Im Anschluss an die Einleitung werden in Teil B der Rechtsrahmen und die theoretischen Grundlagen dargelegt. Die Darstellung des Rechtsrahmens bezieht die historischen Entwicklungen bis hin zur KI-VO ein. Verstärkt thematisiert werden sodann die mit der KI-VO verfolgten Ziele (Erwgr. 1 KI-VO) eines einheitlichen Rechtsrahmens, der Förderung des Binnenmarktes, die Einführung menschenzentrierter und zukunftsorientierter KI und die Schaffung eines Schutzniveaus für die Gesundheit, die Sicherheit und die Grundrechte.⁷ Sowohl die mit der KI-VO einhergehenden Umsetzungsfristen als auch der Strafrahmen der Verordnung werden in diesem Unterkapitel dargelegt. Seinen Abschluss findet das Kapitel mit der Ausführung weiterer einschlägiger Gesetze.

Darauffolgend werden die theoretischen Grundlagen detailliert dargestellt. Hierzu wird zunächst der Begriff der KI erläutert sowie die Konzepte und Technologien der KI (Maschinelles Lernen, Deep Learning und Neuronale Netze) aufgezeigt. Im weiteren Verlauf wird der Begriff der Corporate Governance erläutert und die Rolle im Unternehmen herausgearbeitet. Dabei wird insbesondere auf die Gewährleistung der Regelkonformität sowohl im Hinblick auf gesetzliche als auch interne Pflichten Bezug genommen. Den Abschluss findet Teil B mit der Veranschaulichung der Schnittstelle zwischen Corporate Governance und KI.

Teil C bildet den inhaltlichen Kern der Arbeit und beschäftigt sich mit den aus der KI-VO resultierenden Anforderungen für Unternehmen. Hierzu werden zunächst die vorbereitenden Maßnahmen und damit einhergehend der Anpassungsbedarf der bisher bestehenden Governance-Strukturen analysiert. In diesem Zusammenhang werden erstmalig Einblicke dahingehend gegeben, ob die Entwicklungen im Bereich der KI eine neue Governance-Struktur erfordern oder ob die Anforderungen in die bereits bestehenden Strukturen integriert werden können. Hierbei werden unter anderem Aspekte wie die Definition von Rollen und Verantwortlichkeiten innerhalb des Unternehmens, die Einbindung wichtiger Stakeholder, das Richtlinienmanagement, die Implementierung regulatorischer Überwachungsmaßnahmen sowie der Schulungsbedarf beleuchtet. An die vorbereitenden Maßnahmen schließen die Umsetzungsmaßnahmen an. Neben der Begriffsdifferenzierung zwischen den verschiedenen Akteuren (Art. 3 KI-VO) verfolgt die Verordnung einen risikobasierten Ansatz (Erwgr. 26 KI-VO) was in unterschiedlich hohen Anforderungen resultiert.⁸ Die Strukturierung des Kapitels wird sich

⁷ Vgl. von Welser, GRUP-Prax 2024, 485.

⁸ Vgl. von Welser, GRUP-Prax 2024, 485.

daher an der Struktur der KI-VO und somit an Aspekten wie: Inventarisierung, Klassifizierung sowie der Zuordnung von Rollen und Verantwortlichkeiten orientieren.

Die Ausführungen der EU geben bisher nur begrenzt Hinweise darauf, wie die aus der KI-VO resultierenden Anforderungen im Detail zu bewerten sind. Vor diesem Hintergrund erfolgt im Anschluss an die Darstellung der Anforderungen in Teil D eine kritische Analyse. Anhand dieser Analyse soll bewertet werden, inwieweit die Vorgaben der Verordnung als Herausforderung oder Chance für Unternehmen zu klassifizieren sind. Unter Berücksichtigung der vorherigen Kapitel bietet dieser Abschnitt die Grundlage für den Teil E, in dem die Handlungsempfehlungen für Unternehmen und ein Ausblick auf die prognostizierten Entwicklungen dargelegt werden.

Am Ende der Arbeit werden in einem Fazit die zu Beginn aufgeworfenen Forschungsfragen abschließend diskutiert und beantwortet.

2 Rechtlicher Rahmen und theoretische Grundlagen

Den weiteren Ausführungen vorgelagert werden in dem zweiten Kapitel zunächst der Rechtsrahmen und die theoretischen Grundlagen ausgeführt. Dieses Kapitel soll als Grundlage für die darauffolgende Analyse der KI-VO dienen.

2.1 Wesentliche Rechtsgrundlagen

Die Digitalisierung und damit einhergehend einer ihrer wesentlichen Treiber, die KI-Technologien, entwickeln sich bereits seit einigen Jahren stetig weiter. Diese technologischen Fortschritte gehen mit Veränderungen auf gesetzgeberischer Ebene einher, da die Regulatorik stets an die gesellschaftlichen Entwicklungen angepasst werden muss.⁹

2.1.1 Historische Entwicklung

Während KI zunächst als allgemeiner Teil der technologischen Entwicklung betrachtet wurde und als einschlägig nur die bereits bekannten Gesetze – wie die Datenschutz-Grundverordnung“ (DSGVO)¹⁰, das Allgemeine Gleichbehandlungsgesetz, die Produkthaftungsrichtlinie (ProdHaftRL)¹¹ sowie das Wettbewerbsrecht – galten, wuchs die Diskussion über einen einheitlichen Rechtsrahmen zunehmend. Bereits seit einigen Jahren befassen sich die Organe der EU mit der Förderung und Regulierung von KI.¹²

Im Jahr 2017 fand das „Digitale Gipfeltreffen“ statt und bot ein Diskussionsforum zur Förderung der Digitalisierung und Innovation in Europa. Um das Bewusstsein für eine intensivere Auseinandersetzung mit der Digitalisierung und damit einhergehend auch der KI zu schaffen, berief die EU-Kommission eine Expertengruppe – die sogenannte High-Level Expert Group on Artificial Intelligence (AI HLEG) –

⁹ Vgl. *Europäisches Parlament*, Was ist künstliche Intelligenz und wie wird sie genutzt? 2020, o.S.

¹⁰ Vgl. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 v. 4.5.2016.

¹¹ Vgl. Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates, ABl. Nr. L 22 v. 18.11.2024.

¹² Vgl. *Horstmann*, ZD-Aktuell 2024, 01580.

zusammen. Diese Expertengruppe sollte sich hinsichtlich einer sicheren und vertrauenswürdigen KI beraten.¹³

Im Jahr 2018 schlug die Kommission eine KI-Strategie für die EU vor und schloss hieran mit der Entwicklung von ethischen Leitlinien zur Verwirklichung einer vertrauenswürdigen KI im Jahr 2019 an. Neben dem Bestreben der EU, eine Vorreiterrolle im Bereich der KI einzunehmen, sah sie gleichermaßen das Erfordernis, die Grundrechte und ethischen Regeln zu schützen.¹⁴

Aus den Leitlinien gingen schließlich sieben Kernanforderungen für eine vertrauenswürdige KI hervor: Vorrang menschlichen Handelns und menschlicher Aufsicht, technische Robustheit und Sicherheit, Privatsphäre und Datenqualitätsmanagement, Transparenz, Vielfalt, Nichtdiskriminierung und Fairness, Gesellschaftliches und ökologisches Wohlergehen sowie Rechenschaftspflicht.¹⁵

Mit diesen Leitlinien schaffte der europäische Gesetzgeber eine wesentliche Grundlage für die weiteren rechtlichen Entwicklungen im Bereich der KI.

Im Februar 2020 veröffentlichte die EU das sogenannte KI-Weißbuch – ein strategisches Dokument, das klare Richtlinien zum europäischen Umgang mit KI beinhaltet sowie den Vorschlag eines einheitlichen Rechtsrahmen unterbreitet. Dieser Rahmen wurde neben den Ethik-Leitlinien der AI HLEG für die Zielverwirklichung der Innovationsförderung und der Gefahrenregulierung als essenziell angesehen.¹⁶ Es hieß, dass der Regulierungsrahmen „optimale Ergebnisse für Gesellschaft, Umwelt und Wirtschaft und die Vereinbarkeit mit den Rechtsvorschriften, Grundsätzen und Werten der EU gewährleisten [muss]“.¹⁷

Bereits zu diesem Zeitpunkt war sich die Kommission einig, dass ein risikobasierter Ansatz verfolgt werden sollte, der sowohl die rasanten Entwicklungen im Bereich der KI berücksichtigt als auch Flexibilität für alle weiteren Entwicklungen bietet.¹⁸

Die sich hieran anschließenden Diskussionen mündeten schließlich im April 2021 in einem von der Europäischen Kommission entwickelten Erstentwurf der KI-VO.¹⁹

¹³ Vgl. *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 155.

¹⁴ Vgl. *Horstmann*, ZD-Aktuell 2024, 01580; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 155.

¹⁵ Vgl. Weißbuch Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen v. 19.2.2020, COM (2020) 65 final, S. 11; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 156.

¹⁶ Vgl. *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 156 f.

¹⁷ Weißbuch (2020), S. 11.

¹⁸ Vgl. Weißbuch (2020), S. 11 f.

¹⁹ Vgl. *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 157.

2.1.2 KI-Verordnung

Aufgrund der grenzüberschreitenden Nutzung von KI und der Gefahr einer Aufspaltung des EU-Binnenmarktes durch unterschiedliche nationale Gesetzgebung entschied sich die Europäische Kommission bereits in ihrem ersten Entwurf für einen verbindlichen Rechtsakt in Form einer Verordnung.²⁰

Gemäß Art. 288 Abs. 2 AEUV besitzt eine Verordnung allgemeine Geltung – sie ist somit in all ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat. Anders als Richtlinien bedarf sie keiner Umsetzung in nationales Recht, wodurch für KI-Anbieter sowie -Betreiber die Herausforderung entfällt, sich mit einer Vielzahl an nationalen Rechtsanforderungen auseinandersetzen zu müssen.²¹

Der Verordnungsvorschlag der Kommission eröffnete das Gesetzgebungsverfahren. Die rasanten technologischen Fortschritte stellten die europäische Regulierung vor die Herausforderung ein Gleichgewicht zwischen Regulierung und Innovationsförderung zu schaffen. Bedeutung erlangt dies insbesondere im Zusammenhang mit der Kennzeichnung von KI und den einschlägigen Transparenzfragen. Als Reaktion auf diese Entwicklungen und zur Schaffung von Rechtssicherheit nahmen die EU-Institutionen im Jahr 2023 die Trilogverhandlungen auf. Mit dem Entwurf der KI-VO wurde das Ziel verfolgt, rechtliche Rahmenbedingungen zu schaffen und daraus resultierende Risiken zu minimieren.²²

Eine Einigung erzielten die Mitgliedsländer der EU schließlich Anfang 2024. Im März 2024 erfolgte die Zustimmung des Europäischen Parlaments und der Rat verabschiedete die Verordnung im Anschluss im Mai 2024.²³

2.1.2.1 Hintergrund und Zielsetzung

Die am 12.07.2024 im Amtsblatt der EU verabschiedete KI-VO trat 20 Tage später in Kraft (Art. 113 KI-VO) und schuf schließlich die Basis einer einheitlichen

²⁰ Vgl. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, v. 21.4.2021, COM (2021) 206 final, S. 7.

²¹ Vgl. *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 156 f.; *Wybitul*, BB 2024, 2179.

²² Vgl. *Chibanguza/Steege*, NJW 2024, 1769; *Kreutzer*, Künstliche Intelligenz verstehen, S. 504; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 158.

²³ Vgl. *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 157.

Rechtsgrundlage. Gleichzeitig verdeutlichte die Verordnung den Handlungsbedarf für Unternehmen.²⁴

Die KI-VO verfolgt das Ziel KI-Anbietern, -Einführern, -Händlern und -Nutzern eine einheitliche Rechtsgrundlage in Bezug auf KI zu bieten und hierdurch sowohl den wirtschaftlichen als auch sozialen Fortschritt zu fördern. Auch soll mit der Einführung der Verordnung das Vertrauen in die neuen Technologien gestärkt und die Grundrechte der Menschen geschützt werden.²⁵ In Erwgr. 1 KI-VO werden die zentralen Zwecke der KI-VO aufgeführt.

Die Verordnung folgt einem risikobasierten Ansatz, bei dem die Intensität der Regelungen sich nach dem Risiko für die betroffenen Schutzgüter definiert. Sie umfasst insgesamt 13 Kapitel sowie die Anhänge I bis XIII. Zur weiterführenden Erläuterung sind der KI-VO zudem 180 Erwgr. vorangestellt.²⁶

2.1.2.2 Anwendungsbereich

Der Anwendungsbereich der KI-VO gliedert sich in einen sachlichen, persönlichen und räumlichen Bereich.

2.1.2.2.1 Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich setzt das Vorliegen eines KI-Systems voraus. Diese Voraussetzung, die auf den ersten Blick naheliegend erscheint, stellte den Gesetzgeber während des Gesetzgebungsverfahrens jedoch vor einige Herausforderungen, da bis zu diesem Zeitpunkt keine einheitlich akzeptierte Definition von KI existierte. Es war somit unabdingbar, mit der Einführung der Verordnung und zur Eröffnung des sachlichen Anwendungsbereichs eine KI-Definition festzulegen. In Erwgr. 4 und Art. 3 Nr. 1 KI-VO findet sich die KI-Definition. Im weiteren Verlauf der Arbeit wird auf diese Definition detaillierter eingegangen.²⁷

²⁴ Vgl. *Bundesregierung*, AI Act verabschiedet, 2024, o.S.; *Bülchmann*, Der KI-Act als komplexe Governance-Herausforderung, S. 408-409; *Müller-Peltzer/Schneider*, REL 2022, 9; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 158.

²⁵ Vgl. *Bundesregierung*, Zukunftsthema KI, o.S.; *Vertretung in Deutschland*, KI-Gesetz tritt in Kraft, 2024, o.S.

²⁶ Vgl. Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 1 ff.; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 159 f.

²⁷ Vgl. *Martini/Wendehorst/Wendehorst*, Art. 3 Rn. 3; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 162.

2.1.2.2.2 Persönlicher Anwendungsbereich

Art. 2 Abs. 1 KI-VO regelt, welche Akteure Adressat der Verordnung sind und definiert somit den persönlichen Anwendungsbereich. Während die Verordnung einige Personengruppen aufzählt, ist zu beachten, dass die Aufzählung nicht als abschließend anzusehen ist. Auch für Behörden und Einrichtungen der EU sowie der Mitgliedstaaten lassen sich Rechte und Pflichten aus der Verordnung ableiten. Namentlich benannt werden in Art. 2 Abs. 1 lit. a-g KI-VO als Adressaten in der Verordnung: Anbieter, Betreiber, Einführer und Händler, Produkthersteller, Bevollmächtigte von Anbietern und betroffene Personen in der Union.

Der Begriff „betroffene Personen“, der an mehreren Stellen der Verordnung verwendet wird, findet sich in der Begriffsbestimmung in Art. 3 KI-VO nicht wieder. Der Begriff erweist sich insbesondere für Art. 86 KI-VO als relevant, der das „Recht auf Erläuterung der Entscheidungsfindung im Einzelfall“²⁸ regelt. Aufgrund der Schwerpunktsetzung wird sowohl auf die Begriffsbestimmung als auch die Erläuterung des Art. 86 KI-VO verzichtet.²⁹

In der Gesamtschau der Verordnung fällt auf, dass die Aufzählung der Akteure in Art. 2 Abs. 1 KI-VO nicht zwingend erforderlich ist, da sich der persönliche Anwendungsbereich aus dem jeweiligen Normenadressat der Einzelschriften ergibt.

2.1.2.2.3 Räumlicher Anwendungsbereich

Von zentralerer Bedeutung ist Art. 2 Abs. 1 KI-VO für den räumlichen Anwendungsbereich.

Als maßgeblich gilt für den Anwendungsbereich nicht der Sitz der jeweiligen Person, sondern vielmehr die Tatsache, dass das KI-System auf dem EU-Markt in den Verkehr gebracht oder dort genutzt wird. Mindestens wird jedoch vorausgesetzt, dass das Ergebnis des KI-Systems innerhalb der EU Verwendung findet (Ergebnisprinzip).³⁰ Hieraus resultiert, dass auch KI-Systeme aus Drittstaaten unter die Verordnung fallen und damit einer Umgehung der Vorschriften entgegen gewirkt werden kann.

²⁸ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 110.

²⁹ Vgl. Martini/Wendehorst/Wendehorst, Art. 2 Rn. 30.

³⁰ Vgl. Martini/Wendehorst/Wendehorst, Art. 2 Rn. 4; Wybitul, BB 2024, 2179.

Der Gesetzgeber bestimmt in der Verordnung bewusst einen weiten Anwendungsbereich und hat diesen in Erwgr. 21 und 22 KI-VO konkretisiert.³¹ Die Verordnung verfolgt das Ziel „gleiche Wettbewerbsbedingungen und einen wirksamen Schutz der Rechte und Freiheiten von Einzelpersonen ... zu gewährleisten“.³² Da gemäß Erwgr. 21 KI-VO nicht der Sitz des Anbieters entscheidend ist, sondern der Ort, an dem das Ergebnis des KI-Systems verwendet wird, gilt für Anbieter nicht das Territorialitätsprinzip, sondern das Marktortprinzip. Betreiber hingegen unterliegen dem Territorialitätsprinzip, sofern sie ihren Sitz in der EU haben.³³

2.1.2.3 Umsetzungsfristen

Der Gesetzgeber regelt die Umsetzungsfristen der Verordnung in Art. 113 KI-VO, welcher in einem engen Zusammenhang mit der Übergangsvorschrift Art. 111 KI-VO steht.³⁴

Gemäß Art. 113 KI-VO ist das Inkrafttreten der Verordnung auf den 20. Tag nach der Veröffentlichung im Amtsblatt der EU festgelegt und somit auf den 01.08.2024 datiert. Aufgrund der Vielzahl an unterschiedlichen Anforderungen unterliegt der Geltungsbeginn einer gestaffelten Regelung. Hieraus resultiert, dass die Kapitel I und II ab dem 02.02.2025 in Kraft treten (Art. 113 lit. a KI-VO). Hiervon umfasst sind insbesondere die Vorschriften zu verbotenen Praktiken mit dem Ziel, das Systeme mit einem inakzeptablen Risiko möglichst zeitnah aus dem Verkehr genommen werden.³⁵ Des Weiteren gilt diese Frist für die in Kapitel I aufgeführte KI-Kompetenz gemäß Art. 4 KI-VO.

Für Kapitel III Abschnitt 4, Kapitel V, Kapitel VII, Kapitel XII und Artikel 78 KI-VO wurde mit dem 02.08.2025 und somit zwölf Monate nach Inkrafttreten ebenfalls ein früher Geltungsbeginn vorgesehen (Art. 113 lit. b KI-VO). Von dieser Frist betroffen sind unter anderem die KI-Modelle mit allgemeinem Verwendungszweck (General Purpose AI (GPAI)-Modelle). Als spätester Geltungsbeginn wird für Art. 6 Abs. 1 KI-VO, bei welchem es sich um die Einstufungsvorschrift für Hochrisiko-KI-Systeme handelt, der 02.08.2027 vorgesehen. Alle übrigen und

³¹ Vgl. *Bitkom*, Umsetzungsleitfaden zur KI-Verordnung, 2024, S. 52 f.; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 164.

³² Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 6; vgl. Martini/Wendehorst/*Wendehorst*, Art. 2 Rn. 12.

³³ Vgl. Martini/Wendehorst/*Wendehorst*, Art. 2 Rn. 20.

³⁴ Vgl. Martini/Wendehorst/*Wendehorst*, Art. 113 Rn. 1.

³⁵ Vgl. Martini/Wendehorst/*Wendehorst*, Art. 5 Rn. 11.

nicht explizit aufgeführten Vorschriften der KI-VO gelten gemäß Art. 113 lit. c KI-VO ab dem 02.08.2026.³⁶

Art. 111 KI-VO setzt die Fristen für bereits in den Verkehr gebrachte oder in den Betrieb genommene KI-Systeme sowie GPAI-Modelle fest. Der Artikel führt in dem Zusammenhang in Absatz 1 aus, dass insofern es sich um KI-Systeme mit einer Komponente von IT-Großsystemen handelt und diese vor dem 02.08.2027 in den Verkehr oder Betrieb gebracht worden sind, die Systeme bis Ende 2030 mit der KI-VO in Einklang gebracht werden müssen. Alle Hochrisiko-KI-Systeme, die vor dem 02.06.2026 in den Verkehr gebracht oder in Betrieb genommen worden sind, fallen gemäß Art. 111 Abs. 2 KI-VO grundsätzlich nicht in den Anwendungsbereich der Verordnung. Die Anforderungen aus den Art. 8 ff. KI-VO gelten für ebendiese Systeme nur dann, wenn das System nach dem Inverkehrbringen oder der Inbetriebnahme wesentlich verändert wurde.³⁷

Eine Sonderregelung ergibt sich aus Art. 111 Abs. 2 KI-VO und gilt für KI-Systeme, die für Behörden bestimmt sind, da diese höheren Pflichten unterliegen. Hieraus ergibt sich, dass Behörden auch für bereits in den Verkehr gebrachte oder in Betrieb genommene KI-Systeme, die aus der KI-VO hervorgehenden Pflichten bis zum 02.08.2030 erfüllt haben müssen.³⁸

2.1.2.4 Strafraumen

Mit Art. 99 KI-VO eröffnet der Gesetzgeber das Kapitel über Sanktionen. Dem nachgelagert folgt in Art. 100 KI-VO die Sanktionierung in Form von Geldbußen für Organe, Einrichtungen und sonstige Stellen der Union, während Art. 101 KI-VO die Geldbußen für Anbieter von GPAI-Modellen festlegt.³⁹

Hinsichtlich der monetären Ahndung setzt die Verordnung fest, dass gemäß Art. 99 Abs. 2 KI-VO bei einer Missachtung der in Art. 5 KI-VO genannten verbotenen KI-Praktiken eine Geldbuße von bis zu 35.000.000 Euro oder im Falle von Unternehmen bis zu sieben Prozent des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden kann. Für Verstöße gegen andere Verpflichtungen werden nach Art. 99 Abs. 4 KI-VO Geldbußen von bis zu 15.000.000 Euro oder bei Unternehmen bis zu drei Prozent des Jahresumsatzes verhängt. Im Falle von falschen, unvollständigen oder irreführenden

³⁶ Vgl. *Ammann/Pohle*, CB 2024, 137, 144; *Bierekoven*, ITRB 2024, 264, 265; *Herbst/Panic*, KI-Recht praktisch erklärt, S. 14; *Martini/Wendehorst/Wendehorst*, Art. 113 Rn. 2-13.

³⁷ Vgl. *Binder/Egli*, MMR 2024, 626, 627.

³⁸ Vgl. *Martini/Wendehorst/Wendehorst*, Art. 111 Rn. 7.

³⁹ Vgl. *Martini/Wendehorst/Nemitz*, Art. 99 Rn. 7 f.

Informationen gegenüber notifizierender Stellen oder der nationalen Behörden werden bis zu 7.500.000 Euro oder bis zu einem Prozent des Jahresumsatzes als Strafe auferlegt.

Entscheidend ist bei der Festlegung der Strafe stets, welcher der beiden Beträge höher ist. Eine Ausnahme hiervon bilden gemäß Art. 99 Abs. 6 KI-VO die kleinen und mittleren Unternehmen (KMU). Für sie soll bei der Sanktionierung stets der jeweils niedrigere Betrag gelten und auf diesem Wege die wirtschaftliche Lage der Unternehmen berücksichtigt werden.⁴⁰ Für KMU führt die Verordnung keine eigene Definition. Sie orientiert sich an der Empfehlung der EU-Kommission⁴¹, welche als KMU solche Unternehmen einstuft, die weniger als 250 Mitarbeitende beschäftigen und höchstens einen Jahresumsatz von 50 Millionen Euro oder eine Jahresbilanzsumme von 43 Millionen Euro aufweisen.⁴²

In einer separaten Richtlinie soll zukünftig die Haftung für durch KI verursachte Schäden geregelt werden. Zudem wurde die bisherige Fassung der ProdHaftRL überarbeitet. Die neue EU-Produkthaftungsrichtlinie 2024/2853 wurde am 18.11.2024 im Amtsblatt der EU veröffentlicht und trat schließlich am 09.12.2024 in Kraft. In der Richtlinie wird ausgeführt, dass die bisherige Fassung sich zwar als wichtiges Instrument erwiesen hat, die Aktualisierung jedoch insbesondere aufgrund der Entwicklung der KI-Technologien notwendig war. Erwgr. 3 KI-VO konkretisiert weiter, dass Kläger unabhängig von neuen Technologien auch weiterhin von demselben Schutzniveau profitieren sollen und für alle Unternehmen mehr Rechtssicherheit und gleiche Wettbewerbsbedingungen herrschen.

2.1.3 Weitere relevante Gesetze

Im Rahmen der Arbeit werden wiederholt Schnittstellen zu anderen Gesetzen identifiziert, wodurch Adressaten der KI-VO neben den Pflichten aus der Verordnung auch weitere einschlägige Gesetze beachten und in die Implementierung

⁴⁰ Vgl. *Vertretung in Deutschland*, KI-Gesetz tritt in Kraft, 2024, o.S.; Martini/Wendehorst/Nemitz, Art. 99 Rn. 24 ff.

⁴¹ Vgl. Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinunternehmen sowie der kleinen und mittleren Unternehmen, ABl. Nr. L 124 v. 20.5.2004, S. 39.

⁴² Siehe weiterführend Erwgr. 143 KI-VO.

einbeziehen müssen. Als Beispiele lassen sich in dem Zusammenhang das Bundesdatenschutzgesetz, die ProdHaftRL, die NIS-2-RL⁴³, der Data Act⁴⁴ sowie Data Governance Act⁴⁵ und die DSGVO anführen.⁴⁶

Die Tatsache, dass die KI-VO neben die weiteren Rechtspflichten tritt und diese nicht ersetzt, wird insbesondere aus Art. 2 Abs. 9 sowie Art. 26 Abs. 3 KI-VO deutlich. Diese Regelungen führen an, dass Vorschriften zum Verbraucherschutz und zur Produktsicherheit weiterhin uneingeschränkt Anwendung finden. Zudem wird in Art. 26 Abs. 3 KI-VO explizit ausgeführt, dass die in Art. 26 Abs. 1 und 2 KI-VO genannten Pflichten für Betreiber alle sonstigen Pflichten nach dem Unionsrecht unberührt lassen.⁴⁷

2.2 Künstliche Intelligenz

Um ein fundiertes und einheitliches Verständnis zu schaffen, ist es erforderlich, zunächst die wesentlichen Definitionen im Bereich der KI darzustellen. Diese Definitionen schaffen den Rahmen zur besseren Einordnung und dienen als Grundlage für die weiteren Ausführungen in dieser Arbeit.

2.2.1 Definitionen

Neben der Begriffsbestimmung von KI im Allgemeinen, soll auch für die im Rahmen der KI-VO genannten Begriffe des KI-Systems und des KI-Modells ein einheitliches Verständnis geschaffen werden.

⁴³ Vgl. Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910, 2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. Nr. L 333 v. 27.12.2022.

⁴⁴ Vgl. Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung), ABl. Nr. L 71 v. 22.12.2023.

⁴⁵ Vgl. Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl. Nr. L 152 v. 3.6.2022.

⁴⁶ Vgl. *Becker et al.*, Zukunft der Unternehmensdaten, 2024, S. 9; *Chibanguza/Steege*, NJW 2024, 1769, 1777; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 80; *Voigt/Hüllen*, HdB-KI-Verordnung, S. 5.

⁴⁷ Vgl. *IBM*, Was ist KI-Governance? o.S.; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 118 ff.; *Wybitul*, BB 2024, 2179, 2182.

2.2.1.1 KI

Der Gesetzgeber greift in einer Vielzahl von Gesetzen, wie etwa dem Betriebsverfassungsgesetz (BetrVG), bereits häufig auf den Begriff der KI zurück.⁴⁸ Bisher fehlte jedoch eine einheitliche Definition in der wissenschaftlichen Literatur.⁴⁹

Unter dem Begriff der KI (engl. Artificial Intelligence (AI)) werden zumeist verschiedene Technologien verstanden, welche auf die Lösung komplexer Aufgaben abzielen. In der Vergangenheit unternommene Versuche einer Begriffsbestimmung mündeten in einer unpräzisen Formulierung, sodass ein einheitliches Verständnis von KI bisher ausblieb.⁵⁰

Mit der Einführung der KI-VO definiert der Gesetzgeber den Begriff der KI in Erwgr. 4 KI-VO schließlich als „eine Reihe von Technologien, die sich rasant entwickeln und zu vielfältigem Nutzen für Wirtschaft, Umwelt und Gesellschaft über das gesamte Spektrum industrieller und gesellschaftlicher Tätigkeiten hinweg beitragen“.⁵¹

2.2.1.2 KI-System

Die Definition eines KI-Systems war während des Gesetzgebungsverfahrens ein zentrales und hoch umstrittenes Thema und stellte eine der wesentlichen Debatten dar.⁵² Art. 3 KI-VO führt die für die Verordnung maßgeblichen Begriffsbestimmungen aus und definiert in Art. 3 Nr. 1 KI-VO das KI-System schließlich 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“.*⁵³

Der Gesetzgeber entschied sich somit im Ergebnis für eine Definition, die an die der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

⁴⁸ Vgl. Witteler/Moll, NZA 2023, 327.

⁴⁹ Vgl. Kreutzer, Künstliche Intelligenz verstehen, S. 500.

⁵⁰ Vgl. Becker et al., Zukunft der Unternehmensdaten, 2024, S. 4; Kreutzer, Künstliche Intelligenz verstehen, S. 500.

⁵¹ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 2.

⁵² Vgl. Ammann/Pohle, CB 2024, 137; Martini/Wendehorst/Wendehorst, Art. 3 Rn. 1, 14 ff.

⁵³ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 46; vgl. Witteler/Moll, NZA 2023, 327.

angelehnt ist, jedoch einen gewissen Auslegungsspielraum aufweist.⁵⁴ Auch wenn es zunächst scheint, als könnte eine weite Auslegung im Rahmen eines neuen Regulierungsregimes negative Stimmen nach sich ziehen, bietet die weitgefasste Definition jedoch auch die Chance, dass KI-Technologien leichter angewendet werden können.⁵⁵

Ein wesentliches Merkmal von KI ist die „Operation mit [einem] unterschiedlichen Grad an Autonomie“.⁵⁶ KI-Systeme sollen bis zu einem gewissen Grad in der Lage sein, unabhängig von menschlichem Zutun zu agieren. In Erwgr. 12 KI-VO führt der Gesetzgeber die Definition eines KI-Systems weiter aus. Hervorgehoben wird insbesondere, dass KI-Systeme sich von einfacheren, herkömmlichen Softwaresystemen und Programmierungsansätzen unterscheiden. Es werden von der Definition keine regelbasierten Systeme eingeschlossen, die ausschließlich auf definierten Regeln von Menschen basieren und automatisch Operationen ausführen. In Art. 6 Abs. 1 KI-VO trifft der Gesetzgeber eine Unterscheidung zwischen KI-Systemen als Produkt und als Sicherheitsbauteil eines anderen Produkts. Er macht so deutlich, dass die meisten Hardware-Komponenten nicht von dem Begriff des KI-System umfasst sind.⁵⁷ Die Definition lässt sich zudem auf Basis der in Art. 2 KI-VO genannten Ausschlussstatbestände weiter konkretisieren.

Der Gesetzgeber verfolgt mit den Ausführungen in der KI-VO das Ziel, eine klare Definition des Begriffs „KI-System“ zu etablieren. Hierzu wird eine enge Abstimmung mit internationalen Organisationen angestrebt, um Rechtssicherheit, internationale Konvergenz und Akzeptanz sicherzustellen. Gleichzeitig soll die Definition auch Raum für Flexibilität bieten, damit Dynamiken im Bereich der KI hinreichend berücksichtigt werden können.⁵⁸

2.2.1.3 GPAI-Begriff

Im Rahmen der KI-VO wird zwischen GPAI-Modellen und GPAI-Systemen unterschieden. Bei beiden Kategorien handelt sich um Systeme bzw. Modelle mit einem allgemeinen Verwendungszweck.⁵⁹

⁵⁴ Vgl. *Bronner*, KIR 2024, 55, 57; *Heinze et al.*, KIR 2024, 11, 14.

⁵⁵ Vgl. *Martini/Wendehorst/Wendehorst*, Art. 3 Rn. 5.

⁵⁶ *Martini/Wendehorst/Wendehorst*, Art. 3 Rn. 29.

⁵⁷ Vgl. *Martini/Wendehorst/Wendehorst*, Art. 3 Rn. 23.

⁵⁸ Siehe weiterführend Erwgr. 12 KI-VO.

⁵⁹ Vgl. *Bronner*, KIR 2024, 55, 60.

Art. 3 Nr. 63 KI-VO definiert ein GPAI-Modell als ein KI-Modell, welches „erhebliche allgemeine Verwendbarkeit aufweist“.⁶⁰ Es ist in der Lage – unabhängig von der Art des Inverkehrbringens – viele verschiedene Aufgaben zu erfüllen. Zudem kann das Modell in nachgelagerte Systeme oder Anwendungen integriert werden. Die GPAI-Modelle unterliegen in einigen Vorschriften Sonderregelungen, wie z.B. in Kapitel V und in einigen Abschnitten von Kapitel IX.⁶¹

Auf dem Begriff der GPAI-Modelle bauen die GPAI-Systeme auf, sodass sich die Definition der GPAI-Systeme entsprechend ableitet. Gemäß Art. 3 Nr. 66 KI-VO ist ein GPAI-System „ein KI-System, das auf einem KI-Modell mit allgemeinem Verwendungszweck beruht und in der Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen“.⁶² Insgesamt weist der Begriff jedoch eine geringe Relevanz in der Verordnung auf, da die überwiegenden Vorschriften bereits an den Begriff des GPAI-Modells anknüpfen.⁶³

2.2.1.4 KI-Modell

Der Begriff des KI-Modells wird in der KI-VO nicht explizit definiert, jedoch insbesondere in Art. 3 Nr. 63 KI-VO im Kontext von GPAI-Modellen vorausgesetzt. Die beiden Begriffe „KI-Modell“ und „KI-System“ werden an verschiedenen Stellen der Verordnung voneinander abgegrenzt, wobei ein KI-Modell kein KI-System sein kann. Mit Ausnahme der GPAI-Modelle fallen KI-Modelle somit nicht in den Anwendungsbereich der KI-VO. Die Pflichten für die Akteure ergeben sich nur dann indirekt, wenn ein KI-Modell für die Integration in ein KI-System vorgesehen ist.⁶⁴

Im Rahmen der KI-VO wird der Begriff des KI-Modells enger gefasst, als es das allgemeine Verständnis vermuten lässt. Dies wird nicht zuletzt durch die Definitionen von Anbieter (Art. 3 Nr. 3 KI-VO) und Betreiber (Art. 3 Nr. 4 KI-VO) verdeutlicht. Aus diesen Definitionen geht hervor, dass KI-Modelle im Sinne der Verordnung keinen Betreiber haben und somit nicht in Betrieb genommen, wohl aber in den Verkehr gebracht werden können.

Der wesentliche Unterschied zwischen einem KI-Modell und einem KI-System liegt in ihrer Komplexität. Während sich KI-Modelle auf eine bestimmte Funktion

⁶⁰ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 50.

⁶¹ Vgl. Martini/Wendehorst/Wendehorst, Art. 3 Rn. 395.

⁶² Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 50; vgl. Klos/Taylan, CCZ 2024, 205, 207.

⁶³ Vgl. Martini/Wendehorst/Wendehorst, Art. 3 Rn. 419.

⁶⁴ Vgl. Voigt/Hullen, HdB-KI-Verordnung, S. 6.

konzentrieren und als Grundlage für zahlreiche KI-Systeme dienen, umfassen KI-Systeme weitere Komponenten und sind in der Lage, komplexere Aufgaben zu bewältigen.⁶⁵

2.2.2 Konzepte und Technologien

In Erwgr. 12 KI-VO wird als wesentliches Merkmal eines KI-Systems die Fähigkeit des Ableitens angeführt. Ein KI-System muss dabei nicht nur in der Lage sein, Ausgaben selbst abzuleiten, sondern auch den Prozess nachvollziehen können, durch den die Ausgabe zustande kommt. Während sich zur Erfüllung der Fähigkeit des Ableitens verschiedene Ansätze, Techniken und Modelle entwickelten, hat KI im Laufe der Zeit auch weitere wichtige Impulse erhalten. Hierzu zählt insbesondere das Wachstum der verfügbaren Datenmenge, welches insbesondere auf die zunehmende Verbreitung des Internets sowie die kontinuierliche Erweiterung der Infrastruktur zurückzuführen ist.⁶⁶

2.2.2.1 Turing Test

In der Literatur wird zwischen schwacher und starker KI unterschieden, wobei sich die Differenzierung auf den Grad von Intelligenz und Autonomie des Systems erstreckt.⁶⁷

Schwache KI (Artificial Narrow Intelligence) besitzt keine allgemeine Intelligenz und ist darauf ausgelegt, Aufgaben in einem begrenzten Anwendungsbereich zu lösen. Schwache KI agiert selbstständig, ermittelt Lösungen und optimiert stetig. Starke KI (Artificial General Intelligence) hingegen ist in der Lage, Aufgaben mit demselben Intelligenzniveau wie ein Mensch auszuführen und könnte in bestimmten Bereichen menschliche Fähigkeiten sogar übertreffen.⁶⁸

Alan Turing wird häufig „als Vater der KI“⁶⁹ bezeichnet, da er den bekannten Turing-Test entwickelte. Im Wesentlichen basiert der Test auf der Interaktion von drei Teilnehmern – zwei Menschen und einem Computer. Ziel des Tests ist es, zu untersuchen, ob ein Computer durch sein Verhalten und seine Kommunikation

⁶⁵ Vgl. Martini/Wendehorst/Wendehorst, Art. 3 Rn. 26 f.; Voigt/Hullen, HdB-KI-Verordnung, S. 6 f.

⁶⁶ Vgl. *Europäisches Parlament*, Was ist künstliche Intelligenz und wie wird sie genutzt? 2020, o.S.; Martini/Wendehorst/Wendehorst, Art. 3 Rn. 44; Taulli, Grundlagen der Künstlichen Intelligenz, S. 17.

⁶⁷ Vgl. Dahm/Zehnder, Moderne Personalführung mit Künstlicher Intelligenz, S. 7.

⁶⁸ Vgl. Dahm/Zehnder, Moderne Personalführung mit Künstlicher Intelligenz, S. 7 ff.; Witteler/Moll, NZA 2023, 327.

⁶⁹ Taulli, Grundlagen der Künstlichen Intelligenz, S. 2.

einen Menschen in so einem erheblichen Maße täuschen kann, dass dieser nicht mehr in der Lage ist, zwischen Mensch und Maschine zu unterscheiden.

Das vollständige Bestehen des Turing-Tests wird oft als Voraussetzung für die Klassifikation eines Systems als starke KI betrachtet. Da der Test bisher nicht – mit hinreichender Sicherheit – vollständig abgeschlossen wurde und eine starke KI somit nicht existiert, sind die Ausführungen und Analysen in dieser Arbeit gesamthaft auf dem aktuellen Stand der Entwicklung und somit vor dem Hintergrund der schwachen KI zu betrachten.⁷⁰

2.2.2.2 Trainingsdaten

Die Weiterentwicklung von KI-Systemen basiert maßgeblich auf der Verarbeitung großer Datensätze, die zu einem wesentlichen Anteil (ca. 70 Prozent) aus sogenannten Trainingsdaten bestehen. Trainingsdaten werden definiert als „Daten, die zur Erstellung eines KI-Algorithmus verwendet werden“.⁷¹ Das primäre Ziel von Trainingsdaten besteht darin, die Beziehungen innerhalb eines Algorithmus abzubilden, sodass das KI-System in der Lage ist, Muster zu identifizieren und darauf aufbauend Vorhersagen oder Entscheidungen zu treffen. Im Gegensatz dazu dienen Testdaten der Bewertung und Validierung eines Systems. Sie überprüfen das trainierte System auf seine Ergebnisse und die Verlässlichkeit der Daten.⁷²

Es gilt in dem Zusammenhang zu beachten, dass die Entwicklung von KI-Systemen durch die Verarbeitung unterschiedlicher Datentypen erfolgt. Diese lassen sich in drei Kategorien einteilen: strukturierte Daten, unstrukturierte Daten und semistrukturierte Daten.⁷³

Strukturierte Daten sind Daten, die eine klare Beschriftung und Formatierung aufweisen. Sie werden üblicherweise in Datenbanken oder Tabellenkalkulationen gespeichert. Als Beispiele lassen sich finanzielle Informationen, Sozialversicherungsnummern, Adressen und Produktinformationen anführen.⁷⁴ Unstrukturierte Daten hingegen verfügen über keine vordefinierte Formatierung oder Struktur.

⁷⁰ Vgl. *Taulli*, Grundlagen der Künstlichen Intelligenz, S. 2 ff., 210; *Witteler/Moll*, NZA 2023, 327.

⁷¹ *Taulli*, Grundlagen der Künstlichen Intelligenz, S. 210.

⁷² Vgl. *Pohlmann et al.*, ZVersWiss, 135, 138 f.; *Taulli*, Grundlagen der Künstlichen Intelligenz, S. 76.

⁷³ Vgl. *Taulli*, Grundlagen der Künstlichen Intelligenz, S. 24.

⁷⁴ Vgl. *Becker et al.*, Zukunft der Unternehmensdaten, 2024, S. 2; *Taulli*, Grundlagen der Künstlichen Intelligenz, S. 24.

Sie liegen in einer Vielzahl von Formaten vor und umfassen unter anderem Bilder, Videos, Audiodateien oder freie Texte.⁷⁵ Neben diesen beiden Kategorien existieren semistrukturierte Daten – diese stellen eine Mischform aus strukturierten und unstrukturierten Daten dar. Die Daten weisen zwar eine gewisse Organisation auf, folgen jedoch keinem festen Schema wie strukturierte Daten. In der Gesamtheit aller Daten machen semistrukturierte Daten nur etwa fünf bis zehn Prozent aus.⁷⁶

KI-Systeme werden sowohl mit strukturierten, unstrukturierten als auch semistrukturierten Daten entwickelt. Die Art der verwendeten Daten kann je nach Modellart und Zielsetzung der Systeme variieren. Es mag zunächst nahe liegen, dass die Quantität der Daten das wesentliche Kriterium für den Erfolg eines KI-Modells ist. Dies kann jedoch nicht uneingeschränkt bejaht werden, da eine zunehmende Datenmenge die Qualität der Daten negativ beeinflussen kann. Als eines der wesentlichen Erfolgskriterien gilt die Qualität der Daten, da diese maßgeblich die Qualität des KI-Systems bestimmt. Bereits fehlerhafte Daten führen mit einer hohen Wahrscheinlichkeit zu fehlerhaften Ausgaben des KI-Systems. Zur Sicherstellung der Datenqualität sollten die Daten daher die folgenden Anforderungen erfüllen: Vollständigkeit, Widerspruchsfreiheit, Konsistenz und Aktualität.

Sowohl die Sicherstellung der Datenqualität als auch der Datenmenge ist somit von zentraler Bedeutung, damit die Effektivität und Zuverlässigkeit von KI-Systemen gewährleistet werden kann.⁷⁷

2.2.2.3 Maschinelles Lernen, Deep Learning, Neuronale Netze

Algorithmen bilden die Grundlage einer Software und stellen zur Lösung einer Aufgabe eine eindeutige Vorgabe dar. Neben der Verwendung von Algorithmen stützen sich KI-Systeme zudem auf eine Vielzahl weiterer Methoden.⁷⁸ Begrifflichkeiten wie Neuronale Netze, Deep Learning oder Maschinelles Lernen beschreiben in diesem Zusammenhang vergleichbare, aber nicht synonym anwendbare Technologien. Sie alle stellen Teilgebiete der KI dar.⁷⁹ Deep Learning

⁷⁵ Vgl. *Becker et al.*, Zukunft der Unternehmensdaten, 2024, S. 2; *Taulli*, Grundlagen der Künstlichen Intelligenz, S. 24.

⁷⁶ Vgl. *Taulli*, Grundlagen der Künstlichen Intelligenz, S. 24.

⁷⁷ Vgl. *Heid*, Daten und Datenverarbeitung, o.S.; *Taulli*, Grundlagen der Künstlichen Intelligenz, S. 40.

⁷⁸ Vgl. *Witteler/Moll*, NZA 2023, 327.

⁷⁹ Vgl. *IBM*, Was ist maschinelles Lernen? o.S; *Wennker*, Künstliche Intelligenz in der Praxis, S. 9.

ist eine Unterkategorie des Maschinellen Lernens und basiert auf Neuronalen Netzen, die die Grundlage dieser Methode bilden.⁸⁰

Ziel ist es mit KI-Systemen menschliches Handeln nachzubilden. Hierzu wird sich künstlichen Neuronalen Netzen (Artificial Neural Networks) bedient und versucht, den Aufbau eines biologischen Gehirns nachzubilden. Neuronale Netze stellen einen wesentlichen Teil des Deep Learnings dar und ermöglichen es Computersystemen, komplexe Zusammenhänge in Daten eigenständig zu erkennen.⁸¹ Neuronale Netze sind strukturell durch Knotenschichten organisiert, wobei diese aus einer Eingabeschicht, einer oder mehreren verborgenen Schichten sowie einer Output-Schicht bestehen. Jeder dieser Knoten weist eine Verbindung zu einem anderen Knoten auf und verfügt über einen sogenannten Schwellenwert. Wird der Schwellenwert durch den Output eines Knotens überschritten, wird der Knoten aktiviert und die Daten werden an die nächste Schicht des Netzes weitergegeben.

Neuronale Netze lassen sich in sogenannten Deep-Neural-Networks und einfache neuronalen Netze unterteilen. Als entscheidender Unterschied gilt hierbei die Anzahl der Schichten. Ein Deep Neural Network liegt vor, sobald ein Netz aus mehr als drei Schichten besteht.⁸²

Maschinelles Lernen verfolgt das Ziel, Systeme zu entwickeln, die in der Lage sind, eigenständig aus Daten zu lernen, Muster zu erkennen und darauf basierend Vorhersagen sowie Entscheidungen zu treffen. Diese Systeme verbessern sich kontinuierlich auf Basis ihrer Erfahrungen, die sie während des Lernprozesses sammeln, ohne dabei explizit programmiert zu werden. Man spricht hierbei von selbst-adaptiven Algorithmen.⁸³

Maschinelles Lernen kann in drei Arten des Lernens unterteilt werden:⁸⁴

- Überwachtes Lernen (Supervised Learning): Bei diesem Ansatz erfolgt eine Kombination aus verifizierten Informationen und selbstständiges Erkennen von Erklärungsmustern.
- Unüberwachtes Lernen (Unsupervised Learning): Hierbei stehen keine Lösungen zur Verfügung, sodass die KI eigenständig Muster in den vorgegebenen Datensätzen erkennen muss.

⁸⁰ Vgl. *Ertel*, Grundkurs Künstliche Intelligenz, S. 3; *IBM*, Was ist maschinelles Lernen? o.S.; *Taulli*, Grundlagen der Künstlichen Intelligenz, S. 17 f.

⁸¹ Vgl. *Brune*, Künstliche Intelligenz heute, S. 194 f.; *IBM*, Was ist maschinelles Lernen? o.S.; *Witteler/Moll*, NZA 2023, 327.

⁸² Vgl. *IBM*, Was ist maschinelles Lernen? o.S.

⁸³ Vgl. *Dahm/Zehnder*, Moderne Personalführung mit Künstlicher Intelligenz, S. 4.

⁸⁴ Vgl. *Dahm/Zehnder*, Moderne Personalführung mit Künstlicher Intelligenz, S. 4 ff.

- Verstärkendes Lernen (Reinforcement Learning): Bei diesem Ansatz liegt kein optimaler Lösungsweg vor und die KI lernt durch die Interaktion mit der Datenumgebung einen Lösungsweg zu identifizieren.

Als eine Unterkategorie des Maschinellen Lernens gilt das „Deep Learning“. Diese Technologie ist eine spezielle Methode des Maschinellen Lernens, da sie auf tiefere Neuronale Netze zurückgreift und aufgrund dessen in der Lage ist komplexe Muster in großen und unstrukturierten Datenmengen zu erkennen.⁸⁵ Betrachtet man die Techniken im Einzelnen, zeigt sich, dass das Maschinelle Lernen in einem höheren Maße auf das Eingreifen von Menschen angewiesen ist. Deep Learning und Neuronale Netze agieren demgegenüber autonomer, was sie zu wesentlichen Treibern der stetigen Fortschritte im Bereich der KI macht.⁸⁶

2.2.2.4 Generative KI

Generative KI beschreibt eine Kategorie von KI, die anders als die zuvor dargelegten Technologien darauf ausgelegt ist, eigenständig neue Inhalte zu generieren. Dabei können Texte, Bilder, Musik und/ oder Videos generiert werden. Generative KI greift nicht ausschließlich auf bereits bestehende Datensätze zurück, sondern schafft auch neue Variationen. Diese Eigenschaft spricht generativer KI ein hohes Potential zu, wobei diese Tatsache gleichermaßen eine vorausschauende und anpassungsfähige Governance-Struktur erfordert.⁸⁷

2.3 Corporate Governance

Nicht zuletzt aufgrund zahlreicher Unternehmensskandale im Bereich der Wirtschaftsdelikte und der wachsenden Anzahl an Risiken, entwickelt sich Corporate Governance zunehmend als zentrales Instrument zur Stärkung einer verantwortungsvollen Unternehmensführung.⁸⁸

⁸⁵ Vgl. *Dahm/Zehnder*, Moderne Personalführung mit Künstlicher Intelligenz, S. 6; *DCGK*, 2022, S. 2; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 6.

⁸⁶ Vgl. *IBM*, Was ist maschinelles Lernen? o.S.

⁸⁷ Vgl. *IBM*, Was ist KI-Governance? o.S.

⁸⁸ Vgl. *Kreipl*, Verantwortungsvolle Unternehmensführung, S. 28 f.; *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 256.

2.3.1 Definitionen und Kernaspekte

Als Corporate Governance wird jener Rahmen bezeichnet, in dem ein Unternehmen geführt und überwacht wird – dies umfasst die Gesamtheit der Regeln, Prozesse und Systeme, die eine verantwortungsvolle, transparente und regelkonforme Unternehmensführung gewährleistet.⁸⁹

Corporate Governance ist der Rahmen, innerhalb dessen ein Unternehmen sowohl geleitet als auch kontrolliert wird. Das Bestreben liegt darin, klare Ziele zu setzen sowie einen verantwortungsvollen Umgang mit Risiken sicherzustellen. Zudem sollen die Interessen aller Stakeholder berücksichtigt werden, um Konflikten untereinander entgegenzuwirken.⁹⁰ Die wesentlichen Akteure sind neben dem Vorstand und dem Aufsichtsrat die weiteren Organe der jeweiligen Gesellschaft. Der Vorstand und der Aufsichtsrat sind dazu verpflichtet, gemäß den Prinzipien der sozialen Marktwirtschaft zu handeln und dabei die Transparenz zu fördern. Mit diesen Grundsätzen und der Berücksichtigung der Bedürfnisse der Stakeholder wird sowohl bei internen als auch externen Stakeholdern Vertrauen geschaffen und dadurch ein langfristiger Unternehmenserfolg ermöglicht.⁹¹

Eine effektive Corporate Governance-Struktur zeichnet sich durch die folgenden Elemente aus: Compliance-Management, Risikomanagement und Internes Kontrollsystem (IKS). Diese Bereiche sind dafür verantwortlich, Ziele festzulegen, Risiken zu beurteilen, Maßnahmen aufzusetzen und die Systeme im Unternehmen zu überwachen.⁹²

Obwohl die zuvor aufgeführten Kernelemente in den meisten Definitionen von Corporate Governance enthalten sind, existiert weder eine einheitliche Definition für diesen Begriff noch für die Compliance-Funktion eines Unternehmens.⁹³ Dies führt insbesondere in der Praxis zu Schwierigkeiten bei der Abgrenzung. Ungeachtet der fehlenden Definitionen lassen sich die beiden Funktionen jedoch insofern voneinander abgrenzen, als dass Compliance als Bestandteil einer effektiven Corporate Governance betrachtet werden kann. Während sich die Tätigkeiten von Mitarbeitenden in der Compliance-Abteilung vornehmlich auf die Einhaltung externer und interner Vorschriften konzentrieren, beschäftigt sich die Co-

⁸⁹ Vgl. *Kreipl*, Verantwortungsvolle Unternehmensführung, S. 38 f.; *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 256; *OECD*, G20/OECD, 2024, S. 8.

⁹⁰ Vgl. *Kreipl*, Verantwortungsvolle Unternehmensführung, S. 38 f.

⁹¹ Vgl. DCGK, 2022, S. 2

⁹² Vgl. *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 287.

⁹³ Vgl. *Kreipl*, Verantwortungsvolle Unternehmensführung, S. 43.

porate Governance-Funktion mit der Struktur und Überwachung des Unternehmens im Gesamten. Dies führt auch zu einer Differenzierung der jeweiligen Stakeholder der beiden Funktionen.⁹⁴

2.3.2 Bedeutung für Unternehmen

Die Bedeutung von Corporate Governance hat sich im Laufe der Zeit erweitert. Ursprünglich lag der Fokus primär auf börsennotierten und börsenorientierten Unternehmen, während Corporate Governance heute auch für KMU relevant ist. Zu dieser Entwicklung hat die steigende Anzahl wirtschaftlichen Fehlverhaltens und der daraus resultierenden Regulierungsanforderungen beigetragen.⁹⁵

2.3.2.1 Deutscher Corporate Governance Kodex

Nicht zuletzt aufgrund diverser Unternehmensskandale entschloss sich die Bundesregierung im Jahr 2002 den sogenannten Deutschen Corporate Governance Kodex (DCGK) einzuführen.⁹⁶ Der Kodex definiert Best-Practice-Ansätze für eine gute Unternehmensführung und richtet sich primär an börsennotierte Unternehmen. Gemäß § 161 AktG müssen diese erklären, inwieweit sie den Empfehlungen des Kodex folgen. Die Regelung „Comply or Explain“ (deutsch: „einhalten und erklären“) ermöglicht den Unternehmen Abweichungen, sofern sie ausreichend begründet sind.⁹⁷

Der DCGK wird von der Regierungskommission jährlich überprüft, sodass sichergestellt wird, dass dieser stets den aktuellen Anforderungen entspricht.⁹⁸

2.3.2.2 Business Judgement Rule

Von dem Gedanken ausgehend, dass das Eingehen bestimmter Risiken aus geschäftspolitischer Sicht vereinzelt sinnvoll sein kann, erkannte der Gesetzgeber vor der Einführung des § 93 AktG, dass haftungsfreie Handlungsspielräume für Vorstände unvermeidbar sind.⁹⁹ Aus diesen rechtlichen Überlegungen hat sich

⁹⁴ Vgl. *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 257-259.

⁹⁵ Vgl. *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 268.

⁹⁶ Vgl. *DCGK*, 2022; *Kreipl*, Verantwortungsvolle Unternehmensführung, S. 55.

⁹⁷ Vgl. *Kreipl*, Verantwortungsvolle Unternehmensführung, S. 56; *MüKoAktG/Goette*, § 161 Rn. 1.

⁹⁸ Vgl. *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 279.

⁹⁹ Vgl. *BGH*, Urt. v. 21.4.1997, II ZR 175/95, 1926 - *ARAG/Garmenbeck*; *Berwanger*, Business Judgement Rule, o.S.

im Laufe der Zeit die sogenannte „Business Judgement Rule“¹⁰⁰ entwickelt. Sie dient als Leitlinie für Vorstände und Geschäftsführer im Rahmen ihrer Entscheidungskompetenz. Sofern diese im guten Glauben und im Unternehmensinteresse handeln, sind sie vor einer Haftung geschützt, vorausgesetzt sie halten die gebotenen Sorgfaltspflichten ein (§ 93 Abs. 1 AktG bzw. § 43 GmbHG).¹⁰¹

2.3.2.3 Three-Lines-of-Defense-Modell

Im Anschluss an die Etablierung einer Governance-Struktur ist es erforderlich, dass die hierdurch definierte Unternehmensstruktur sowie die sich daraus ergebenden Unternehmensabläufe regelmäßig überprüft und verbessert werden. Die Verantwortung für die Implementierung eines effektiven Kontroll- und Überwachungssystems liegt bei der Geschäftsleitung eines Unternehmens. Zur Abbildung der wiederkehrenden Aktivitäten wie das Durchführen, Überprüfen und Verbessern wurde ursprünglich in der Finanzbranche das Three-Lines-of-Defense-Modell als Bestandteil der Corporate Governance-Struktur geschaffen. Das Modell erweist sich aufgrund seiner Flexibilität jedoch auch für andere Branchen, die mit Risiken und Compliance-Anforderungen konfrontiert sind, als wertvoll.¹⁰² Das Modell verfolgt das Ziel, durch drei voneinander unabhängige Verteidigungslinien die Geschäftsleitung bei der Erfüllung ihrer Kontroll- und Überwachungsaufgabe zu unterstützen.¹⁰³

Als erste Verteidigungslinie werden die operativen Einheiten eines Unternehmens definiert. Diese sind im Rahmen des täglichen Geschäftsablaufs für das Risikomanagement verantwortlich und für die Implementierung prozessintegrierter interner Kontrollen in ihrem jeweiligen Tätigkeitsbereich.¹⁰⁴

Die zweite Verteidigungslinie besteht klassischerweise aus unabhängigen Funktionen wie dem Risikomanagement und der Compliance-Funktion. Diese Bereiche fungieren als Kontroll- und Überwachungsfunktionen des Unternehmens und stellen somit auch die Funktionsfähigkeit der in der ersten Verteidigungslinie etablierten Kontrollmechanismen sicher. Darüber hinaus werden von der zweiten

¹⁰⁰ „Regel der geschäftlichen Beurteilung“; Vgl. *MüKoAktG/Spindler*, § 93 Rn. 120 f.; *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 269.

¹⁰¹ Vgl. *MüKoAktG/Spindler*, § 93 Rn. 120 f.; *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 257, 269.

¹⁰² Vgl. *Kreipl*, Verantwortungsvolle Unternehmensführung, S. 88.

¹⁰³ Vgl. *Becker et al.*, *HdB-MaRisk*, S. 308 f.; *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 257, 278 f.

¹⁰⁴ Vgl. *Becker et al.*, *HdB-MaRisk*, S. 309; *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 278 f.

Verteidigungslinie Richtlinien für den Umgang mit Risiken im Unternehmen entwickelt. Zudem dienen sie als Beratung und Unterstützung für die erste Verteidigungslinie.¹⁰⁵

Die Interne Revision bildet die dritte Verteidigungslinie. Diese überwacht die ersten beiden Verteidigungslinien und stellt deren Funktionsfähigkeit, insbesondere in Bezug auf das Kontrollsystem, sicher.¹⁰⁶

Mit Hilfe des Three-Lines-of-Defense-Modells kann eine klare Zuordnung der Verantwortlichkeiten vorgenommen und die vollständige Überwachung sowie Kontrolle der Risiken innerhalb des Unternehmens sichergestellt werden.

Im weiteren Verlauf der Arbeit wird das Three-Lines-of-Defense-Modell im Rahmen der Auslegung der KI-VO herangezogen. Dabei ist zu berücksichtigen, dass nicht alle Unternehmen über solche Strukturen im Rahmen ihrer Corporate Governance verfügen, sodass die in dieser Arbeit dargestellten Ausführungen nur als Orientierung anzusehen sind.

2.3.2.4 IDW-Prüfungsstandard

Compliance-Management, Risikomanagement und IKS sind wesentliche Komponenten der Corporate Governance und können regelmäßigen Prüfungen unterliegen. Während das Corporate Governance-System häufig in seiner Gesamtheit geprüft wird, besteht auch die Möglichkeit, einzelne Teilgebiete zu prüfen. Neben freiwilliger Prüfungsmöglichkeiten bestehen Verpflichtungen im Rahmen gesetzlich vorgeschriebener Abschlussprüfungen. Auch die interne Revision, als unabhängige Kontrollinstanz, stellt die Funktionsfähigkeit des IKS sicher, prüft die Effektivität des Risikomanagementprozesses und die Einhaltung rechtlicher sowie interner Vorgaben (Compliance-Management).¹⁰⁷

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) hat die sogenannten IDW-Prüfungsstandards (IDW PS) in Form von Richtlinien entwickelt. Sie dienen zur Schaffung eines einheitlichen Rahmens für die Durchführung von Prüfungen und definieren spezifische Anforderungen für unterschiedliche Prüfungsbereiche. Die IDW PS 980, 981 und 982 bilden die Grundlage für die Überprüfung des Compliance-Management-Systems, des Risikomanagementsystems und IKS. Sie ermöglichen sowohl eine Prüfung des Corporate-Governance-Management-Systems als Ganzes als auch eine isolierte Prüfung einzelner Teilbereiche. Die

¹⁰⁵ Vgl. *Becker et al.*, HdB-MaRisk, S. 309; *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 278 f.

¹⁰⁶ Vgl. *Becker et al.*, HdB-MaRisk, S. 309.

¹⁰⁷ Vgl. *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 286 ff.

genannten Standards tragen wesentlich zu der Bewertung der Wirksamkeit von Corporate Governance-Strukturen bei.¹⁰⁸

Auf die spezifischen Prüfungsstandards und -vorgaben wird aufgrund des Schwerpunkts und Umfangs der vorliegenden Arbeit nicht weiter eingegangen.

2.4 Schnittstelle Corporate Governance und Künstliche Intelligenz

Gesetzliche Vorgaben und Corporate Governance überschneiden sich an der Schnittstelle zwischen verantwortungsvoller Unternehmensführung und regulatorischen Anforderungen. Eine effiziente und regelkonforme Unternehmensführung setzt die Prüfung regulatorischer Anforderungen sowie deren Integration in bestehende Governance-Strukturen voraus. Nur so können Unternehmen sicherstellen, dass sowohl gesetzliche Anforderungen eingehalten als auch betriebswirtschaftliche Ziele erreicht werden.

Der Vorstand sowie der Aufsichtsrat repräsentieren den zentralen Kern eines Unternehmens, dessen Schutz eine wesentliche Aufgabe der Corporate Governance-Funktionen darstellt. Die Funktionen der Corporate Governance fungieren als eine schützende Hülle, die den Kern vor externen Risiken und potenziellen Haftungsansprüchen abschirmen.¹⁰⁹

¹⁰⁸ Vgl. *IDW*, IDW Verlautbarungen, S. 2; *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 280 ff.

¹⁰⁹ Vgl. *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 256, 286 f.

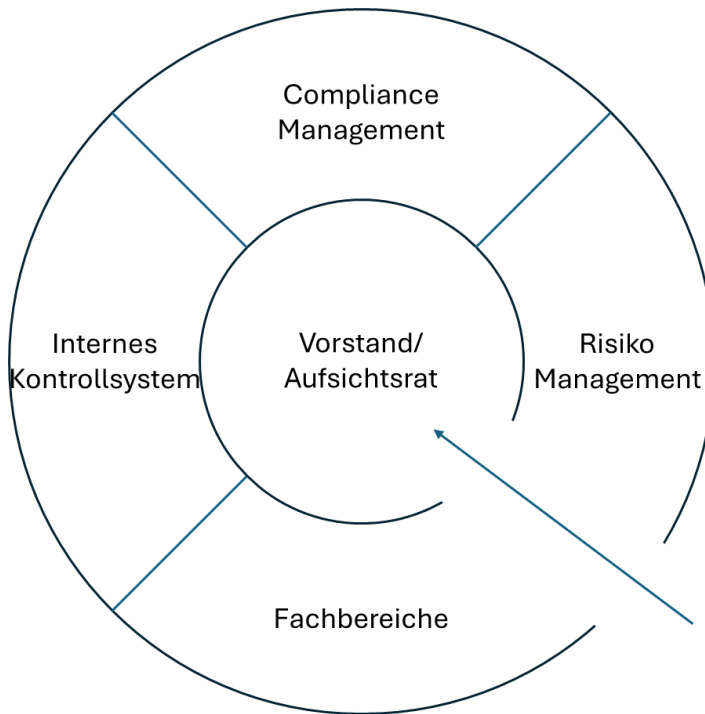
Abbildung 1: Corporate Governance als Schutzmechanismus

Abbildung 1 veranschaulicht in Anlehnung der bisherigen Ausführungen die Elemente einer Corporate Governance sowie die Beziehung dieser zueinander. Deutlich wird insbesondere, dass die Governance eines Unternehmens den Rahmen aller Teilfunktionen bildet und somit für alle Stakeholder im Unternehmen von Relevanz ist. Die zentralen Funktionen der Corporate Governance zielen darauf ab, die Unternehmensführung zu schützen, zu überwachen und die Entscheidungen kritisch zu prüfen.¹¹⁰ Besonders hervorzuheben ist, dass Corporate Governance die gesamte Organisation umfasst, sodass auch die einzelnen Fachbereiche eines Unternehmens eine wesentliche Rolle spielen. Nur im Falle eines reibungslosen Zusammenspiels aller Funktionen kann der Vorstand umfassend vor allen Risiken geschützt werden.¹¹¹

Die neuen KI-Technologien bieten einerseits das Potential zur Risikominimierung, andererseits können sie jedoch auch neue Risiken aufdecken oder erzeugen.

¹¹⁰ Vgl. Schackmann/Ziegler, Praxisorientiertes Managementwissen, S. 256.

¹¹¹ Vgl. Kreipl, Verantwortungsvolle Unternehmensführung, S. 1, 104; Schackmann/Ziegler, Praxisorientiertes Managementwissen, S. 257.

gen. Sie bergen gleichzeitig die Gefahr fehlerhafter Ergebnisse oder Vorhersagen. Auch Erwgr. 5 KI-VO führt aus, dass der Einsatz von KI Risiken mit sich bringen kann und auch das öffentliche Interesse sowie durch das Unionsrecht geschützte Rechte geschädigt werden können. Dies unterstreicht die Notwendigkeit einer effektiven KI-Governance, die darauf ausgerichtet ist, die mit dem Einsatz von KI verbundenen Risiken zu identifizieren und angemessen zu kontrollieren.¹¹²

Unternehmen stehen vor der Herausforderung, regulatorische Vorgaben und Richtlinien umzusetzen, ohne ihre Innovationsfähigkeit einzuschränken. Klar definierte Rahmenbedingungen, die sowohl die Regelkonformität als auch einen Spielraum für Innovation bieten, sind dabei unerlässlich.¹¹³

Mit der Einführung der KI-VO werden klare Anforderungen an den Einsatz von KI-Systemen definiert, die sich an deren Gefährdungspotential orientieren. Betreiber und Anbieter solcher Systeme sind verpflichtet, diese Anforderungen zu erfüllen und durch erhöhte Transparenzpflichten nachzuweisen. Fest etablierte Governance-Strukturen spielen dabei eine entscheidende Rolle: Sie gewährleisten neben der Einhaltung regulatorischer Vorgaben auch die Förderung des Vertrauens der Stakeholder.¹¹⁴ Dies bildet eine wesentliche Grundlage für einen nachhaltigen Unternehmenserfolg und die Akzeptanz innovativer Technologien.

Durch die mit der KI-Governance einhergehenden regelmäßigen Audits und Überprüfungen wird die Konformität der eingesetzten KI-Systeme mit den geltenden Standards sowie die kontinuierliche Anpassungsmöglichkeit sichergestellt. Hinzu kommt auch, dass mit der zunehmenden Bedeutung und Einführung der KI-VO die Zuständigkeiten und Verantwortlichkeiten definiert werden müssen. Im Rahmen von Governance-Strukturen werden Kommunikationswege und Entscheidungsprozesse festgelegt, um eine effektive Zusammenarbeit zwischen den beteiligten Akteuren sicherzustellen.¹¹⁵ Versäumen es Unternehmen, auf neue Risiken angemessen zu reagieren, ihre Governance-Strukturen anzupassen oder Kommunikationswege zu optimieren, können sich Lücken im Governance-Rahmen ergeben. Diese Lücken können dazu führen, dass Risiken auf die Unternehmensführung durchschlagen. Insofern diese Lücken aufgrund einer Verletzung der Sorgfaltspflicht entstehen, drohen der Unternehmensführung haftungsrechtliche Konsequenzen gemäß § 93 Abs. 1 AktG bzw. § 43 GmbHG.¹¹⁶

¹¹² Vgl. *Becker et al.*, Zukunft der Unternehmensdaten, 2024, S. 13; *Reese*, BB 2024, 1515.

¹¹³ Vgl. *Reese*, BB 2024, 1515.

¹¹⁴ Vgl. *Kreipl*, Verantwortungsvolle Unternehmensführung, S. 35 f.

¹¹⁵ Vgl. *Reese*, BB 2024, 1515, 1517.

¹¹⁶ Vgl. *Schackmann/Ziegler*, Praxisorientiertes Managementwissen, S. 257, 269.

Abbildung 1 verdeutlicht, dass eine unzureichende Erfüllung der Aufgaben einer Funktion die Durchdringung der Risiken begünstigt und die Unternehmensführung hierdurch der Unternehmenshaftung ausgesetzt ist.

Auch auf Unionsebene wurde im Rahmen der KI-VO eine Governance-Struktur etabliert und somit die Bedeutung ebendieser im Zusammenhang mit KI hervorgehoben (Art. 64 ff. KI-VO). Die Struktur umfasst mit dem KI-Büro (Art. 64 KI-VO), dem Europäischen Gremium für KI (Art. 65 und 66 KI-VO), dem Beratungsforum (Art. 67 KI-VO) und dem wissenschaftlichen Gremium (Art. 68 KI-VO) vier Institutionen. Ziel dieser Governance-Struktur ist es gemäß Erwgr. 138 f. KI-VO die Mitgliedstaaten einerseits zu entlasten und andererseits eine harmonisierte Anwendung der Verordnung innerhalb der EU zu gewährleisten.¹¹⁷

Während das KI-Büro im Wesentlichen die Kommission unterstützt, besteht die Aufgabe des KI-Gremiums in der Koordination der verschiedenen Akteure und der Harmonisierung der Sicherstellung einer einheitlichen Auslegung und Anwendung der Verordnung. Das Beratungsforum wird auf Ersuchen des KI-Gremiums oder der Kommission tätig und stellt insbesondere technisches Fachwissen bereit. Insbesondere bei komplexen Fragestellungen im Bereich der GPAI-Modelle erhält das KI-Büro Unterstützung durch das wissenschaftliche Gremium, das aus unabhängigen Sachverständigen besteht.¹¹⁸

¹¹⁷ Vgl. Martini/Wendehorst/*Roth-Isigkeit*, Art. 64 Rn. 2; *Vertretung in Deutschland*, KI-Gesetz tritt in Kraft, 2024, o.S.

¹¹⁸ Vgl. *Deutscher Bundestag*, Positionspapier, S. 4; Martini/Wendehorst/*Roth-Isigkeit*, Art. 64 Rn. 2.

3 Umsetzungsleitfaden – Anforderungen KI-Verordnung

Nachdem nun die Grundlagen der KI und die Schnittstelle zur Corporate Governance dargelegt worden sind, werden in diesem Kapitel die Anforderungen aus der KI-VO genauer beleuchtet.

3.1 Vorabprüfung

Bevor sich Unternehmen mit der Umsetzung der Anforderungen aus der KI-VO auseinandersetzen, müssen sie prüfen, ob sie in den Anwendungsbereich fallen und somit Adressat der Verordnung sind.

Hierzu sollte zunächst die Frage, ob Berührungspunkte zu KI-Systemen bestehen beantwortet werden. Insofern diese Frage bejaht werden kann, ist der sachliche Anwendungsbereich der KI-VO eröffnet.¹¹⁹ Auch die Frage, ob der räumliche Anwendungsbereich greift, muss beantwortet werden. Letzteres ist der Fall, wenn das Unternehmen auf dem EU-Markt agiert und ein KI-System auf diesem Markt in den Verkehr bringt, in Betrieb nimmt oder dessen Ergebnisse innerhalb der EU verwendet.¹²⁰

Eine differenzierte Bewertung des Anwendungsbereichs setzt eine Inventarisierung aller im Unternehmen eingesetzten KI-Systeme sowie deren Klassifizierung voraus. Erst auf dieser Grundlage kann abschließend beurteilt werden, in welcher Form der persönliche, sachliche und räumliche Anwendungsbereich eröffnet ist. Die abschließende Bewertung erfolgt somit parallel zu den Umsetzungsmaßnahmen.

Es ist hervorzuheben, dass die in dieser Arbeit beschriebenen Prüfungsschritte nicht zwingend als chronologisch anzusehen sind. Vielmehr kann auch eine parallele Betrachtung und Bearbeitung vereinzelt zielführend sein.

3.2 Vorbereitende Maßnahmen

Angesichts der Vielzahl einschlägiger Rechtsgebiete, wie z.B. Datenschutz, Wettbewerbsrecht und Markenrecht, verfügen viele Unternehmen bereits über etablierte Governance-Strukturen sowie Compliance- und Datenschutz-Management-Systeme. Diese bestehenden Strukturen sollten seitens der Unternehmen

¹¹⁹ Vgl. Martini/Wendehorst/Wendehorst, Art. 3 Rn. 3; Ulbricht et al., Praxishandbuch KI und Recht, S. 162.

¹²⁰ Vgl. Martini/Wendehorst/Wendehorst, Art. 2 Rn. 4; Wybitul, BB 2024, 2179.

genutzt und entsprechend den Vorgaben aus der KI-VO ausgebaut bzw. optimiert werden.¹²¹

Analog der bereits beschriebenen Corporate Governance-Strukturen umfasst der Begriff der KI-Governance, ein System aus Rahmenwerken, Regeln und Prozessen, die in einem Unternehmen implementiert werden. Mit Hilfe der Etablierung einer solchen KI-Governance-Struktur können Unternehmen sicherstellen, dass der Einsatz von KI-Anwendungen in Übereinstimmung mit den rechtlichen und ethischen Vorgaben erfolgt. Eine effektive Governance-Struktur kann dazu beitragen, die Innovationspotentiale von KI vollständig auszuschöpfen, ohne diese dabei zu hemmen.

Auch nach außen schafft eine funktionierende KI-Governance-Struktur Transparenz, Zuverlässigkeit und Vertrauen.¹²²

3.2.1 Identifizierung Rollen und Verantwortlichkeiten

Um die Anforderungen der KI-VO effektiv umzusetzen, ist es zunächst erforderlich, die Zuständigkeiten im Unternehmen zu definieren. Die Überwachung kann durch eine bereits bestehende Kontrollfunktion in der zweiten Verteidigungslinie, wie z.B. Compliance oder Risikomanagement, erfolgen. Alternativ besteht die Möglichkeit, eine neue Abteilung für die spezifischen Anforderungen im Bereich KI zu schaffen. Diese Einheit könnte in der ersten Verteidigungslinie angesiedelt werden, wodurch die bereichsübergreifende Zusammenarbeit im Unternehmen gefördert wird und sich gleichzeitig die Möglichkeit der internen Überprüfung durch die zweite Verteidigungslinie bietet.¹²³

Die KI-VO verlangt im Gegensatz zu anderen Gesetzen keine Benennung eines KI-Beauftragten. Aufgrund der Tatsache, dass sowohl die Implementierung der KI-Systeme als auch die Einhaltung der gesetzlichen Anforderungen ein hohes Maß an Fachwissen voraussetzt, stellt die Ernennung eines solchen KI-Beauftragten jedoch ein für Unternehmen strategisch sinnvolles Mittel dar. Analog der Ernennung eines Datenschutzbeauftragten gemäß Art. 37 ff. DSGVO dient der KI-Beauftragte als zentrale Kontaktperson für KI-bezogene Fragestellungen. Neben der Sicherstellung der Einhaltung aller Standards fungiert der KI-Beauftragte

¹²¹ Vgl. *Buchalik/Gehrmann*, CR 2024, 145, 152; *Klos/Taylan*, CCZ 2024, 205, 210.

¹²² Vgl. *Kreutzer*, Künstliche Intelligenz verstehen, S. 472 f.; *Reese*, BB 2024, 1515, 1518.

¹²³ Vgl. *Spitznagel*, Vertrauenswürdige KI, 2024, o.S.

auch als Vermittler zwischen verschiedenen Unternehmensbereichen und der Geschäftsleitung.¹²⁴

Insbesondere zu Beginn scheint die Einrichtung eines KI-Gremiums sinnvoll, damit sowohl ein koordinierter Ansatz im Umgang mit KI geschaffen werden als auch das Fachwissen der Governance-Einheiten zwecks Einführung eines neuen Rechtsrahmens gebündelt werden kann. Auch langfristig kann ein solches Gremium von Vorteil sein, um die Überwachung und Steuerung der KI-Themen im Unternehmen kontinuierlich sicherzustellen. Das Gremium sollte die wichtigsten Bereiche – sowohl Fachbereiche als auch Kontrollfunktionen – umfassen. Eine mögliche Zusammensetzung ergibt sich aus der Rechtsabteilung, Compliance, Risikomanagement, Datenschutz, Informationstechnologie (IT), Personal sowie einer gegebenenfalls etablierten KI-Abteilung.¹²⁵

Dadurch, dass die KI-Governance integraler Bestandteil der bestehenden Governance-Strukturen wird und aus verschiedenen Funktionen des Unternehmens besteht, kann sichergestellt werden, dass hinsichtlich des KI-Risikos alle relevanten Prozesse integriert und angemessen berücksichtigt werden. Mit Hilfe der engen Zusammenarbeit zwischen allen relevanten Kontrollfunktionen wird zudem stetig sichergestellt, dass sämtliche Einheiten eingebunden und hinsichtlich der Risikobewertung abgeholt werden.¹²⁶

3.2.2 Einbindung Betriebsrat

Mit der Einführung von KI-Systemen werden auch Betriebsräte zunehmend vor Herausforderungen gestellt. Insbesondere die Tatsache der fehlenden Fachkenntnis im Bereich der KI-Technologien und die damit verbundene Schwierigkeit, die potenziellen Auswirkungen zu bewerten, sorgt für Unsicherheiten. Neben vielen Chancen birgt der Einsatz von KI auch eine Vielzahl von Risiken, welche sich unter anderem auf die Sicherheit der Arbeitnehmenden auswirken können.¹²⁷ Auch im Hinblick auf den Einsatz von KI verfügt der Betriebsrat (BR) über umfassende Mitbestimmungsrechte, die in den §§ 87 ff. BetrVG geregelt sind und bei der Einführung solcher Systeme nicht außer Acht gelassen werden dürfen.¹²⁸

Damit die Unternehmen den Schutz der Mitarbeitenden auch weiterhin angemessen gewährleisten können und ein rechtlicher Rahmen geschaffen werden kann, müssen die internen Vorgaben präzisiert und erweitert werden. Als eine sinnvolle

¹²⁴ Vgl. *Klos/Taylan*, CCZ 2024, 205, 210; *Martini/Wendehorst/Wendehorst*, Art. 4 Rn. 18 f.

¹²⁵ Vgl. *Klos/Taylan*, CCZ 2024, 205, 210; *Kreutzer*, Künstliche Intelligenz verstehen, S. 472.

¹²⁶ Vgl. *Reese*, BB 2024, 1515, 1518.

¹²⁷ Vgl. *Lugowski*, Rahmen-Betriebsvereinbarung KI, 2024, o.S.

¹²⁸ Vgl. *Krimphove*, ZWH 2024, 249, 253.

Maßnahme erweist sich hierbei der Beschluss einer Rahmen-Betriebsvereinbarung für den Umgang mit KI. Mit Hilfe dieser Vereinbarung soll nicht das Ziel verfolgt werden, den Einsatz von KI zu erschweren, sondern vielmehr eine Grundlage für deren Einsatz und den Schutz der Mitarbeitenden zu schaffen.¹²⁹

Inhaltlich sollte solch eine Betriebsvereinbarung insbesondere folgende Themen aufgreifen: Zielsetzung des Einsatzes von KI, ethische Grundsätze, Einhaltung gesetzlicher Bestimmungen, Festlegung der Verantwortlichkeiten, Datenschutz, Schulung und Qualifizierung sowie die Implementierung von angemessenen Kontroll- und Überwachungsmechanismen.¹³⁰

Neben einer allgemeinen Betriebsvereinbarung steht es den Unternehmen frei, weitere und somit spezifischere Vereinbarungen zu treffen. Ein Beispiel hierfür ist die Nutzung von generativen KI-Modellen wie ChatGPT. Hierbei eröffnet sich die Möglichkeit, die Nutzung ebendieser Modelle unternehmensspezifisch einzugrenzen, aber auch vollständig zu untersagen. Damit den Mitarbeitenden und somit auch der Arbeitseffizienz die neuen Technologien jedoch nicht vorenthalten bleiben, besteht für Unternehmen die Möglichkeit, unternehmenseigene, den externen Modellen gleichwertige Systeme zu entwickeln oder entwickeln zu lassen. Diese können insbesondere aus datenschutzrechtlicher Sicht in einem geschützteren internen Umfeld eingesetzt werden.¹³¹

3.2.3 Identifizierung bestehender Governance-Strukturen und Prozessschritte

Damit Unternehmen sich optimal auf die bevorstehenden Anpassungen ihrer Strukturen vorbereiten können, ist es von entscheidender Bedeutung, in der Phase der Vorbereitung zunächst die bestehenden Governance-Strukturen und bereits implementierten Prozessschritte zu identifizieren. Hierbei ist es wichtig, sowohl die bestehenden Organisationsmodelle zu berücksichtigen als auch die bereits angewandten Prozesse für konventionelle IT-Systeme zu analysieren und dokumentieren. Zudem sollten weitere einschlägige rechtliche Entwicklungen fortlaufend beobachtet und während der Implementierungsphase der KI-VO be-

¹²⁹ Vgl. *Krimphove*, ZWH 2024, 249, 253; *Lugowski*, Rahmen-Betriebsvereinbarung KI, 2024, o.S.

¹³⁰ Vgl. *Lugowski*, Rahmen-Betriebsvereinbarung KI, 2024, o.S.

¹³¹ Vgl. *Lugowski*, Rahmen-Betriebsvereinbarung KI, 2024, o.S.

rücksichtigt werden. Als Beispiel für die Finanzbranche lässt sich in dem Zusammenhang die Verordnung über digitale operationale Resilienz (Digital Operational Resilience Act, DORA)¹³² anführen.

Hierdurch wird deutlich, dass eine frühzeitige Einbindung der zentralen Stakeholder von wesentlicher Bedeutung ist. Neben der Rechtsabteilung, Compliance und Risikomanagement umfasst dies auch den Vorstand. Als besonders relevant erweist sich in dem Zusammenhang auch die Abteilung für IT, die eine zentrale Rolle bei der technischen Umsetzung von KI einnimmt.¹³³

Unternehmen stellen durch die Analyse der bereits bestehenden Strukturen sowie der frühzeitigen Einbindung aller relevanten Stakeholder sicher, dass Synergien optimal genutzt und die Effektivität der Governance-Strukturen gesteigert werden.¹³⁴

3.2.4 Einführung Meldewege und Überwachungsmaßnahmen

Für den Gebrauch von KI-Systemen sind klare Meldewege und wirksame Überwachungsmaßnahmen zu definieren und die Anforderungen in einer Richtlinie verbindlich festzuhalten. Auch bei bereits bestehenden Risiken wurde in der Vergangenheit häufig auf die Einführung spezifischer Richtlinien als rechtlicher Rahmen zurückgegriffen, sodass dieser Ansatz auch im Umgang mit den KI-Risiken sinnvoll erscheint.¹³⁵

3.2.4.1 KI-Richtlinie

Eine solche KI-Richtlinie stellt eine klassische Compliance-Maßnahme dar und trägt wesentlich dazu bei, dass die mit dem Einsatz von KI-Systemen einhergehenden Risiken minimiert werden.¹³⁶

Zu Beginn der Richtlinie führt eine Einleitung in das Thema ein und erläutert dabei den Hintergrund und den Anwendungsbereich der KI-Richtlinie hinreichend. Zudem muss die Richtlinie die Verantwortlichkeiten im Unternehmen klar definieren.

¹³² Vgl. Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnung (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, ABI. Nr. L 333 v. 27.12.2022.

¹³³ Vgl. *Kreutzer*, Künstliche Intelligenz verstehen, S. 472.

¹³⁴ Vgl. *Reese*, BB 2024, 1515, 1517.

¹³⁵ Vgl. *Kreutzer*, Künstliche Intelligenz verstehen, S. 472 f.

¹³⁶ Vgl. *Kreutzer*, Künstliche Intelligenz verstehen, S. 472 f.; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 116.

Hierbei sollte sowohl auf den für KI verantwortlichen Bereich als auch – falls vorhanden – auf den KI-Beauftragten eingegangen werden. Neben den Hauptverantwortlichen werden auch die Rollen der Risiko- und Kontrollfunktionen im Zusammenhang mit KI erläutert sowie die Aufgaben jedes einzelnen Mitarbeitenden des Unternehmens aufgegriffen. Damit ein einheitliches Verständnis geschaffen werden kann, empfiehlt es sich zudem, die wesentlichen Anforderungen der KI-VO, wie z.B. die Risikoklassifizierungen, aufzugreifen und darzulegen.¹³⁷

Damit die für KI verantwortlichen Einheiten die Erfüllung der regulatorischen sowie internen Vorgaben sicherstellen können, finden sich in der Richtlinie auch Ausführungen hinsichtlich des KI-Governance Prozesses. Diese Ausführungen umfassen beispielsweise den Melde-, Überprüfungs- und Betreuungsprozess für KI-Anwendungsfälle. Aber auch datenschutzrechtliche Fragen sowie Compliance-Anforderungen sollten in diesem Rahmen Berücksichtigung finden.¹³⁸

Essenziell ist zudem, dass das Unternehmen eine umfassende KI-Strategie entwickelt und diese für alle Mitarbeitenden zugänglich in der KI-Richtlinie dokumentiert. Sowohl für die Entwicklung der Richtlinie als auch insbesondere der KI-Strategie sind alle relevanten Stakeholder im Unternehmen abzuholen und einzubinden. Im Rahmen der KI-Strategie sollte sich das Unternehmen hinsichtlich der Kernfragen „Wie definieren wir im Unternehmen KI?“, „Wofür setzen wir KI ein?“, „Welche KI setzen wir ein?“ und „Welche Vision verfolgen wir mit dem Einsatz von KI?“ positionieren. Diese Positionierung dient als Orientierung und schafft für Mitarbeitende Transparenz hinsichtlich der Unternehmensziele.¹³⁹

Mitarbeitende werden mit Hilfe dieser Richtlinie in ihrer täglichen Arbeit unterstützt, indem sie eine klare Vorgabe bietet und wertvolle Hinweise von den internen KI-Experten bereitstellt. Auf diese Weise kann ein regelkonformes Verhalten des Unternehmens sichergestellt werden.¹⁴⁰

3.2.4.2 Regulatorische Überwachungsmaßnahmen

Neben der in der KI-Richtlinie aufgeführten Melde- und Überwachungsstrukturen sollte es ebenfalls einen klar definierten Prozess zur regelmäßigen Überwachung und Überprüfung sowohl der unternehmensinternen KI-Initiativen als auch der Einhaltung interner Vorgaben, insbesondere der KI-Richtlinie, geben. Auch die

¹³⁷ Vgl. *Heidrich Rechtsanwälte*, KI Richtlinie, o.S.

¹³⁸ Vgl. *Kreutzer*, Künstliche Intelligenz verstehen, S. 472 f.; *Reese*, BB 2024, 1515, 1519; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 116.

¹³⁹ Vgl. *Protschky et al.*, WuM 2024, o.S.; *Reese*, BB 2024, 1515, 1517.

¹⁴⁰ Vgl. *IBM*, Was ist KI-Governance? o.S.; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 116.

Effektivität der KI-Governance muss regelmäßig geprüft werden. Wie bereits zuvor in dem Kapitel der Rollen und Verantwortlichkeiten dargelegt, erweist es sich als sinnvoll, die Hauptverantwortlichkeit der KI-Themen in einen Bereich der ersten Verteidigungslinie zu legen und so die wirksame und unabhängige Kontrollfunktion durch die zweite Verteidigungslinie sicherzustellen.¹⁴¹

3.2.4.3 Durchführung Sensibilisierungs- und Schulungsmaßnahmen

Aus den beiden vorherigen Unterkapiteln geht sowohl bei der Festlegung der Verantwortlichkeiten als auch aus der Rahmen-Betriebsvereinbarung hervor, dass es für ein Unternehmen unabdingbar ist, die Mitarbeitenden hinsichtlich der Nutzung von KI hinreichend zu sensibilisieren.¹⁴² Die KI-VO unterstreicht die Bedeutung dieses Erfordernisses, indem sie Art. 4 KI-VO mit der kürzesten Umsetzungsfrist versieht (siehe B I 2 c).

Art. 3 Nr. 56 KI-VO definiert den Begriff der KI-Kompetenz als

*„Fähigkeit, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chance und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden“.*¹⁴³

Die Verordnung verpflichtet Unternehmen dazu, geeignete Maßnahmen zu ergreifen, damit insbesondere die für KI verantwortlichen Funktionen, aber auch alle anderen Mitarbeitenden über hinreichend Fachkenntnisse im Bereich KI verfügen. Dabei richtet sich die Einstufung des „ausreichende[n] Maß an KI-Kompetenz“¹⁴⁴ nach den bisherigen Kenntnissen der Mitarbeitenden sowie der beruflichen Rolle innerhalb des Unternehmens.¹⁴⁵

Neben der Schaffung eines Rechtsrahmens ist es wichtig, dass Unternehmen eine Kultur der KI-Governance etablieren. Dies erfordert, dass bei allen Mitarbeitenden ein Bewusstsein für den verantwortungsvollen Umgang mit KI-Systemen geschaffen wird und die internen Strukturen eine offene Kommunikation zwi-

¹⁴¹ Vgl. Kreutzer, Künstliche Intelligenz verstehen, S. 473.

¹⁴² Vgl. Klos/Taylan, CCZ 2024, 205, 211; Ulbricht et al., Praxishandbuch KI und Recht, S. 115.

¹⁴³ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 49.

¹⁴⁴ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 51.

¹⁴⁵ Vgl. Klos/Taylan, CCZ 2024, 205, 211.

schen allen Stakeholdern und Schlüsselfunktionen im Unternehmen fördern. Insbesondere für Mitarbeitende aus der IT, welche bereits über technisches Fachwissen verfügen, bieten sich Schulungen im Hinblick auf regulatorische Aspekte an. Es ist essenziell, dass die Mitarbeitenden neben den rein technischen Fähigkeiten auch mit den Richtlinien und Verfahren in ihrem Unternehmen vertraut sind. Hierfür eignen sich sowohl Schulungen als auch umfassende Schulungsprogramme.¹⁴⁶ Schulungen können zum einen in Präsenz stattfinden, aber auch in einem Online-Format durchgeführt werden. Für Mitarbeitende, welche sich im Rahmen ihrer beruflichen Tätigkeit primär auf den Einsatz von KI-Systemen konzentrieren, kann die Teilnahme an speziellen Schulungsprogrammen sinnvoll sein. Diese Programme können intern organisiert oder durch externe Seminare ergänzt werden. Besonders zertifizierte Lehrgänge gewährleisten, dass die Mitarbeitenden über ein standardisiertes Kompetenzniveau verfügen. Sie verleihen dem Unternehmen die Möglichkeit, die Qualifikation der Mitarbeitenden durch Zertifikate gegenüber externen Stellen nachzuweisen. Wichtig ist, dass die Fortbildungsprogramme regelmäßig durchgeführt werden und die Mitarbeitenden kontinuierlich auf dem aktuellen Stand der technologischen und rechtlichen Entwicklungen gehalten werden.¹⁴⁷

Insbesondere für Abteilungen, die sich vornehmlich mit KI-Systemen beschäftigen, ist es sinnvoll, sogenannte Multiplikatoren einzusetzen. Diese Experten können ihr Wissen und die Strategie in Bezug auf den Einsatz von KI im Unternehmen verbreiten.¹⁴⁸ Um die Effektivität der Arbeit weiter zu maximieren, empfiehlt sich zudem eine teamübergreifende Einbindung der Multiplikatoren.¹⁴⁹

Neben der Vermittlung von Fachwissen im Bereich KI besteht für Unternehmen auch die Möglichkeit, in Vorbereitung auf den Einsatz bestimmter KI-Systeme alle Mitarbeitenden übergreifend zu schulen. Diese Art der unternehmensspezifischen Weiterbildung gewährleistet eine umfassende Vorbereitung auf den bevorstehenden Einsatz von KI-Systemen.

Die Entwicklung von KI-Kompetenz ist nicht ausschließlich als eine unternehmensinterne Aufgabe anzusehen, sondern vielmehr als ein gesamtgesellschaftlicher Auftrag. Nur wenn Unternehmen, Bildungseinrichtungen, politische Ent-

¹⁴⁶ Vgl. *Kreutzer*, Künstliche Intelligenz verstehen, S. 473; Martini/Wendehorst/*Wendehorst*, Art. 4 Rn. 14; *Reese*, BB 2024, 1515, 1518.

¹⁴⁷ Vgl. Martini/Wendehorst/*Wendehorst*, Art. 4 Rn. 13 ff.

¹⁴⁸ Vgl. *Kreutzer*, Künstliche Intelligenz verstehen, S. 473.

¹⁴⁹ Vgl. Martini/Wendehorst/*Wendehorst*, Art. 4 Rn. 16 f.; *Reese*, BB 2024, 1515, 1517.

scheidungsträger und die Gesellschaft zusammenarbeiten, kann eine umfassende und nachhaltige Förderung der KI-Kompetenz erreicht werden und die Herausforderungen, die der Einsatz von KI mit sich bringt, bewältigt werden.¹⁵⁰

Insbesondere für kleinere Unternehmen sind nicht zwingend umfassende Schulungsprogramme erforderlich – auch KI-Richtlinien oder interne Leitlinien stellen geeignete Kompetenzvermittlungsmaßnahmen dar.¹⁵¹

3.3 Umsetzungsmaßnahmen

Neben der Vorabprüfung und der Etablierung eines Governance-Rahmens ist die Operationalisierung der Anforderungen aus der KI-VO von entscheidender Bedeutung. Nur durch eine effektive Umsetzung der Anforderungen kann sichergestellt werden, dass die rechtliche Konformität bei der Nutzung von KI hinreichend gewahrt wird.

Für die Unternehmen besteht die wesentliche Herausforderung insbesondere darin, die abstrakt formulierten Vorgaben der KI-VO und die aus ihr resultierenden Anforderungen individuell auf das eigene Unternehmen zu übertragen und effizient in den Alltag zu integrieren.¹⁵²

3.3.1 Erstellung KI-Verzeichnis

Unternehmen stehen vor der Herausforderung, die Vorgaben aus Richtlinien, Verordnungen und Standards in konkrete Maßnahmen zu übertragen. Damit dies gelingt, empfiehlt es sich, zunächst eine Bestandsaufnahme aller im Unternehmen eingesetzten Systeme sowie bevorstehender Initiativen in einem Verzeichnis durchzuführen. Im Anschluss ist zu prüfen, ob diese Systeme als KI-Systeme im Sinne der KI-VO zu klassifizieren sind.¹⁵³

Unternehmen steht dabei frei, das KI-Verzeichnis in Form einer einfachen Excel-Datei zu erstellen oder auf ein hierfür geeignetes System zurückzugreifen. Beide Ansätze erlauben im weiteren Verlauf eine Verknüpfung mit zusätzlichen Informationen, wodurch die Verwaltung und Aktualisierung des Verzeichnisses erleichtert wird.

¹⁵⁰ Vgl. Martini/Wendehorst/Wendehorst, Art. 4 Rn. 22 f.

¹⁵¹ Vgl. Martini/Wendehorst/Wendehorst, Art. 4 Rn. 12.

¹⁵² Vgl. Spitznagel, Vertrauenswürdige KI, 2024, o.S.

¹⁵³ Vgl. Klos/Taylan, CCZ 2024, 205, 210; Spitznagel, Vertrauenswürdige KI, 2024, o.S.

Zu der Bestandsaufnahme zählt neben der Zusammenstellung aller Systeme auch die Identifikation relevanter sowie einschlägiger Gesetze. Dies beinhaltet vornehmlich die KI-VO, schließt jedoch auch andere, bereits bestehende Gesetze ein (siehe B I 3).¹⁵⁴

3.3.2 Identifizierung Rollen und System-Verantwortliche

Auch in Bezug auf die einzelnen KI-Systeme ist es erforderlich, dass die Rollen und Verantwortlichkeiten eindeutig definiert sind. Im Anschluss an die Identifikation des Bestands an vorhandenen KI-Systemen sowie geplanter KI-Initiativen, muss für jedes System eine verantwortliche Person im Unternehmen bestimmt werden. Diese fungiert für alle künftigen Anliegen als zentrale Kontaktperson und trägt die Verantwortung für etwaige Anpassungen sowie potenzielle Risiken.

Für jedes KI-System wird im nächsten Schritt individuell bewertet, welche spezifische Rolle das Unternehmen im Sinne der KI-VO einnimmt. Die in Teil B dieser Arbeit bereits dargestellten Adressaten bilden die Grundlage der Einordnung. Dabei ist hervorzuheben, dass die Rolle als Adressat für jedes KI-System variieren kann. Dies führt dazu, dass unterschiedliche Pflichten zu erfüllen sind. Aus diesem Grund ist eine Prüfung der Adressateneigenschaft für jedes einzelne KI-System unverzichtbar und sollte vor der weiterführenden Analyse der Anforderungen erfolgen.¹⁵⁵

3.3.2.1 Anbieter

Da ein Großteil der Pflichten der KI-VO die Anbieter von KI-Systemen betreffen, kommt der Definition dieses Begriffs eine zentrale Bedeutung zu.¹⁵⁶

Art. 3 Nr. 3 KI-VO definiert den Begriff Anbieter als „eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle“¹⁵⁷, die KI-Systeme oder GPAI-Modelle entwickelt und diese unter eigenem Namen in den Verkehr bringt oder in Betrieb nimmt.¹⁵⁸

¹⁵⁴ Vgl. *Spitznagel*, Vertrauenswürdige KI, 2024, o.S.

¹⁵⁵ Vgl. *Herbst/Panic*, KI-Recht praktisch erklärt, S. 16; *Klos/Taylan*, CCZ 2024, 205, 210.

¹⁵⁶ Vgl. *Martini/Wendehorst/Wendehorst*, Art. 3 Rn. 63.

¹⁵⁷ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 46; vgl. *Ammann/Pohle*, CB 2024, 137, 138.

¹⁵⁸ Vgl. *Bierekoven*, ITRB 2024, 264, 267; *Ebers/Streitbürger*, RDi 2024, 393, 398; *Martini/Wendehorst/Wendehorst*, Art. 3 Rn. 64; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 165.

Art. 3 KI-VO führt diese Begrifflichkeiten weiter aus, wobei unter dem Inverkehrbringen das erstmalige Bereitstellen auf dem Unionsmarkt (Art. 3 Nr. 9 KI-VO) subsumiert wird. Dies impliziert die Abgabe eines KI-Systems oder GPAI-Modells im Rahmen einer Geschäftstätigkeit mit dem Ziel des Vertriebs oder der Verwendung auf dem Unionsmarkt. Gemäß Art. 3 Nr. 10 KI-VO ist dabei unerheblich, ob das Inverkehrbringen oder die Inbetriebnahme entgeltlich oder unentgeltlich erfolgt.¹⁵⁹ Dem Begriff des Inverkehrbringens kommt im Rahmen der KI-VO eine entscheidende Bedeutung zu, da er sowohl für den Anwendungsbereich der Verordnung als auch weitere wichtige Definitionen eine wesentliche Grundlage bildet.¹⁶⁰

Als Inbetriebnahme klassifiziert der Gesetzgeber die Bereitstellung zum Erstgebrauch. Diese kann sowohl an den Betreiber oder zum Eigengebrauch erfolgen (Art. 3 Nr. 11 KI-VO). Aus den Definitionen in Art. 3 Nr. 3-4 KI-VO geht hervor, dass der Gesetzgeber unter der Inbetriebnahme einen „Akt der Bereitstellung“¹⁶¹ versteht, sodass die Nutzung eines KI-Systems durch den Betreiber nicht unter diesen Begriff fällt.¹⁶² Der Begriff der Inbetriebnahme wird in den Bestimmungen der Verordnung häufig mit dem des Inverkehrbringens zusammen verwendet.¹⁶³ Betrachtet man die Definitionen der Verordnung, fällt auf, dass die Inbetriebnahme – im Gegenteil zum Inverkehrbringen – keinen Bezug zu einer Geschäftstätigkeit herstellt. Während der Begriff des Anbieters in Teilen an die des Herstellers gemäß der ProdHaftRL angelehnt ist, weicht Art. 4 Nr. 9 ProdHaftRL von der KI-VO insofern ab, als das der Artikel verlangt, dass auch die Inbetriebnahme im Rahmen einer Geschäftstätigkeit erfolgen muss. Es kann jedoch vermutet werden, dass auch im Rahmen der KI-VO vom Gesetzgeber eine Gleichbehandlung hinsichtlich der Geschäftstätigkeit angestrebt wird.¹⁶⁴

Ein weiteres Element der Definition besteht darin, dass der Anbieter das Inverkehrbringen in eigenem Namen oder mit seiner Handelsmarke vornimmt. Hierdurch wird die handelnde Person ohne weitere Erfordernisse als Anbieter erkennbar.¹⁶⁵ Darüber hinaus bleibt unklar, ob das Merkmal „unter eigenem Namen oder mit eigener Handelsmarke“ ausschließlich für die Variante des Inverkehrbringens

¹⁵⁹ Vgl. *Bitkom*, Umsetzungsleitfaden zur KI-Verordnung, 2024, S. 52 f.; *Ebers/Streitböcker*, RDi 2024, 393, 398; *Martini/Wendehorst/Wendehorst*, Art. 3, Rn. 67 f.

¹⁶⁰ Vgl. *Martini/Wendehorst/Wendehorst*, Art. 3 Rn. 108.

¹⁶¹ *Martini/Wendehorst/Wendehorst*, Art. 3 Rn. 133.

¹⁶² Vgl. *Herbst/Panic*, KI-Recht praktisch erklärt, S. 17; *Martini/Wendehorst/Wendehorst*, Art. 3 Rn. 133.

¹⁶³ Vgl. *Martini/Wendehorst/Wendehorst*, Art. 3 Rn. 131; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 165.

¹⁶⁴ Vgl. *Martini/Wendehorst/Wendehorst*, Art. 3 Rn. 134.

¹⁶⁵ Vgl. *Martini/Wendehorst/Wendehorst*, Art. 3 Rn. 64; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 165.

gilt oder ob dies auch auf die Inbetriebnahme Anwendung findet. Auch wenn man zunächst davon ausgehen kann, dass das Merkmal beide Varianten umfasst, so werden bei der Inbetriebnahme – insbesondere im Falle des Eigengebrauchs – doch geringere Anforderungen an die Sichtbarkeit gestellt. Die KI-VO selbst schafft in diesem Punkt keine abschließende Klarheit, sodass in Einzelfällen auf das Verständnis des „Herstellers“ in bereits bestehenden Rechtsakten zurückgegriffen werden muss.¹⁶⁶

3.3.2.2 Betreiber

Neben der Definition des Anbieters ist auch der Begriff des Betreibers in der KI-VO von zentraler Bedeutung. Gemäß Art. 3 Nr. 4 KI-VO wird der Betreiber als „eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet“¹⁶⁷ definiert. Eine Ausnahme bildet gemäß Art. 2 Abs. 10 KI-VO die Nutzung eines KI-Systems im Rahmen einer rein privaten Tätigkeit. Als Betreiber ist somit in erster Linie diejenige Person zu qualifizieren, die ein KI-System eigenverantwortlich zu geschäftlichen Zwecken nutzt.¹⁶⁸

In der Praxis gilt zudem, dass, wenn ein KI-System von einem Mitarbeitenden eines Unternehmens verwendet wird, das Unternehmen selbst als Betreiber zu klassifizieren ist und nicht der einzelne Mitarbeitende. Dies lässt sich auch aus dem Wortlaut der Verordnung „eigener Verantwortung“¹⁶⁹ schließen.¹⁷⁰ Der Begriff des Betreibers gilt, ebenso wie der des Anbieters, gleichermaßen als Konkretisierung des Anwendungsbereiches sowie als Bezugspunkt einiger Pflichten. In diesem Zusammenhang sind insbesondere Art. 26, 27, 50 Abs. 3-4 und 71 Abs. 3 KI-VO von Relevanz, die die Pflichten des Betreibers regeln und im weiteren Verlauf der Arbeit detaillierter analysiert werden.¹⁷¹

Sowohl die Definition des Anbieters als auch des Betreibers sind nach der KI-VO weit gefasst. Es fällt jedoch auf, dass der Gesetzgeber lediglich in Art. 2 Abs. 1 lit. a KI-VO und in Bezug auf das Inverkehrbringen eine Unterscheidung zwischen

¹⁶⁶ Vgl. Martini/Wendehorst/Wendehorst, Art. 3 Rn. 64 m.w.N.

¹⁶⁷ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 47; Herbst/Panic, KI-Recht praktisch erklärt, S. 26.

¹⁶⁸ Vgl. Ammann/Pohle, CB 2024, 137, 139; Ulbricht et al., Praxishandbuch KI und Recht, S. 169.

¹⁶⁹ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 46.

¹⁷⁰ Vgl. Bierekoven, ITRB 2024, 264, 267 f.; Ebers/Streitböcker, RDt 2024, 393, 399; Ulbricht et al., Praxishandbuch KI und Recht, S. 166.

¹⁷¹ Vgl. Martini/Wendehorst/Wendehorst, Art. 3 Rn. 79.

normalen KI-Systemen und GPAI-Modellen trifft, während die Definition des Betreibers diese Differenzierung nicht umfasst. Auf den ersten Blick könnte allein der Wortlaut der Verordnung vermuten lassen, dass die KI-VO nur dann Anwendung findet, wenn GPAI-Anbieter ein GPAI-Modell in den Verkehr bringen, während die Verwendung des Outputs eines solchen Modells nicht erfasst wäre. Diese auf den ersten Blick unklare Formulierung erweist sich jedoch als insoweit stimmig, als dass KI-Modelle bei ihrer Inbetriebnahme zu KI-Systemen werden und somit automatisch von der Definition umfasst sind.¹⁷²

3.3.2.3 Sonstige Akteure

Art. 3 Nr. 6 KI-VO definiert auch den Einführer als „eine in der Union ansässige oder niedergelassene natürliche oder juristische Person“¹⁷³, die ein KI-System, welches den Namen oder die Handelsmarke einer natürlichen oder juristischen Person im Drittland trägt, in den Verkehr bringt. Dem Einführer obliegt somit die Aufgabe, KI-Systeme von Anbietern, die außerhalb des Unionsgebietes niedergelassen sind, zu importieren und durch das Inverkehrbringen im Unionsgebiet eine höhere Verantwortung zu übernehmen. Die hieraus resultierenden erweiterten Pflichten sind in Art. 23 KI-VO beschrieben. Die Inbetriebnahme obliegt allein dem Anbieter, sodass dies nicht durch den Einführer erfolgen kann.¹⁷⁴

Keine weiteren Ausführungen trifft der Gesetzgeber hinsichtlich des Erfordernisses, dass Einführer in der Union ansässig oder niedergelassen sein müssen. Während Stimmen in der Literatur zur Stärkung der Rechtssicherheit eine Konkretisierung der Begriffe wünschen, interpretieren andere Stimmen diese Formulierung als einen Fehler.¹⁷⁵ Aufgrund der Identifizierung des Fehlers wurde dieses Erfordernis in der neuen ProdHaftRL von 2024 nicht übernommen. Der Tatsache geschuldet, dass die KI-VO die Einschränkung auch weiterhin enthält, werden alle Akteure, welche nicht in der Union ansässig sind, nach der KI-VO als Händler eingestuft.¹⁷⁶ Diese definiert die Verordnung in Art. 3 Nr. 7 KI-VO als „eine natür-

¹⁷² Vgl. Martini/Wendehorst/Wendehorst, Art. 3 Rn. 82; Ulbricht et al., Praxishandbuch KI und Recht, S. 166.

¹⁷³ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 46.

¹⁷⁴ Vgl. Ammann/Pohle, CB 2024, 137, 139; Martini/Wendehorst/Wendehorst, Art. 3 Rn. 99.

¹⁷⁵ Vgl. Bitkom, Umsetzungsleitfaden zur KI-Verordnung, 2024, S. 45; Martini/Wendehorst/Wendehorst, Art. 3 Rn. 100.

¹⁷⁶ Vgl. Martini/Wendehorst/Wendehorst, Art. 3 Rn. 100.

liche oder juristische Person in der Lieferkette, die ein KI-System auf dem Unionsmarkt bereitstellt“¹⁷⁷, wobei Anbieter und Einführer ausdrücklich ausgenommen sind.¹⁷⁸ In Art. 24 KI-VO finden sich die für Händler geltenden Pflichten.

Auch von der KI-VO umfasst sind gemäß Art. 2 Abs. 1 lit. e KI-VO Produkthersteller sowie gemäß Art. 2 Abs. 1 lit. f KI-VO Bevollmächtigte von Anbietern, die nicht in der Union niedergelassen sind. Beide Akteure werden in Art. 3 Nr. 8 KI-VO als Adressaten der Verordnung bezeichnet. Als Produkthersteller gilt, wer KI-Systeme in Verbindung mit einem Produkt in den Verkehr bringt oder in Betrieb nimmt. Das Inverkehrbringen oder die Inbetriebnahme erfolgt unter eigenem Namen oder der eigenen Handelsmarke (Art. 2 Abs. 1 lit. e KI-VO). Eigene Pflichten ergeben sich für Produkthersteller nicht, jedoch können diese gemäß Art. 25 Abs. 1 KI-VO – ähnlich der anderen Akteure – zu Anbietern von Hochrisiko-KI-Systemen werden.¹⁷⁹

Ein Bevollmächtigter wird gemäß Art. 3 Nr. 5 KI-VO als „eine in der Union ansässige oder niedergelassene natürliche oder juristische Person“¹⁸⁰ definiert, die von einem Anbieter eines KI-Systems oder GPAI-Modells schriftlich bevollmächtigt wurde, den aus der Verordnung resultierenden Pflichten im Namen des Anbieters nachzukommen. Besondere Relevanz erlangen die Bevollmächtigten als in der Union niedergelassene Ansprechpartner, da Erwgr. 82 S. 1 KI-VO voraussetzt, dass unter allen Umständen ein in der Union niedergelassener Ansprechpartner zur Gewährleistung der Konformität benannt werden muss. Die Eigenschaft eines Bevollmächtigten wird somit entgegen den anderen Akteuren nicht durch die KI-VO begründet, sondern durch einen Akt der Bevollmächtigung des Anbieters sowie der Zustimmung des Bevollmächtigten. Eigenständige Pflichten ergeben sich für den Bevollmächtigten nicht, da dieser ausschließlich die Aufgaben des Anbieters wahrnimmt.¹⁸¹

3.3.3 Einteilung Risikoklassen

Der Gesetzgeber verfolgt im Rahmen der KI-VO einen risikobasierten Ansatz, der eine Einteilung von KI-Systemen in verschiedene Kategorien vorsieht.¹⁸² Die Unterscheidung der Risikokategorien bildet bei der Einhaltung der regulatori-

¹⁷⁷ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 46.

¹⁷⁸ Vgl. *Ammann/Pohle*, CB 2024, 137, 139.

¹⁷⁹ Vgl. *Bitkom*, Umsetzungsleitfaden zur KI-Verordnung, 2024, S. 49; *Herbst/Panic*, KI-Recht praktisch erklärt, S. 26.

¹⁸⁰ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 46.

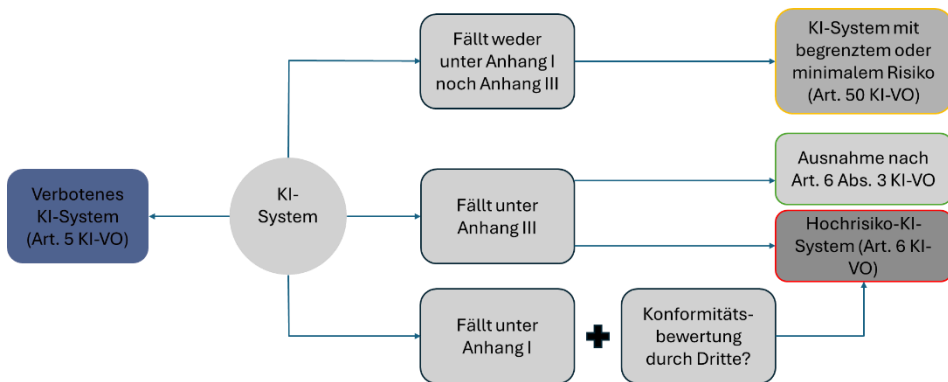
¹⁸¹ Vgl. *Bitkom*, Umsetzungsleitfaden zur KI-Verordnung, 2024, S. 50.

¹⁸² Vgl. *Bronner*, KIR 2024, 55, 57.

schen Anforderungen eine zentrale Grundlage. Damit Unternehmen, die im Rahmen der Bestandsaufnahme identifizierten KI-Systeme den entsprechenden Risikokategorien zuordnen können, empfiehlt sich die Anwendung eines einheitlichen Schemas. Mit Hilfe dessen wird nicht nur die konsistente Bewertung sichergestellt, sondern auch die Transparenz der Entscheidungen. Um eine bestmögliche Transparenz gegenüber allen Stakeholdern zu gewährleisten – sowohl innerhalb des Unternehmens als auch gegenüber externen Stakeholdern wie Regulierungsbehörden – bietet es sich an, die Zuordnung der eigenen Rolle, die Risikoklassifizierung sowie die hieraus resultierenden Pflichten im KI-Verzeichnis weiterzuführen. Das Verzeichnis sollte eine umfassende Dokumentation enthalten, die die Anforderungen an das Unternehmen klar nachvollziehbar macht.¹⁸³ Ein transparentes Vorgehen dient nicht nur der internen Governance, sondern fördert auch das Vertrauen der Stakeholder im Umgang mit KI-Risiken.¹⁸⁴

Nachfolgendes Schema soll als Beispiel dienen und bietet die Grundlage für die weiteren Ausführungen in diesem Kapitel.

Abbildung 2: Prüfungsschema Risikokategorien



Quelle: in Anlehnung an Klos/Taylan, CCZ 2024, 205, 210.

Anhand Abbildung 2 wird ersichtlich, dass die KI-VO die KI-Systeme in unterschiedliche Risikokategorien einteilt: unannehmbares Risiko (verbotene KI-Systeme), hohes Risiko, begrenztes Risiko und minimales Risiko. Handelt es sich bei dem vorliegenden System um kein verbotenes KI-System im Sinne des Art. 5 KI-VO besteht die Möglichkeit, dass das System den Regelungen aus Anhang

¹⁸³ Vgl. Klos/Taylan, CCZ 2024, 205, 210 f.

¹⁸⁴ Vgl. Reese, BB 2024, 1515; Schackmann/Ziegler, Praxisorientiertes Managementwissen, S. 277.

I oder III unterliegt. In diesem Fall handelt es sich – unter Berücksichtigung bestimmter Voraussetzungen wie den Ausnahmen nach Art. 6 Abs. 3 KI-VO sowie einer Konformitätsbewertung – um ein Hochrisiko-KI-System im Sinne von Art. 6 KI-VO. Alle anderen Fälle stellen KI-Systeme mit einem begrenzten oder minimalen Risiko dar.

Nach der finalen Einordnung der Systeme verfügen Unternehmen über ein Verzeichnis, welches sämtliche KI-Systeme im Unternehmen zusammenfasst. Dieses Verzeichnis dokumentiert zudem die eigene Rolle als Akteur, die Risikoklassifizierung und schlussendlich gibt es Aufschluss über die hieraus resultierenden Pflichten.

Zum besseren Verständnis werden die beiden Schritte – Risikoklassifizierung und damit einhergehende Anforderungen – in den einzelnen Kategorien jeweils zusammen behandelt.

3.3.3.1 Unannehmbares Risiko

Sobald die in einem Unternehmen eingesetzten KI-Systeme in einem Verzeichnis zusammengefasst sind, empfiehlt es sich, zunächst zu prüfen, ob eines der Systeme unter die verbotenen Praktiken im Sinne der KI-VO fällt.

Der Gesetzgeber führt die verbotenen Praktiken entsprechend dem risikobasierten Ansatz in Kapitel II KI-VO aus. Das Kapitel umfasst jene KI-Praktiken, die ein unannehmbares Risiko darstellen, insbesondere in Bezug auf die Wahrung der Grundrechte. Diese Konsequenz ergibt sich nicht zuletzt aus dem in Art. 1 Abs. 1 KI-VO genannten Ziel, eine vertrauenswürdige KI zu fördern und ein hohes Schutzniveau, auch in Bezug auf die in der Charta festgehaltenen Grundrechte, aufzubauen.

Berücksichtigt werden sollte im Zusammenhang von Art. 5 KI-VO die Verwendung des Begriffs „Praktiken“. Anders als die Kapitel III bis V KI-VO, welche Hochrisiko-KI-Systeme, Arten weiterer KI-Systeme und GPAI-Modelle umfassen, sind die in Art. 5 Abs. 1 KI-VO aufgelisteten Praktiken nicht auf bestimmte Sektoren begrenzt. Ausnahme bildet der Umstand, dass die Formulierung selbst eine Begrenzung auf einen Sektor impliziert. Damit KI-Systeme nicht für Zwecke eingesetzt werden können, die nicht mit den europäischen Grundwerten vereinbar sind, adressiert Kapitel II KI-VO vornehmlich die auf KI-bezogenen Tätigkeiten. Hiervon umfasst sind das Inverkehrbringen, die Inbetriebnahme sowie die Verwendung von KI-Systemen zu einem bestimmten Zweck (siehe C III 2).¹⁸⁵

¹⁸⁵ Vgl. Martini/Wendehorst/Wendehorst, Art. 5 Rn. 2 f.

Als verbotene Praktiken legt die KI-VO folgende Fallgruppen fest.¹⁸⁶

- Unterschwellige Beeinflussung oder absichtlich manipulative oder täuschende Techniken
- Ausnutzen von in der KI-VO genannten menschlichen Schwächen
- Klassifizierung anhand von Verhaltens- oder Persönlichkeitsmerkmalen (Social Scoring)
- Kriminalitäts-Profilings¹⁸⁷
- Datenbanken zur Gesichtserkennung
- Ableiten von Emotionen am Arbeitsplatz und in Bildungseinrichtungen
- Biometrische Kategorisierung auf Basis persönlicher Merkmale
- Biometrische Echtzeit-Fernidentifizierungssysteme im öffentlichen Raum zur Strafverfolgung

Weitere Ausführungen zu den verbotenen KI-Praktiken und den verschiedenen Fallgruppen finden sich in Erwgr. 28-45 KI-VO. Diese dienen Unternehmen als Orientierungshilfe, um eine weitergehende Differenzierung der Kategorien vorzunehmen. Dabei ist zu beachten, dass die zuvor aufgeführten Fallkonstellationen nicht in allen Fällen vollständig verboten sind. Teilweise nennt die Verordnung lediglich Einschränkungen hinsichtlich der Fallgruppen oder stellt Voraussetzungen für den Einsatz auf. Ein Beispiel und gleichzeitig eine Sonderkonstellation stellt Art. 5 Abs. 1 UAbs. 1 lit. h KI-VO dar. Es handelt sich hierbei um die biometrische Echtzeit-Fernidentifizierung (Art. 3 Nr. 42 KI-VO). Unternehmen sollten hierbei besonders berücksichtigen, dass es sich nicht um ein uneingeschränktes Verbot handelt. Der Gesetzgeber führt zwar an, dass die Verwendung ebensolcher Systeme grundsätzlich untersagt ist, das Verbot jedoch nur gilt, insofern die unter Art. 5 Abs. 1 UAbs. 1 lit. h und Abs. 2-7 KI-VO genannten Voraussetzungen nicht eingehalten werden.¹⁸⁸

Die Ausführungen, die verbotenen Praktiken betreffend, sind somit seitens der Unternehmen sorgfältig zu analysieren. Möglich ist auch, dass die Kommission gemäß Art. 96 Abs. 1 lit. b KI-VO zukünftig Leitlinien zur weiteren Auslegung des

¹⁸⁶ Vgl. *Herbst/Panic*, KI-Recht praktisch erklärt, S. 20; Martini/Wendehorst/Wendehorst, Art. 5 Rn. 1 ff.; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 171.

¹⁸⁷ „Jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Personen zu analysieren oder vorherzusagen.“ Martini/Wendehorst/Wendehorst, Art. 3 Rn. 364.

¹⁸⁸ Vgl. Martini/Wendehorst/Wendehorst, Art. 5 Rn. 4.

Art. 5 KI-VO erlässt. Der Zeitpunkt und die konkrete Umsetzung sind bis jetzt jedoch noch nicht bekannt.¹⁸⁹

Sanktionsrechtlich zieht die Verwendung von verbotenen KI-Praktiken für die betroffenen Akteure gemäß Art. 99 KI-VO das höchste Strafmaß nach sich.¹⁹⁰

3.3.3.2 Begrenztes und minimales Risiko

Neben den verbotenen Praktiken existieren auch KI-Systeme mit einem begrenzten Risiko. Die Verordnung bündelt diese in Kapitel IV KI-VO. Art. 50 KI-VO ist der einzige Artikel dieses Kapitels und umfasst insbesondere KI-Systeme, die zur unmittelbaren Interaktion mit natürlichen Personen dienen. In den Anwendungsbereich fallen neben Chatbots zudem KI-Systeme (auch GPAI-Modelle), die „synthetische Audio-, Bild-, Video- oder Textinhalte ... erzeugen“¹⁹¹ sowie Systeme zur Emotionserkennung und/oder biometrischen Kategorisierung.¹⁹²

Zwar misst der Gesetzgeber diesen KI-Systemen ein geringeres Risiko als den verbotenen Praktiken oder den Hochrisiko-KI-Systemen zu, jedoch erachtet er die Einführung besonderer Transparenzpflichten aufgrund des bestehenden Schadenpotentials dennoch als erforderlich. Dies unterstreicht der Gesetzgeber in Erwgr. 132 KI-VO. Die Systeme kommen aufgrund ihrer Funktionen den menschlichen Fähigkeiten sehr nahe und bergen das Risiko der Manipulation bzw. Verwechslung.¹⁹³ Es ist daher erforderlich, dass die Interagierenden über die Tatsache, dass es sich um ein KI gesteuertes System handelt, informiert sind.

Für Anbieter sind die in Art. 50 Abs. 1 und 2 KI-VO und für Betreiber die in Art. 50 Abs. 3 und 4 KI-VO genannten Anforderungen einschlägig. Darüber hinaus stellt der Gesetzgeber für die KI-Systeme dieser Risikokategorie keine weiteren Regulierungsanforderungen.¹⁹⁴

Falls ein KI-System sowohl unter einen der Tatbestände von Art. 50 Abs. 1-4 KI-VO fällt als auch Merkmale eines Hochrisiko-KI-Systems gemäß den Bestimmungen in Kapitel III KI-VO aufweist, sieht Art. 50 Abs. 6 KI-VO vor, dass die Anforderungen aus beiden Regelungen parallel angewendet werden. Die aus den Anforderungen resultierenden Transparenzpflichten verfolgen jedoch unterschiedli-

¹⁸⁹ Vgl. Martini/Wendehorst/Wendehorst, Art. 5 Rn. 6.

¹⁹⁰ Vgl. Herbst/Panic, KI-Recht praktisch erklärt, S. 20; Martini/Wendehorst/Wendehorst, Art. 5 Rn. 7 f.

¹⁹¹ Martini/Wendehorst/Martini, Art. 50 Rn. 42.

¹⁹² Vgl. Klos/Taylan, CCZ 2024, 205, 209; Martini/Wendehorst/Martini, Art. 50 Rn. 42.

¹⁹³ Vgl. Klos/Taylan, CCZ 2024, 205, 209; Martini/Wendehorst/Martini, Art. 50 Rn. 1, 9.

¹⁹⁴ Vgl. Martini/Wendehorst/Martini, Art. 50 Rn. 9.

che Ziele: Während Art. 50 KI-VO darauf abzielt, den betroffenen natürlichen Personen die Möglichkeit zu geben, KI-Systeme und deren Ergebnisse erkennen und einordnen zu können, verfolgt Art. 13 KI-VO das Ziel, dass sowohl Anbieter als auch Betreiber sicherstellen, dass der Einsatz ihrer KI-Systeme rechtskonform erfolgt. Aufgrund der unterschiedlichen Intention ist es unabdingbar, dass die mit dem Einsatz verbundenen Inhalte und Prüfungsschritte nach außen hinreichend nachvollziehbar sind.¹⁹⁵

Bei der Einstufung von KI-Systemen in die Kategorie des minimalen Risikos handelt es sich um keine gesetzliche Bezeichnung aus der KI-VO. Der Begriff hat sich jedoch mittlerweile etabliert und wird auch von der EU-Kommission in ihren „Frage und Antwort“ Veröffentlichungen verwendet. Von dieser Kategorie sind alle Systeme umfasst, die keiner der anderen Risikokategorien zugeordnet werden können. Hieraus lässt sich ableiten, dass diese Systeme zumindest aus rechtlicher Sicht nicht in den Anwendungsbereich der KI-VO fallen und sich somit keine weiteren Pflichten für ebendiese Systeme ergeben.¹⁹⁶

Art. 95 KI-VO sieht für beide Kategorien (begrenztes und minimales Risiko) die Möglichkeit vor, freiwillig Verhaltenskodizes zu erstellen.

Bevollmächtigte, Einführer und Händler treffen nach Art. 50 KI-VO für diese Risikokategorien keine Verpflichtungen.

3.3.3.3 Hohes Risiko

Lässt sich ein KI-System als Hochrisiko-KI-System klassifizieren, ergeben sich aus der KI-VO umfangreiche Pflichten.¹⁹⁷ Der Gesetzgeber stuft ein KI-System als hochriskant ein, wenn von diesem ein erhebliches Risiko für die Unionswerte, die Sicherheit und die Grundrechte ausgeht.¹⁹⁸

Damit ein KI-System als hochriskant gilt, müssen Unternehmen gemäß Art. 6 Abs. 1 KI-VO prüfen, ob zwei Voraussetzungen kumulativ vorliegen. Zum einen muss das KI-System als Sicherheitsbauteil eines Produktes verwendet werden. Das Produkt, in welchem das KI-System verwendet wird, muss dabei unter die in Anhang I KI-VO aufgelisteten Harmonisierungsvorschriften der Union fallen. Darüber hinaus ist es auch möglich, dass es sich bei dem KI-System selbst um solch ein Produkt handelt. Bei den Harmonisierungsvorschriften handelt es sich um

¹⁹⁵ Vgl. Martini/Wendehorst/Martini, Art. 50 Rn. 123.

¹⁹⁶ Vgl. Klos/Taylan, CCZ 2024, 205, 209.

¹⁹⁷ Vgl. Klos/Taylan, CCZ 2024, 205, 208.

¹⁹⁸ Siehe weiterführend Erwgr. 46-48 KI-VO; Ulbricht et al., Praxishandbuch KI und Recht, S. 172.

Regeln, die für alle Unternehmen und Organisationen einschlägig sind, die KI-Systeme in der EU anbieten oder anwenden – sogenannte technische Standards. Durch die Aufnahme der Harmonisierungsvorschriften in die KI-VO soll in der EU eine einheitliche Handhabung hinsichtlich KI-Systemen sichergestellt werden.¹⁹⁹ Des Weiteren muss gemäß Art. 6 Abs. 1 lit. b KI-VO eine Bewertung dahingehend erfolgen, ob das Produkt die festgelegten Anforderungen und Normen erfüllt (Konformitätsbewertung).

Art. 6 Abs. 2 KI-VO verweist auf Anhang III KI-VO, der neben Art. 6 Abs. 1 KI-VO weitere Systeme auflistet, die als hochriskant anzusehen sind. Für Unternehmen gilt es somit Art. 6 KI-VO sowohl in Verbindung mit Anhang I als auch Anhang III zu lesen und zu beachten, dass die Einstufung als hochriskant sowohl auf Produktebene als auch in Bezug auf spezifische Anwendungen erfolgen kann.

Wie Abbildung 2 verdeutlicht, gibt es einen Ausnahmetatbestand nach Art. 6 Abs. 3 KI-VO. Hiernach gilt ein KI-System nicht als hochriskant, sofern es keine Entscheidungen wesentlich beeinflusst und somit kein erhebliches Risiko für „die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt“.²⁰⁰ Sofern Unternehmen also Hochrisiko-KI-Systeme einsetzen, diese jedoch unter den Ausnahmetatbestand fallen, unterliegen diese nicht den Pflichten nach Art. 8 ff. KI-VO. Allerdings sind Unternehmen nach Art. 6 Abs. 4 KI-VO dazu angehalten, ihre Bewertung zu dokumentieren, das KI-System in der EU-Datenbank zu registrieren und auf Verlangen der Aufsichtsbehörde eine Bewertungsdokumentation vorlegen zu können.²⁰¹

Eine vollumfängliche Darstellung aller Pflichten für Hochrisiko-KI-Systeme würde den Umfang dieser Arbeit überschreiten, sodass nur die wesentlichen Aspekte weiter ausgeführt werden.

3.3.3.3.1 Konformitätsbewertung, Konformitätserklärung und CE-Kennzeichnung

Unternehmen, die in ihrem KI-Verzeichnis KI-Systeme identifizieren, bei welchen sie als Anbieter agieren, sind gemäß Art. 43, 47 und 48 KI-VO dazu verpflichtet,

¹⁹⁹ Vgl. *Herbst/Panic*, KI-Recht praktisch erklärt, S. 25; *Martini/Wendehorst/Rusche-meier*, Art. 6 Rn. 54 ff.; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 157.

²⁰⁰ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 54.

²⁰¹ Vgl. *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 176.

vor dem Inverkehrbringen oder der Inbetriebnahme ein Konformitätsbewertungsverfahren zu durchlaufen, eine EU-Konformitätserklärung auszustellen und eine CE-Kennzeichnung an das Hochrisiko-KI-System anzubringen.²⁰²

Die KI-VO unterscheidet bei der Durchführung einer Konformitätsbewertung zwischen zwei verschiedenen Verfahren. Im Falle eines Bewertungsverfahrens auf Grundlage einer internen Kontrolle ist der Anbieter dazu angehalten, zu überprüfen, ob den Anforderungen aus Art. 8-15 und Art. 17 KI-VO entsprochen wird und ob der Entwurfs- und Entwicklungsprozess sowie die Beobachtungen nach dem Inverkehrbringen mit der technischen Dokumentation übereinstimmen.²⁰³ Abbildung 2 lässt erkennen, dass das Konformitätsverfahren auch durch Dritte durchgeführt werden kann. In diesem Fall wird das Verfahren durch eine notifizierte Stelle vorgenommen und das Qualitätsmanagement (Art. 17 KI-VO) sowie die technische Dokumentation (Art. 11 KI-VO) durch ebendiese geprüft.²⁰⁴

Konnte das Unternehmen im Rahmen eines Konformitätsbewertungsverfahrens nachweisen, dass das Hochrisiko-KI-System den Anforderungen aus Art. 8-15 KI-VO hinreichend nachkommt, muss der Anbieter vor dem Inverkehrbringen bzw. der Inbetriebnahme eine elektronisch unterzeichnete EU-Konformitätserklärung nach Art. 16 lit. g KI-VO in Verbindung mit Art. 47 KI-VO ausstellen, die ebendies bestätigt.²⁰⁵

Wichtig ist für Anbieter von KI-Systemen Art. 47 KI-VO, aus welchem hervorgeht, dass die Konformitätsbewertung für die nationalen Behörden zehn Jahre verfügbar bleiben muss.²⁰⁶ Insgesamt gilt, dass das Konformitätsverfahren erneut durchgeführt werden muss, wenn sich das KI-System wesentlich verändert (Art. 43 Abs. 4 KI-VO). Als wesentlich wird das Hinzufügen von weiteren algorithmischen Verfahren angesehen und nicht die Erweiterung von Trainingsdaten.²⁰⁷ Die Erweiterung eines bestehenden KI-Systems mit Kfz-Versicherungsdaten um Haftpflichtdaten wird somit nicht als wesentliche Änderung angesehen.

²⁰² Vgl. *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 186.

²⁰³ Siehe weiterführend Anhang VI KI-VO.

²⁰⁴ Siehe weiterführend Anhang VII KI-VO.

²⁰⁵ Siehe weiterführend Anhang VI KI-VO.

²⁰⁶ Vgl. *Herbst/Panic*, KI-Recht praktisch erklärt, S. 27; Martini/Wendehorst/*Gerdemann*, Art. 47 Rn. 13.

²⁰⁷ Siehe weiterführend Martini/Wendehorst/*Gerdemann*, Art. 43 Rn. 58 ff.

Damit auch nach außen kenntlich wird, dass das Produkt den gesetzlichen Anforderungen entspricht, muss der Anbieter gemäß Art. 16 lit. h KI-VO in Verbindung mit Art. 48 KI-VO eine CE-Kennzeichnung anbringen. Auch aus ihr geht gleichermaßen die Konformität mit den Anforderungen der KI-VO hervor.²⁰⁸

3.3.3.2 Technische Dokumentation

Um das Konformitätsverfahren zu erleichtern und eine fundierte Grundlage zu schaffen, sind Anbieter gemäß Art. 11 KI-VO dazu verpflichtet, eine aussagekräftige technische Dokumentation zu erstellen. Die Inhalte dieser Dokumentation ergeben sich aus Art. 11 iVm. Anhang IV KI-VO.²⁰⁹

Die Dokumentation dient insbesondere den national zuständigen Behörden und den notifizierten Stellen, damit diese hinreichend die Erfüllung der Anforderungen aus Art. 8 ff. KI-VO nachvollziehen können.²¹⁰ Haben Anbieter den Verdacht, dass ein in Betrieb genommenes oder in den Verkehr gebrachtes Hochrisiko-KI-System nicht den festgelegten Anforderungen entspricht, ist Art. 20 KI-VO zu berücksichtigen. Gleiches gilt, sofern das System ein Risiko im Sinne des Art. 79 KI-VO birgt.

Falls Betreiber feststellen, dass die Verwendung des KI-Systems gemäß Betriebsanleitung dazu führen könnte, dass sich ein Risiko aus Art. 79 Abs. 1 KI-VO verwirklicht, sind auch sie nach Art. 26 Abs. 5 KI-VO verpflichtet, die entsprechenden Anbieter, Händler und die Marktüberwachungsbehörde zu informieren.

Unternehmen sollten der technischen Dokumentation besondere Aufmerksamkeit widmen, da diese als Nachweis für die Regelkonformität ihrer Systeme dient. Anbieter müssen die Dokumentation gemäß Art. 11 Abs. 1 KI-VO vor der Inbetriebnahme bzw. des Inverkehrbringens erstellen und kontinuierlich auf dem aktuellen Stand halten.

Erleichterte Anforderungen gelten für KMU und Start-ups. Diese dürfen nach Art. 11 Abs. 1 UAbs. 2 S. 3 KI-VO die technische Dokumentation in einer vereinfachten Form vorlegen. Hierzu erarbeitet die Kommission ein entsprechendes Formular, welches von den notifizierten Stellen akzeptiert werden muss. Im Sinne einer horizontalen Regulierung normiert Art. 11 Abs. 2 KI-VO, dass die techni-

²⁰⁸ Siehe weiterführend Erwgr. 129 S. 1 KI-VO; *Herbst/Panic*, KI-Recht praktisch erklärt, S. 27.

²⁰⁹ Vgl. *Herbst/Panic*, KI-Recht praktisch erklärt, S. 23; *Klos/Taylan*, CCZ 2024, 205, 208.

²¹⁰ Vgl. *Bitkom*, Umsetzungsleitfaden zur KI-Verordnung, 2024, S.96; *Herbst/Panic*, KI-Recht praktisch erklärt, S. 23; *Martini/Wendehorst/Braun Binder/Egli*, Art. 11 Rn. 4.

sche Dokumentation bei den Systemen, die bereits den Harmonisierungsvorschriften des EU-Produktsicherheitsrechts unterliegen (Anhang I KI-VO), zusammen erstellt wird.²¹¹

Aufmerksamkeit sollten Anbieter außerdem auf die Tatsache richten, dass die Kommission gemäß Art. 11 Abs. 5 KI-VO unter Berücksichtigung des technischen Fortschritts dazu befugt ist, Änderung an Anhang IV KI-VO und somit an den Anforderungen an die technische Dokumentation vorzunehmen.

Gemäß Art. 18 KI-VO sind Anbieter verpflichtet, die technische Dokumentation für einen Zeitraum von zehn Jahren nach dem Inverkehrbringen oder der Inbetriebnahme des KI-Systems aufzubewahren.

3.3.3.3 Aufbewahrungs- und Transparenzpflichten

Art. 18 Abs. 1 KI-VO spezifiziert neben der technischen Dokumentation auch die Aufbewahrungspflichten für Unterlagen zum Qualitätsmanagement (Art. 17 KI-VO), genehmigte Änderungen, Entscheidungen oder sonstige Dokumente der notifizierten Stelle und zur EU-Konformitätsbewertung (Art. 47 KI-VO).

Auch die von Hochrisiko-KI-Systemen erzeugten Protokolle (Art. 12 KI-VO) müssen gemäß Art. 19 Abs. 1 KI-VO aufbewahrt werden. Die Aufbewahrungsfrist muss dabei angemessen sein und beträgt mindestens sechs Monate. Diese Verpflichtung gilt auch für Betreiber gemäß Art. 26 Abs. 9 KI-VO.

Insbesondere Anbieter von Finanzunternehmen sollten die Bestimmungen aus Art. 18 Abs. 3, Art. 19 Abs. 2 und Art. 26 Abs. 6 KI-VO berücksichtigen.

Insgesamt empfiehlt es, sich die unternehmensinternen Aufbewahrungsfristen analog zu den in anderen Gesetzen festgelegten Fristen zu dokumentieren und für alle Mitarbeitenden zugänglich zu machen (z.B. in Form einer Richtlinie).

Zusätzlich verlangt der Gesetzgeber von Anbietern, dass sie ihre Hochrisiko-KI-Systeme hinreichend transparent konzipieren (Art. 13 Abs. 1 iVm. Erwgr. 72 KI-VO). In diesem Zusammenhang gilt es für Anbieter Art. 13 Abs. 2 KI-VO zu beachten. Dieser setzt die Bereitstellung von Betriebsanleitungen voraus. Die Anforderungen an den Inhalt dieser Anleitungen sind in der Verordnung klar definiert.

²¹¹ Vgl. *Bitkom*, Umsetzungsleitfaden zur KI-Verordnung, 2024, S. 99; Martini/Wendehorst/*Braun Binder/Egli*, Art. 11 Rn. 15 ff.; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 179.

Betreiber sind gemäß Art. 26 Abs. 1 KI-VO dazu angehalten technische und organisatorische Maßnahmen (TOMs) zu ergreifen, um sicherzustellen, dass die KI-Systeme in Übereinstimmung mit den bereitgestellten Betriebsanleitungen verwendet werden.

3.3.3.3.4 Folgenabschätzung

Art. 26 und 27 KI-VO normieren die Pflichten für Betreiber von Hochrisiko-KI-Systemen. Gemäß Art. 27 Abs. 1 KI-VO sind Betreiber verpflichtet, vor der Inbetriebnahme eines Hochrisiko-KI-Systems eine Grundrechts-Folgenabschätzung (GFA) durchzuführen. Diese dient der Abschätzung der potenziellen Auswirkungen der KI-Systeme auf die Grundrechte. Die spezifischen Anforderungen an den Inhalt der GFA werden in Art. 27 Abs. 1 KI-VO aufgeführt.

Eine zentrale Schnittstelle der KI-VO besteht zur DSGVO. Ein Beispiel hierfür ist die Verpflichtung, die GFA gemäß Art. 27 KI-VO in Verbindung mit der Datenschutz-Folgenabschätzung (DSFA) durchzuführen. Die Notwendigkeit einer DSFA ergibt sich aus Art. 26 Abs. 9 KI-VO. Dabei kann die GFA als Ergänzung zur DSFA betrachtet werden, wie in Art. 27 Abs. 4 KI-VO festgelegt.²¹²

Betreiber von Hochrisiko-KI-Systemen sollten die Entwicklungen hinsichtlich Art. 27 Abs. 5 KI-VO aufmerksam verfolgen. Gemäß dieser Vorschrift wird das Büro für KI einen Fragebogen erarbeiten, der Betreibern als Hilfsmittel zur Erfüllung ihrer Pflichten dient.²¹³

3.3.3.3.5 Risikomanagement

Um den mit dem Einsatz von KI-Systemen einhergehenden Risiken entgegenzuwirken und den Vorstand eines Unternehmens hinreichend abzusichern, stellt die Verordnung in Art. 9 KI-VO die Anforderung eines Risikomanagementsystems.²¹⁴

Die Verordnung selbst nimmt keine explizite Begriffsdefinition für das Risikomanagementsystem vor. Nach allgemeinem Verständnis werden von dem Risikomanagement jedoch alle Tätigkeiten, die der Identifikation, Bewertung und Bewältigung von Risiken dienen umfasst.²¹⁵ Dabei bezieht sich die Funktion des

²¹² Vgl. *Kindshofer*, ZD 2024, 673, 675; Martini/Wendehorst/*Eisenberger*, Art. 27 Rn. 57.

²¹³ Vgl. Martini/Wendehorst/*Eisenberger*, Art. 27 Rn. 59.

²¹⁴ Siehe weiterführend Erwgr. 65 KI-VO; vgl. *Klos/Taylan*, CCZ 2024, 205, 208; Martini/Wendehorst/*Braun Binder/Egli*, Art. 9 Rn. 1.

²¹⁵ Vgl. Martini/Wendehorst/*Braun Binder/Egli*, Art. 9 Rn. 15.

Risikomanagements in einem Unternehmen auf sämtliche Risiken, einschließlich solcher, die außerhalb des Kontextes von KI liegen.

Unter Berücksichtigung von Abbildung 1 und der Ausführungen zur Corporate Governance-Struktur bietet sich für die Unternehmen die Möglichkeit, auf bereits bestehende Maßnahmen aus der Risikomanagement Funktion zurückzugreifen und diese um KI-spezifische Risiken zu erweitern. Als Beispiel lässt sich die von der ISO (International Organization for Standardization) entwickelte Norm ISO 31000: Risk Management anführen.²¹⁶ Anders als die IDW-Standards, welche branchenspezifisch in Deutschland gelten, bietet die ISO branchenübergreifend internationale Standards. Diese stellen einen gleichen Standard im Hinblick auf Qualität und Sicherheit für Produkte und Dienstleistungen her.²¹⁷

Neben bereits bestehenden Standards werden derzeit von nationalen und internationalen Organisationen freiwillige Standards für das KI-Risikomanagement entwickelt. Ein exemplarischer Standard ist die kürzlich veröffentlichte ISO/IEC 23894:2023, die einen Leitfaden für den Umgang mit Risiken im Zusammenhang mit KI enthält. Dieser Standard wurde in Zusammenarbeit zwischen ISO und der Internationalen Elektronischen Kommission (IEC) entwickelt.²¹⁸

Die Verordnung verpflichtet Unternehmen, ein Risikomanagementsystem einzurichten, anzuwenden, zu dokumentieren und aufrechtzuerhalten. Obwohl die KI-VO diese Begriffe nicht expliziert definiert, kann ein System als „eingesetzt“ angesehen werden, wenn die Regeln, Verfahren und Anweisungen von der verantwortlichen Einheit erstellt und durch die Entscheidungsträger genehmigt worden sind. Die Anforderung des „Anwendens“ wird erfüllt, wenn die Mitarbeitenden des Unternehmens wissen, welche Maßnahmen erwartet werden und entsprechend handeln. Den Dokumentationsanforderungen kommen Unternehmen hinreichend nach, wenn sie den Ablaufprozess und die getroffenen Maßnahmen in einer für die Aufsichtsbehörden nachvollziehbaren Weise dokumentieren. Schlussendlich gilt, dass sichergestellt werden muss, dass das Risikomanagementsystem während des gesamten Lebenszyklus des KI-Systems aufrechterhalten wird.²¹⁹

²¹⁶ Vgl. Martini/Wendehorst/Braun Binder/Egli, Art. 9 Rn. 8; Ulbricht et al., Praxishandbuch KI und Recht, S. 217.

²¹⁷ Vgl. ISO, Standards, o.S.

²¹⁸ Vgl. Martini/Wendehorst/Braun Binder/Egli, Art. 9 Rn. 8; Ulbricht et al., Praxishandbuch KI und Recht, S. 217.

²¹⁹ Vgl. Ulbricht et al., Praxishandbuch KI und Recht, S. 216.

Die Schritte des Risikomanagementsystem sind in Art. 9 Abs. 2 S. 2 KI-VO geregelt, während die Ausgestaltung der Risikomanagementmaßnahmen sich anhand Art. 9 Abs. 5 KI-VO ableiten lässt.²²⁰

3.3.3.3.6 Daten Governance

Hochwertige Daten sind für die Entwicklung und Leistungsfähigkeit von KI-Modellen/-Systemen entscheidend und zeichnen sich zudem durch geringe Fehler und Verzerrungen aus.²²¹

Die KI-VO erkennt diese Bedeutung und hält in Art. 10 KI-VO die Anforderungen an die Qualität sowie das Management von Daten fest, die für die Entwicklung und das Training von Hochrisiko-KI-Systemen relevant sind. Aufgrund der Tatsache, dass die Vorschrift auf die Entwicklung und nicht die Verwendung von KI-Systemen abstellt, lässt sich im Wege der Auslegung ableiten, dass die Adressaten der Vorschrift die Anbieter dieser Systeme sind.²²²

Insbesondere den Trainings-, Validierungs- und Testdaten erlegt die Verordnung hohe Qualitätsanforderungen auf. In Art. 10 Abs. 3 S. 1, 2 und 3 und Abs. 4 KI-VO werden drei Gruppen von Kriterien für die Datenqualität definiert.²²³ Hierzu zählen unter anderem Anforderungen an die Vollständigkeit und Fehlerfreiheit der Daten. Mit der Formulierung in Art. 10 Abs. 3 KI-VO „so weit wie möglich“²²⁴ wird der Umstand großer Datenmengen berücksichtigt und der Anbieter auf diese Weise geschützt.²²⁵

Auch hinsichtlich der Datenanforderungen müssen die Verantwortlichkeiten und Rollen im Unternehmen klar geregelt sein. Daraus ergibt sich die Notwendigkeit der Einführung eines Daten-Governance-Verfahrens. Dieses Verfahren ist analog den anderen Governance-Strukturen im Umgang mit Daten, ein System der Regelung und Organisation.²²⁶ Ein solches Governance-System sollte die folgenden Kernkompetenzen enthalten: Identifizierung von Zielen, Festlegung von Verantwortlichkeiten und Rollen (inkl. klarer Führungsstruktur), Identifizierung und

²²⁰ Vgl. *Herbst/Panic*, KI-Recht praktisch erklärt, S. 22; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 216 f.

²²¹ Vgl. *Herbst/Panic*, KI-Recht praktisch erklärt, S. 23; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 178.

²²² Vgl. *Herbst/Panic*, KI-Recht praktisch erklärt, S. 23; *Steinrötter/Markert*, RD 2024, 400, 401.

²²³ Vgl. *Martini/Wendehorst/Braun Binder/Egli*, Art. 10 Rn. 59.

²²⁴ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 57.

²²⁵ Vgl. *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 178.

²²⁶ Vgl. *Herbst/Panic*, KI-Recht praktisch erklärt, S. 23.

Minderung potenzieller Risiken, Implementierung operativer Kontrollen, Bereitstellung kontinuierlicher Schulungen und regelmäßige Überprüfung der Daten-Governance.²²⁷

Anbieter von Hochrisiko-KI-Systemen müssen zudem berücksichtigen, dass sie auch dazu angehalten sind, neben den Anforderungen aus der KI-VO die Vorgaben der DSGVO (personenbezogene Daten) und der Datenverordnung (nicht personenbezogene Daten) zu beachten.²²⁸ Art. 10 Abs. 5 KI-VO räumt insoweit eine Ausnahme ein, als das unter bestimmten Voraussetzungen die Verarbeitung personenbezogener Daten, welche gemäß Art. 9 Abs. 1 DSGVO grundsätzlich verboten ist, dennoch zulässig sein kann.²²⁹

3.3.3.3.7 Qualitätsmanagement

Um die Einhaltung der Anforderungen der KI-VO sicherzustellen, haben Anbieter von Hochrisiko-KI-Systemen gemäß Art. 17 Abs. 1 KI-VO ein Qualitätsmanagementsystem einzurichten.²³⁰ Dieses System muss Regeln, Verfahren und Anweisungen enthalten, um die betrieblichen Prozesse verständlich abzubilden, systematisch zu organisieren und ordnungsgemäß zu dokumentieren.²³¹ Die englische Formulierung „ordly manner“ verdeutlicht, dass mit „ordnungsgemäß“ eine Dokumentation „in geordneter Art und Weise“²³² gemeint ist. Um eine solche Ordnung zu gewährleisten, müssen Anbieter dieser Systeme eine klare interne Verteilung der Aufgaben und Verantwortlichkeiten vornehmen. Ratsam ist es, den Datenschutzbeauftragten, IT-Sicherheitskräfte und sonstige Fachkräfte in das System einzubinden, um eine umfassende Compliance zu gewährleisten. Die Steuerung und konsolidierte Dokumentation erfolgen dabei in einer zentralen Einheit, die einen umfassenden Überblick gewährleistet (z.B. der für KI verantwortlichen Einheit), unter Einbindung aller relevanten Funktionen. Zur Sicherstellung einer systematischen und strukturierten Vorgehensweise können die Verschriftlichung von Strategien und Verfahren sowie eine umfassende Dokumentation dienen.²³³

Art. 17 Abs. 1 KI-VO führt die Mindestinhalte auf, die das Qualitätsmanagementsystem umfassen muss. Die Umsetzung dieser Inhalte muss gemäß Art. 17 Abs. 2 KI-VO angemessen und im Verhältnis zur Größe der Organisation erfolgen.

²²⁷ Vgl. *Bitkom*, Umsetzungsleitfaden zur KI-Verordnung, 2024, S. 96.

²²⁸ Vgl. *Bitkom*, Umsetzungsleitfaden zur KI-Verordnung, 2024, S. 96.

²²⁹ Vgl. *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 178.

²³⁰ Vgl. *Herbst/Panic*, KI-Recht praktisch erklärt, S. 22; Martini/Wendehorst/*Eisenberger*, Art. 17 Rn. 1.

²³¹ Vgl. Martini/Wendehorst/*Eisenberger*, Art. 17 Rn. 11.

²³² Vgl. Martini/Wendehorst/*Eisenberger*, Art. 17 Rn. 11.

²³³ Vgl. *Herbst/Panic*, KI-Recht praktisch erklärt, S. 22.

Hieraus ergeben sich insbesondere für KMU geringere Anforderungen als für große Unternehmen.²³⁴

Anbieter von KI-Systemen, die bereits sektorspezifischen Anforderungen unterliegen, können die in der KI-VO aufgeführten Inhalte in ein bereits bestehendes Qualitätsmanagement integrieren und sind nicht dazu angehalten, die Governance-Strukturen anzupassen. Ein ähnliches Vorgehen gilt für Finanzinstitute gemäß Art. 17 Abs. 4 KI-VO.²³⁵

3.3.3.3.8 Menschliche Aufsicht

Dem Anbieter eines Hochrisiko-KI-Systems obliegt gemäß Art. 14 Abs. 1 KI-VO die Pflicht, die Systeme so zu entwickeln, dass sie während der Verwendung von natürlichen Personen beaufsichtigt werden können. Das Erfordernis der menschlichen Aufsicht stellt einen Kernbaustein des Grundrechtsschutzes dar, um die Risiken und potenziellen Gefahren intelligenter Systeme zu minimieren.²³⁶

Die Aufsichtsmaßnahmen müssen von dem Anbieter so ausgestaltet sein, dass sie dem Grad der Autonomie und Kontext der Nutzung nach angemessen sind. Hierfür gilt es bereits vor Inverkehrbringen bzw. der Inbetriebnahme des KI-Systems Vorkehrungen zu treffen, wie sie in Art. 4 Abs. 3 lit. a und b KI-VO beschrieben werden. Art. 14 Abs. 4 KI-VO legt zudem fest, in welcher Form die Systeme den Betreibern zur Verfügung zu stellen sind. Diese wiederum sind gemäß Art. 26 Abs. 2 KI-VO dazu verpflichtet, natürlichen Personen die menschliche Aufsicht zu übertragen und die erforderliche Kompetenz zur Erfüllung der Anforderungen sicherzustellen.²³⁷

Zur Gewährleistung eines effektiven Schutzes müssen Betreiber die Verantwortlichkeit der Aufsichtsperson im Innenverhältnis klar regeln und die notwendigen Weiterbildungsmaßnahmen zur Kompetenzerweiterung sicherstellen.

Eine Ausnahmeregelung beschreibt Art. 14 Abs. 5 KI-VO für die biometrische Fernidentifizierung (Art. 3 Nr. 41 KI-VO).

²³⁴ Vgl. Martini/Wendehorst/*Eisenberger*, Art. 17 Rn. 28.

²³⁵ Vgl. Martini/Wendehorst/*Eisenberger*, Art. 17 Rn. 30 f.

²³⁶ Vgl. Klos/*Taylan*, CCZ 2024, 205, 208; Martini/Wendehorst/*Martini*, Art. 14 Rn. 35.

²³⁷ Vgl. *Herbst/Panic*, KI-Recht praktisch erklärt, S. 25; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 181 f.

3.3.3.3.9 Pflichten gegenüber Behörden

Gemäß Art. 21 Abs. 1 KI-VO sind Anbieter verpflichtet, auf begründete Anfrage der zuständigen Behörden alle Unterlagen vorzulegen, die zur Überprüfung der Konformität erforderlich sind. Hierzu gehört unter Umständen auch der Zugang zu den unter ihrer Kontrolle liegenden Protokollen (Art. 12 iVm. Art. 19 KI-VO). Betreiber sind gemäß Art. 16 Abs. 12 KI-VO gleichermaßen verpflichtet, bei allen Maßnahmen im Zusammenhang mit Hochrisiko-KI-Systemen mit den Behörden zu kooperieren. Die Verpflichtung der Zusammenarbeit mit den Behörden verdeutlicht erneut die zentrale Bedeutung der Einhaltung der Aufbewahrungspflichten gemäß Art. 18 und 19 KI-VO.²³⁸

Sowohl Anbieter und deren Bevollmächtigte als auch Betreiber unterliegen gemäß Art. 49 KI-VO einer Registrierungspflicht für Hochrisiko-KI-Systeme in der gemäß Art. 71 KI-VO einzurichtenden EU-Datenbank. Dies gilt auch dann, wenn das KI-System dem Ausnahmetatbestand nach Art. 6 Abs. 3 KI-VO unterliegt.²³⁹ Diese Pflicht soll neben der erhöhten Transparenz auch eine Unterstützung für die Marktüberwachungsbehörden und ihre Überwachungs- und Kontrolltätigkeiten bieten.²⁴⁰ Betreiber sind verpflichtet, gemäß Art. 26 Abs. 8 KI-VO ein nicht in der EU-Datenbank registriertes KI-System nicht in Betrieb zu nehmen. In einem solchen Fall ist der Anbieter oder Händler entsprechend zu informieren.

Für Anbieter von Hochrisiko-KI-Systemen ergibt sich aus Art. 73 KI-VO eine zusätzliche Meldepflicht bei schwerwiegenden Verstößen (Art. 3 Nr. 49 KI-VO) gegenüber der Marktüberwachungsbehörden. Diese Pflicht ist im Zusammenhang mit der Verpflichtung zur Beobachtung nach dem Inverkehrbringen nach Art. 72 KI-VO zu sehen. Art. 26 Abs. 5 KI-VO beschreibt zudem spezifische Bedingungen, die eine Anwendung von Art. 73 KI-VO auf Betreiber erforderlich machen können. Unternehmen sind daher dazu angehalten im Rahmen des Qualitätsmanagements nach Art. 17 Abs. 1 lit. i KI-VO ein adäquates Meldeverfahren einzurichten. Hierzu gilt es, klare interne Meldewege zu definieren und zu dokumentieren (siehe C II 4).

3.3.3.3.10 Genauigkeit, Robustheit und Cybersicherheit

Mit Art. 15 KI-VO wird insbesondere das von der EU verfolgte Ziel einer vertrauenswürdigen und ethischen KI unterstützt. Hochrisiko-KI-Systeme sind nach Art.

²³⁸ Vgl. Martini/Wendehorst/*Eisenberger*, Art. 21 Rn. 1 ff.; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 186; *Voigt/Hullen*, HdB-KI-Verordnung, S. 98 f.

²³⁹ Vgl. *Ebers/Streitböcker*, RDi 2024, 393, 399.

²⁴⁰ Vgl. Martini/Wendehorst/*Gerdemann*, Art. 49 Rn. 1.

15 Abs. 1 KI-VO mit einem „angemessene[m] Maß an Genauigkeit, Robustheit und Cybersicherheit“²⁴¹ zu entwickeln.

In Bezug auf die Genauigkeit sind Anbieter nach Art. 15 Abs. 3 KI-VO dazu verpflichtet, entsprechende Angaben in den beiliegenden Betriebsanleitungen (Art. 13 KI-VO) zu machen und die Betreiber über das Leistungskennzahlenniveau in einer leicht verständlichen Weise zu informieren (Erwgr. 74 KI-VO). Die Systeme müssen zudem nach Art. 15 Abs. 4 S. 1 und 2 KI-VO so widerstandsfähig wie möglich gestaltet werden. Hierzu sind Anbieter angehalten TOMs zu entwickeln. Erwgr. 75 KI-VO bietet konkrete Anhaltspunkte dahingehend, welche Maßnahmen zur Gewährleistung der Robustheit in Betracht kommen.²⁴²

Zudem fordert Art. 15 Abs. 5 KI-VO, dass Hochrisiko-KI-Systeme auch gegen unbefugte Eingriffe Dritter resistent sein müssen. Hierzu ist ergänzend Erwgr. 76 KI-VO heranzuziehen, welcher genauere Ausführungen zu einem angemessenen Cybersicherheitsniveau gibt. Anbieter sollten außerdem beachten, dass gemäß Erwgr. 77 KI-VO jene Hochrisiko-KI-Systeme, die in den Anwendungsbe- reich des EU-Cyber Resilience Act²⁴³ fallen, durch die Erfüllung der dortigen An- forderungen zugleich den Anforderungen der KI-VO gerecht werden.²⁴⁴

Es empfiehlt sich daher eine Prüfung bereits bestehender Vorkehrungen und der Konsolidierung ebendieser.

3.3.3.4 GPAI-Modelle

Als eine weitere Kategorie im Rahmen der KI-VO gelten die GPAI-Modelle, die eine von dem Risiko eines KI-Systems unabhängige Kategorie bilden. Unternehmen sind daher verpflichtet, neben der bisher dargelegten Risikoklassen zu prü- fen, ob sie als Anbieter eines GPAI-Modells einzustufen sind.²⁴⁵

Während GPAI-Systeme im Rahmen der Risikoklassifizierung mit KI-Systemen gleichzustellen sind, unterliegen GPAI-Modelle gemäß den Bestimmungen in Art. 51 ff. KI-VO einem eigenständigem Regelungssystem.²⁴⁶ Da ein GPAI-Modell

²⁴¹ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 61.

²⁴² Vgl. *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 182.

²⁴³ Vgl. Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), ABl. Nr. L 81 v. 20.11.2024.

²⁴⁴ Vgl. Martini/Wendehorst/*Martini*, Art. 15 Rn. 90; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 183.

²⁴⁵ Vgl. *Klos/Taylan*, CCZ 2024, 205, 209.

²⁴⁶ Vgl. *Chibanguza/Steege*, NJW 2024, 1769, 1774.

stets in ein System integriert sein muss, bestehen die in Art. 51 ff. KI-VO beschriebenen Pflichten ausschließlich für Anbieter sowie deren Bevollmächtigte.²⁴⁷

Die Pflichten für Anbieter werden nach dem Vorliegen eines systemischen Risikos gemäß Art. 3 Nr. 65 KI-VO differenziert. Aus Art. 53 KI-VO ergeben sich die allgemeinen Pflichten für Anbieter von GPAI-Modellen, während Art. 55 KI-VO spezifischere Pflichten für Anbieter von GPAI-Modellen mit systematischem Risiko ausführt.

Die Bestimmungen in Anhang XI KI-VO sind ergänzend zu den Anforderungen in Art. 51 ff. KI-VO zu sehen – sie treffen weitere Ausführungen hinsichtlich der technischen Dokumentation für GPAI-Modelle gemäß Art. 53 Abs. 1 lit. a KI-VO.

3.3.4 Erstellung Pflichtenkatalog

Für Unternehmen empfiehlt es, sich neben der Erstellung eines Verzeichnisses einen allgemeinen Pflichtenkatalog zu entwickeln. Dieser Pflichtenkatalog kann vor, parallel oder nach der Risikoklassifizierung implementiert werden. In diesem Katalog sollen die Pflichten aller Akteure strukturiert zusammengestellt werden.

Zur übersichtlichen Darstellung bietet sich eine tabellarische Aufbereitung des Pflichtenkatalogs an. Eine Möglichkeit könnte darin bestehen, dass für jeden Akteur im Sinne der KI-VO ein separates Tabellenblatt erstellt wird. In dieser Tabelle können sodann der jeweiligen Risikokategorie die Pflichten zugeordnet werden.

Führt man die bisherigen Ausführungen und insbesondere die im letzten Kapitel dargestellten Pflichten zusammen, lassen sich folgende Inhalte für den Pflichtenkatalog erkennen.

3.3.4.1 Anbieter

Für Anbieter ergeben sich im Rahmen der KI-VO die weitreichendsten Pflichten.²⁴⁸

Besondere Beachtung verdient in diesem Zusammenhang Art. 25 Abs. 1 KI-VO. Dieser regelt, dass unter den dort genannten Voraussetzungen die in Art. 16 KI-VO definierten Anbieterpflichten auf andere Personen, insbesondere Händler, Einführer oder Betreiber übergehen können. In diesen Fällen gilt die betreffende

²⁴⁷ Vgl. *Chibanguza/Steege*, NJW 2024, 1769, 1774.

²⁴⁸ Vgl. *Martini/Wendehorst/Wendehorst*, Art. 3 Rn. 63.

Person als neuer Anbieter und ist verpflichtet, den entsprechenden Anforderungen der Verordnung nachzukommen.²⁴⁹

Unternehmen, die die Rolle des Anbieters eines KI-Systems übernehmen, sollten die folgenden Artikel der KI-VO berücksichtigen:

3.3.4.1.1 Begrenztes/minimales Risiko

- Art. 50 Abs. 1 und 2 iVm. Abs. 5 KI-VO: Transparenzpflichten für bestimmte Systeme
- Art. 95 KI-VO: Freiwillige Aufstellung von Verhaltenskodizes

3.3.4.1.2 Hohes Risiko

- Art. 6 Abs. 4 KI-VO: Dokumentierungspflicht und Registrierungspflicht
- Art. 9 KI-VO: Einrichtung Risikomanagementsystem
- Art. 10 KI-VO: Erstellen eines Daten-Governance-Verfahrens
- Art. 11 Abs. 1 und 2 KI-VO: Sicherstellung technischer Dokumentation
- Art. 12 KI-VO: Aufzeichnungspflicht
- Art. 13 Abs. 1, 2 und 3 KI-VO: Transparenzpflichten und Bereitstellung von Betriebsanleitungen
- Art. 14 KI-VO: Sicherstellung menschlicher Aufsicht
- Art. 15 KI-VO: Gewährleistung von Genauigkeit, Robustheit und Cybersicherheit
- Art. 16 KI-VO: Pflichten Anbieter von Hochrisiko-KI-Systemen
- Art. 17 KI-VO: Einrichtung Qualitätsmanagement
- Art. 18 und 19 KI-VO: Einhaltung Aufbewahrungsfristen für Dokumente und Protokolle
- Art. 20 Abs. 1 und 2 KI-VO: Pflicht zu Korrekturmaßnahmen und Informationspflicht
- Art. 21 KI-VO: Gewährleistung der Zusammenarbeit mit den Behörden
- Art. 22 KI-VO: Ernennung eines Bevollmächtigten und Gewährleistung Aufgabenerfüllung
- Art. 25 Abs. 3 KI-VO: Pflichtübernahme des Produktherstellers
- Art. 43, 47 und 48 KI-VO: Pflicht zur Konformitätsbewertung, EU-Konformitätserklärung und CE-Kennzeichnung

²⁴⁹ Vgl. *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 192.

- Art. 49 Abs. 1 und 2 KI-VO: Einhaltung Registrierungspflicht in der EU-Datenbank
- Art. 50 Abs. 1 und 2 iVm. Abs. 5 KI-VO: Transparenzpflichten für bestimmte Systeme
- Art. 72 KI-VO: Beobachtungspflichten nach dem Inverkehrbringen
- Art. 73 Abs. 1-4 und 5 KI-VO: Meldepflichten und Untersuchungspflicht schwerwiegender Fälle
- Art. 80 Abs. 4 und 5 KI-VO: Konformitätspflicht Ausnahmetatbestand
- Art. 82 Abs. 1 und 2 KI-VO: Pflicht Korrekturmaßnahmen im Falle eines Risikos für Gesundheit und Sicherheit von Personen, für Grundrechte oder andere Aspekte des Schutzes des öffentlichen Interesses

3.3.4.1.3 GPAI-Modelle

- Art. 50 Abs. 1 iVm. Abs. 5 KI-VO: Transparenzpflichten für bestimmte Systeme
- Art. 53 Abs. 1 lit. a und b und Abs. 2 KI-VO: Erstellung/ Aktualisierung technischer Dokumentation und Zurverfügungstellung für Anbieter
- Art. 53 Abs. 1 lit. c und Abs. 2 KI-VO: Strategie zur Einhaltung des Urheberrechts
- Art. 53 Abs. 1 lit. d und Abs. 2 KI-VO: Erstellung Zusammenfassung Trainingshinhalte
- Art. 54 Abs. 1 und 2 KI-VO: Benennung Bevollmächtigter
- Art. 55 KI-VO: Pflichten für GPAI-Modelle mit systematischem Risiko
- Art. 91 Abs. 1, 3 und 5 KI-VO: Dokumentations- und Informationsanforderungen
- Art. 93 Abs. 1 KI-VO: Pflicht zum Nachkommen der Kommissions-Auforderungen

3.3.4.2 Betreiber

Auch für Betreiber von KI-Systemen ergeben sich durch die KI-VO Pflichten, welche es zu berücksichtigen gilt. Konkret handelt es sich dabei um die folgenden Vorschriften:

3.3.4.2.1 Begrenztes/minimales Risiko

- Art. 50 Abs. 3 und 4 iVm. Abs. 5 KI-VO: Transparenzpflichten für bestimmte Systeme
- Art. 95 KI-VO: Freiwillige Aufstellung von Verhaltenskodizes

3.3.4.2.2 Hohes Risiko

- Art. 14 Abs. 3 lit. b KI-VO: Vorkehrungen für menschliche Aufsicht
- Art. 25 Abs. 1, 2 und 3 KI-VO: Übergang der Anbieterpflichten
- Art. 26 Abs. 1 und 2 KI-VO: TOMs und Sicherstellung menschliche Aufsicht
- Art. 26 Abs. 4 KI-VO: Qualitätssicherung Eingabedaten
- Art. 26 Abs. 5 KI-VO: Überwachung anhand Betriebsanleitung und Informationspflichten
- Art. 26 Abs. 6 KI-VO: Aufbewahrungspflicht Protokolle
- Art. 26 Abs. 7 KI-VO: Informationspflicht gegenüber Arbeitnehmervertretern und Arbeitnehmern
- Art. 26 Abs. 8 KI-VO: Registrierungspflicht
- Art. 26 Abs. 9 KI-VO: DSFA
- Art. 26 Abs. 10 KI-VO: Pflichten biometrische Fernidentifizierung
- Art. 26 Abs. 11 KI-VO: Informationspflicht gegenüber natürlichen Personen
- Art. 27 Abs. 1 und 3 KI-VO: GFA
- Art. 50 Abs. 3 und 4 iVm. Abs. 5 KI-VO: Transparenzpflichten für bestimmte Systeme
- Art. 86 Abs. 1 KI-VO: Pflicht zur aussagekräftigen Erläuterung gegenüber betroffenen Personen

3.3.4.3 Bevollmächtigte

Anbieter, die außerhalb der EU niedergelassen sind, sind gemäß der KI-VO dazu verpflichtet, einen in der EU niedergelassenen Bevollmächtigten zu benennen. Dieser übernimmt die Verantwortung für die Einhaltung der Anforderungen der KI-VO und hat insbesondere die folgenden Pflichten wahrzunehmen;:²⁵⁰

²⁵⁰ Siehe weiterführend Erwgr. 82 KI-VO.

3.3.4.3.1 Hohes Risiko

- Art. 22 Abs. 3 KI-VO: Pflichten anstelle des Anbieters
- Art. 33 Abs. 4 KI-VO: Pflicht zur Auftragsbeendigung

3.3.4.3.2 GPAI-Modelle

- Art. 54 Abs. 3 KI-VO: Pflichten anstelle des Anbieters
- Art. 54 Abs. 4 KI-VO: Ansprechpartner Büro für Künstliche Intelligenz oder zuständige Behörden
- Art. 54 Abs. 5 KI-VO: Pflicht zur Auftragsbeendigung

3.3.4.4 Einführer

Einführer unterliegen durch das Inverkehrbringen von KI-Systemen ebenfalls spezifischen Verpflichtungen, insbesondere im Hinblick auf Hochrisiko-KI-Systeme:

- Art. 23 Abs. 1 KI-VO: Sicherstellung Konformität mit der Verordnung
- Art. 23 Abs. 2 KI-VO: Konformitätsanforderungen und Informationspflicht
- Art. 23 Abs. 3 KI-VO: Angabe Name, Handelsname oder Handelsmarke
- Art. 23 Abs. 4 KI-VO: Gewährleistung von Lagerungs- und Transportbedingungen
- Art. 23 Abs. 5 KI-VO: Aufbewahrungsfristen
- Art. 23 Abs. 6 KI-VO: Pflicht zur Informations- und Dokumentenübermittlung an Behörden
- Art. 23 Abs. 7 KI-VO: Pflicht zur Zusammenarbeit mit den Behörden

3.3.4.5 Händler

Auch für Händler gibt es im Zusammenhang mit Hochrisiko-KI-Systemen die folgenden Pflichten zu beachten:

- Art. 24 Abs. 1 KI-VO: Überprüfung CE-Kennzeichnung, EU-Konformitätserklärung, Betriebsanleitung und Pflichtenerfüllung seitens Anbieter und Einführer
- Art. 24 Abs. 2 KI-VO: Konformitätsanforderungen und Informationspflicht
- Art. 24 Abs. 3 KI-VO: Gewährleistung von Lagerungs- und Transportbedingungen

- Art. 24 Abs. 4 KI-VO: Pflicht zu Korrekturmaßnahmen und Informationspflicht
- Art. 24 Abs. 5 KI-VO: Pflicht zur Informations- und Dokumentenübermittlung an Behörden
- Art. 24 Abs. 6 KI-VO: Pflicht zur Zusammenarbeit mit den Behörden

3.3.5 Mapping: KI-Verzeichnis und Pflichtenkatalog

Sobald das KI-Verzeichnis erstellt und sowohl Rolle als auch Risiko bestimmt wurden, können die in dem Pflichtenkatalog zusammengetragenen Pflichten den einzelnen Systemen zugeordnet werden.²⁵¹

Es obliegt dem Unternehmen zu entscheiden, ob die Pflichten in das Verzeichnis übertragen werden. Falls ja, verfügt das Unternehmen im Anschluss über eine transparente Übersicht aller KI-Systeme sowie den daraus resultierenden Pflichten. Darüber hinaus haben sich die Unternehmen mit der Erstellung eines Pflichtenkatalogs eine Übersicht aller relevanter Anforderungen für Anbieter, Betreiber, Bevollmächtigte, Einführer und Händler aus der KI-VO erstellt. Dieser Katalog sollte den für die KI-Systeme verantwortlichen Mitarbeitenden bereitgestellt werden und als Leitfaden bei der Einführung neuer KI-Systeme dienen.²⁵²

Idealerweise obliegt einer zentral verantwortlichen Person (z.B. dem KI-Beauftragten) die Pflege des Verzeichnisses und des Pflichtenkatalogs. Auf diese Weise kann sichergestellt werden, dass etwaige rechtliche sowie interne Änderungen berücksichtigt werden und die Dokumentation stets aktuell bleibt.

²⁵¹ Vgl. *Klos/Taylan*, CCZ 2024, 205, 210.

²⁵² Vgl. *Klos/Taylan*, CCZ 2024, 205, 210 f.

4 Kritische Analyse der Anforderungen

Die bisherigen Ausführungen dieser Arbeit geben Aufschluss über den Umfang der KI-VO sowie den hieraus resultierenden Anforderungen für Unternehmen. Eine zentrale Fragestellung in diesem Zusammenhang ist, welche Chancen und Herausforderungen sich aus der Einführung der KI-VO für Unternehmen ergeben.

4.1 Chancen

Der Einsatz von KI bietet Unternehmen viele Vorteile und eröffnet zahlreiche Chancen. Hierzu zählen unter anderem die Analyse großer Datenmengen und die hieraus resultierende Effizienzsteigerung.²⁵³ Zudem können mit Hilfe des Einsatzes von KI subjektive Einflüsse ausgeschaltet und objektivere Ergebnisse erzielt werden, was die Entscheidungsqualität erheblich verbessert.²⁵⁴

Fraglich ist jedoch, welche konkreten Chancen sich aus der Verabschiedung der KI-VO für Unternehmen ergeben.

4.1.1 Rechtssicherheit durch einheitliche Regulierung

Mit der Einführung der KI-VO wurde ein einheitlicher Rechtsrahmen für die Regulierung von KI-Technologien innerhalb der EU erschaffen.²⁵⁵

Von dieser Harmonisierung profitieren Unternehmen insbesondere durch die damit einhergehende Rechtssicherheit. Diese wurde durch die Entscheidung der Gesetzgebung, die KI-VO in Form einer Verordnung zu erlassen, besonders gestärkt. Ein wesentlicher Vorteil dieses Ansatzes liegt darin, dass Unternehmen nicht verpflichtet sind, sich an unterschiedliche nationale Vorgaben anzupassen. Somit wird innerhalb der EU eine einheitliche Regulierung gewährleistet.²⁵⁶ Dieser Umstand bedeutet nicht nur für die Unternehmen eine Erleichterung bei der Umsetzung der Anforderungen, sondern auch für die Arbeit der zuständigen Behörden – insbesondere bei der Prüfung der Konformität von KI-Systemen.

Hinzu kommt, dass durch den harmonisierten Rechtsrahmen Unternehmen die Möglichkeit eingeräumt wird, KI-Systeme in mehreren EU-Ländern einsetzen zu

²⁵³ Vgl. *Schneider*, ARP 2023, 194, 195.

²⁵⁴ Vgl. *Knappertsbusch/Gondlach*, Arbeitswelt und KI 2030, S. 80.

²⁵⁵ Vgl. *Bundesregierung*, AI Act verabschiedet, 2024, o.S.

²⁵⁶ Vgl. *Wybitul*, BB 2024, 2179.

können, ohne dass Anpassungen an nationale regulatorische Vorgaben erforderlich sind. Insbesondere für kleinere Unternehmen, welche häufig über begrenzte Ressourcen verfügen, ist dies von Vorteil. Durch die einheitlichen Regelungen trägt die Verordnung zudem zur Schaffung eines fairen Wettbewerbsumfelds aller Marktteilnehmer bei.²⁵⁷

4.1.2 Gewährleistung eines hohen Schutzniveaus

Im Rahmen der KI-VO wird dem Schutz der Grundrechte und der Sicherheit der Menschen ein besonders hoher Stellenwert zugemessen. Dies wird insbesondere dadurch deutlich, dass bereits Erwgr. 1 KI-VO diesen Aspekt im Zusammenhang mit dem übergeordneten Zweck der Regulierung hervorhebt.²⁵⁸

Damit dieser Schutz gewährleistet werden kann, wurde der zuvor erwähnte risikobasierte Ansatz gewählt. Hochrisiko-KI-Systeme unterliegen strengen Anforderungen und umfassenden Überwachungen, da der Gesetzgeber bei der Nutzung solcher Systeme ein besonders hohes Risiko für die in der Verordnung definierten Schutzgüter erkennt.²⁵⁹

Auch der Vermeidung von Diskriminierung durch den Einsatz von KI trägt der Gesetzgeber Rechnung. Hierzu führt der Gesetzgeber in Erwgr. 27 KI-VO die von der Expertengruppe AI HLEG entwickelten sieben Grundsätze, zu denen auch der Grundsatz der Nichtdiskriminierung gehört, an. Hiermit wird das Erfordernis, dass KI-Systeme ohne „diskriminierende Auswirkungen und unfaire Verzerrungen“²⁶⁰ entwickelt werden verdeutlicht.

4.2 Risikobasierte Regulierung

Der Gesetzgeber verfolgt mit der Verordnung einen risikobasierten Ansatz und ermöglicht somit eine dem Risiko angemessene Regulierung. Hierdurch wird sowohl einer Unter- als auch Überregulierung entgegengewirkt.²⁶¹ Der risikobasierte Ansatz berücksichtigt insbesondere den aktuellen Stand der Technik und kann bei zukünftigen Veränderungen angepasst werden, was ihn gegenüber innovativen Entwicklungen flexibler macht.

²⁵⁷ Siehe weiterführend Erwgr. 121 KI-VO.

²⁵⁸ Vgl. von Welser, GRUP-Prax 2024, 485.

²⁵⁹ Siehe weiterführend Erwgr. 7 KI-VO.

²⁶⁰ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 8.

²⁶¹ Siehe weiterführend Erwgr. 26 KI-VO.

Durch die klar differenzierten Regelungen wird zudem sowohl für Anbieter als auch Betreiber von KI-Systemen eine verlässliche Grundlage geschaffen. Insbesondere der Umstand, dass Hochrisiko-KI-Systeme strengerem Anforderungen unterliegen und zudem bestimmte Zertifizierungen nachweisen müssen, stärkt das Vertrauen in die Regulierung von KI-Systemen. Die KI-VO sorgt durch den risikobasierten Ansatz dafür, dass die in der EU eingesetzten KI-Systeme „sicher, transparent, ethisch vertretbar, unvoreingenommen und unter menschlicher Kontrolle sind“.²⁶²

Ein weiterer Vorteil ist, dass durch den risikobasierten Ansatz eine Reduzierung des Kostenaufwands für Unternehmen geschaffen wird. Insbesondere für KI-Systeme mit minimalem oder begrenztem Risiko wird durch das Fehlen umfassender Vorgaben der regulatorische Aufwand deutlich reduziert.

4.2.1 Zunehmendes Vertrauen in KI-Technologien

Mit der Einführung des Regelwerkes wird maßgeblich das Vertrauen in die KI-Technologien gestärkt, da die Einhaltung der Anforderungen einheitliche Standards schafft und dadurch ein hohes Maß an Transparenz gewährleistet.²⁶³ Auch auf Verbraucherseite wird das Vertrauen in die von Anbietern auf den EU-Markt gebrachten KI-Systeme durch die einheitlichen Standards erheblich gestärkt. Verbraucher können sich darauf verlassen, dass die eingesetzten KI-Systeme den hohen Sicherheitsanforderungen der KI-VO entsprechen.²⁶⁴

Einer der wesentlichen Aspekte der KI-VO ist der Ausbau der KI-Kompetenz, wie in Art. 4 KI-VO dargelegt. Diese Anforderung versieht die Verordnung mit einer vergleichsweisen kurzen Umsetzungsfrist (Art. 113 lit. a KI-VO) und misst ihr hierdurch eine besondere Priorität zu. Unternehmen sind daher bereits jetzt dazu angehalten, die KI-Kompetenz bei ihren Mitarbeitenden systematisch auszubauen. Es ist anzunehmen, dass mit zunehmender Fachkenntnis der Mitarbeitenden auch das Vertrauen in die KI-Technologien wächst.

Hinzu kommt, dass der Ausbau der Kompetenz auf allen Ebenen – einschließlich der Governance-Funktionen – dazu führt, dass die Mitarbeitenden sich die Nutzung der neuen Technologie zum Vorteil machen, was zu einer Steigerung der Effektivität ihrer Arbeit führt. Insbesondere für die Kontroll- und Überwachungsfunktionen innerhalb eines Unternehmens, welche in ihrer täglichen Arbeit mit KI als neues Risiko konfrontiert sind, bietet der Einsatz von KI-Technologien auch

²⁶² Europäische Kommission, Künstliche Intelligenz, o.S.

²⁶³ Vgl. Bundesregierung, AI Act verabschiedet, 2024, o.S.

²⁶⁴ Vgl. Deutscher Bundestag, Positionspapier, S. 2.

im Bereich der Überwachung und Regulierung Raum für eine signifikante Effizienzsteigerung.²⁶⁵

4.2.2 Förderung der Innovation

Insbesondere KMU und Start-ups gelten durch ihre neuen Ideen und Entwicklungen als zentrale Treiber der Innovation. Die KI-VO schafft einen rechtlichen Rahmen, der darauf abzielt, das Potential ebendieser Unternehmen zu erkennen und zu fördern.²⁶⁶ Dies wird insbesondere durch die Einrichtung der Reallabore gemäß Art. 57 KI-VO verdeutlicht. Hierdurch schafft der Gesetzgeber eine kontrollierte Versuchs- und Testumgebung, in der innovative KI-Technologien unter realen Bedingungen getestet werden können, ohne dass die Unternehmen den Anforderungen aus der KI-VO vollständig ausgesetzt sind.

Mit Erwgr. 139 KI-VO sowie Art. 62 Abs. 1 lit. a KI-VO wird dem Aspekt der Innovationsförderung besondere Bedeutung zugemessen, indem Start-ups und KMU ein bevorzugter Zugang zu den Reallaboren eingeräumt wird.²⁶⁷ Diese profitieren von der gezielten Förderung und der Möglichkeit, innovative Technologien unter weniger hohen Anforderungen zu entwickeln und zu testen.²⁶⁸ Die hieraus resultierende Förderung neuer Produkte und Dienstleistungen trägt wesentlich zu einer Qualitätssteigerung auf dem europäischen Markt bei.²⁶⁹

Die Bundesregierung verfolgt das Ziel, Deutschland zu einem der führenden Märkte im Bereich der KI-Technologien zu etablieren.²⁷⁰ Durch die Unterstützung von Innovation wird die Wettbewerbsfähigkeit des europäischen Binnenmarktes wesentlich gestärkt und somit eines der übergeordneten Ziele der KI-VO.²⁷¹

4.2.3 Ausgestaltungsmöglichkeiten für Unternehmen

Positiv herausstellen lässt sich zudem, dass die Verordnung den Unternehmen die Möglichkeit zur aktiven Mitgestaltung der Regulierung bietet. Insbesondere die freiwilligen Verhaltenskodizes in Art. 95 KI-VO unterstreichen diesen Aspekt.

²⁶⁵ Vgl. *Soong*, CNL 2024, 12.

²⁶⁶ Siehe weiterführend Erwgr. 8 und 143 KI-VO; vgl. *Krimphove*, ZWH 2024, 249 f.

²⁶⁷ Vgl. *Deloitte*, EU AI Act, 2024, o.S.

²⁶⁸ Vgl. *Deloitte*, EU AI Act, 2024, o.S.; *Voigt Hullen*, HdB-KI-Verordnung, S. 179.

²⁶⁹ Vgl. *Europäisches Parlament*, Was ist künstliche Intelligenz und wie wird sie genutzt? 2020, o.S.

²⁷⁰ Vgl. *Bundesregierung*, AI Act verabschiedet, 2024, o.S.; *Bundesregierung*, Zukunftsthema KI, o.S.

²⁷¹ Siehe weiterführend Erwgr. 1 KI-VO.

Unternehmen wird durch die Selbstregulierung die Möglichkeit geboten, das hohe Schutzniveau der Hochrisiko-KI-Systeme auf andere Systeme in ihrem Bestand auszuweiten.²⁷² Die Verhaltenskodizes bilden somit eine sinnvolle Ergänzung zu der gesetzlichen Regulierung und ermöglichen Unternehmen, branchenspezifische Anforderungen an die eingesetzten KI-Systeme zu stellen. Durch diesen Ansatz erreicht der Gesetzgeber eine praxisnahe Umsetzung der KI-VO.

4.3 Herausforderungen

Neben dem Bestreben, einen einheitlichen Rechtsrahmen zum sicheren Einsatz von KI zu etablieren, stellt die KI-VO die Unternehmen auch vor eine Reihe von Herausforderungen, die es zu bewältigen gilt.²⁷³

4.3.1 Risikobasierter Ansatz

Während der von der KI-VO verfolgte risikobasierte Ansatz zunächst aufgrund seiner differenzierten Regulierung viele Vorteile bietet, stellt sich die Frage, wie praktikabel und sinnvoll eine Vorabestufung von KI-Systemen tatsächlich ist.²⁷⁴ Risiken, die mit einem System verbunden sind, treten häufig erst während der Nutzung und mit der Zeit deutlich hervor, sodass eine verlässliche Bewertung im Vorfeld nur eingeschränkt möglich ist.²⁷⁵

Hinzu kommt, dass die Verordnung gemäß Erwgr. 1 KI-VO das Ziel verfolgt, zukunftsorientiert zu agieren und die Regelungen an den aktuellen Stand der Technologie anzupassen. Dieses Ziel erfordert Mechanismen zur regelmäßigen Überprüfung und Aktualisierung. Diesem Umstand hat der Gesetzgeber mit Art. 112 KI-VO Rechnung getragen. Insbesondere durch eine jährliche Überprüfung der Aktualität der Hochrisiko-KI-Systeme in Anhang III und den verbotenen Praktiken in Art. 5 KI-VO. Aber auch auf weitere zentrale Bereiche der Verordnung erstrecken sich diese regelmäßigen Überprüfungsmechanismen.

Diese Flexibilität ermöglicht es, die KI-VO an technologische Entwicklungen anzupassen und trägt dazu bei, das Ziel der Verordnung – einen innovativen Umgang mit KI-Technologien – zu fördern. Allerdings birgt die regelmäßige Überprüfung und Anpassung der Verordnung (Art. 112 KI-VO) auch Herausforderungen für Unternehmen. Insbesondere in der Anfangsphase der Umsetzung können die

²⁷² Vgl. Martini/Wendehorst/Hartmann, Art. 95 Rn. 3.

²⁷³ Vgl. Becker et al., Zukunft der Unternehmensdaten, 2024, S. 8.

²⁷⁴ Vgl. Bronner, KIR 2024, 55, 62; Müller, EuZ 2022, S. A 15.

²⁷⁵ Vgl. Müller, EuZ 2022, S. A. 15.

Überprüfungen zu Unsicherheiten führen und den Aspekt der Rechtssicherheit beeinträchtigen. Bereits jetzt sehen sich Unternehmen, die Hochrisiko-KI-Systeme entwickeln oder betreiben, hohen Anforderungen ausgesetzt, welche sowohl technisch als auch organisatorisch als anspruchsvoll eingestuft werden.²⁷⁶

Zu hohe Anforderungen können die Innovationsförderung hemmen, da Unternehmen neue Technologien möglicherweise aufgrund zu komplexer Anforderungen langsamer vorantreiben. Das Ziel der Verordnung, Innovation und die Wettbewerbsfähigkeit der Unternehmen zu stärken, kann hierdurch potenziell gefährdet werden.

4.3.2 Diskriminierung

Im Zusammenhang mit dem Einsatz von KI wird vermehrt betont, dass KI-Technologien die Möglichkeit bieten, subjektive Einflüsse zu minimieren und durch objektivere Entscheidungen Diskriminierungen zu vermeiden.²⁷⁷ Eine objektive KI-Entscheidung ist jedoch nur bei einem vollumfänglichen Zugriff auf qualitativ hochwertige Datenbestände zu gewährleisten. Kann dies nicht erfüllt werden, wird die hierdurch entstehende Gefahr der Voreingenommenheit aus informationstechnischer und juristischer Sicht als „Bias“ bezeichnet.²⁷⁸

Im Rahmen der Verordnung findet diese Thematik ebenfalls Berücksichtigung. Bereits in Erwgr. 27 KI-VO thematisiert der Gesetzgeber, dass Hochrisiko-KI-Systeme so entwickelt werden müssen, dass sie keine diskriminierenden Auswirkungen haben. Art. 10 und 15 KI-VO legen zudem besonderen Wert auf die Qualität der Daten und fordern, dass die KI-Systeme ausschließlich mit verzerrungsfreien Daten trainiert werden (Art. 10 Abs. 2 lit. f KI-VO).

Was zunächst als wesentlicher Vorteil erscheint, birgt für Unternehmen einen erheblichen Aufwand im Bereich der Datenaufarbeitung und -prüfung. Die hohen Anforderungen an die Transparenz umfassen auch die Nachvollziehbarkeit von KI-Entscheidungen (Art. 12 KI-VO). Als besonders herausfordernd erweist sich das sogenannte „Black-Box-Problem“: Auch wenn KI-Systeme mit bekannten und qualitativ hochwertigen Daten trainiert werden, sind die Entscheidungen im Einzelfall für Menschen nicht mehr nachvollziehbar.²⁷⁹ Die Nachvollziehbarkeit

²⁷⁶ Vgl. *Binder/Egli*, MMR 2024, 626, 629.

²⁷⁷ Vgl. *Dahm/Zehnder*, *Moderne Personalführung mit Künstlicher Intelligenz*, S. 47; *Knappertsbusch/Gondlach*, *Arbeitswelt und KI 2030*, S. 75.

²⁷⁸ Vgl. *Herbst/Panic*, *KI-Recht praktisch erklärt*, S. 23; *Pohlmann et al.*, *ZVersWiss*, 135, 137.

²⁷⁹ Vgl. *Dahm/Zehnder*, *Moderne Personalführung mit Künstlicher Intelligenz*, S. 65; *Ulbricht et al.*, *Praxishandbuch KI und Recht*, S. 100.

von KI-Entscheidungen und die Datenerhebung, so wie sie in Art. 10 KI-VO gefordert wird, sind somit mit einem erheblichen technischen Aufwand verbunden. Unternehmen, insbesondere KMU und Start-ups, sind daher dazu angehalten, neue Programme zu entwickeln oder einzukaufen, damit sie den Anforderungen der KI-VO hinreichend nachkommen können.

Aufgrund der dargelegten Schwierigkeiten, Verzerrungen und Diskriminierungen zuverlässig zu erkennen und zu vermeiden, erhöht sich das Risiko, dass Unternehmen die mit einem KI-System verbundenen Risiken nicht hinreichend kontrollieren können und somit die Vorgaben der KI-VO nicht vollständig erfüllen.

In diesen Fällen haben Unternehmen mit hohen Sanktionierungen gemäß Art. 99 KI-VO zu rechnen. Neben finanziellen Strafen können Unternehmen mit Reputationsschäden konfrontiert werden, die negative Auswirkungen auf die Marktstellung haben.²⁸⁰

4.3.3 Umsetzungsfristen

Mit der KI-VO gehen weitreichende Anforderungen und unter Umständen hohe Sanktionierungen einher. Trotz der Komplexität bleibt den Unternehmen nur begrenzt Zeit für die Umsetzung, da erste Vorgaben bereits nach sechs Monaten in Kraft treten (Art. 113 lit. a KI-VO). Unternehmen sind daher angehalten, ihre Strategien und internen Prozesse zeitnah an die Vorgaben der KI-VO anzupassen. Dieser Umstand hat insbesondere Auswirkungen auf die Governance-Funktionen der Unternehmen und erzeugt erheblichen Handlungsdruck. Neben der Drucksituation und der fehlenden Zeit für eine hinreichende Vorbereitung, besteht das Risiko von Fehlern sowie einer unzureichenden Erfüllung der Vorschriften aus der KI-VO. Dies kann nicht nur Sanktionierungen nach sich ziehen, sondern durch die hierdurch entstehende Mehrarbeit auch zu einem erhöhten Ressourceneinsatz führen.

Hinzu kommt, dass die Verordnung zwar Regelungen hinsichtlich der Sanktionierung trifft, jedoch viele Haftungsfragen insbesondere im Zusammenhang mit Schäden, die durch KI-Systeme verursacht werden, weiterhin offen bleiben.²⁸¹ Bereits seit 2022 liegt ein erster Entwurf einer Richtlinie zur außervertraglichen

²⁸⁰ Vgl. *Protschky et al.*, WuM 2024, o.S.

²⁸¹ Vgl. *Chibanguza/Steege*, NJW 2024, 1769, 1775; *Martini/Wendehorst/Rusche-meier*, Art. 6 Rn. 20; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 160.

zivilrechtlichen Haftung im Kontext von KI vor, die jedoch bisher noch nicht verabschiedet wurde.²⁸²

Darüber hinaus bleibt die Gültigkeit anderer bestehender Rechtsvorschriften durch die KI-VO unberührt, was insbesondere die Anforderungen der DSGVO erneut in den Fokus rückt.²⁸³ Durch den Einsatz von KI-Systemen werden große Mengen sensibler Daten verwendet, wodurch potentiell Datenschutzverletzungen auftreten können. Unternehmen sind demnach dazu angehalten, mit dem Einsatz von KI nicht nur die Anforderungen der KI-VO zu prüfen, sondern auch die Konformität mit den bereits bestehenden Gesetzen (z.B. DSGVO, Data Act und NIS-2-RL) sicherzustellen.²⁸⁴ Durch diesen Umstand und der Tatsache, dass einige rechtliche Fragestellungen trotz der Einführung der KI-VO weiterhin ungeklärt bleiben, gestalten sich die vorgesehenen Umsetzungsfristen für Unternehmen als besonders anspruchsvoll.

4.3.4 Ungenaue Beschreibungen

Die KI-VO beschreibt zwar ausführlich, welche Funktionen KI-Systeme erfüllen müssen und welchen Anforderungen die Akteure nachzukommen haben, lässt dabei aber konkrete Hinweise für die praktische Umsetzung weitestgehend unberücksichtigt. Hinzu kommt, dass zahlreiche wesentliche Begrifflichkeiten in der KI-VO nicht oder nur unzureichend definiert werden. Als Beispiele hierfür lassen sich sowohl die Definition eines KI-Systems in Art. 3 Nr. 1 KI-VO sowie die Begriffe Transparenz und Risikomanagement anführen. Hinsichtlich einiger Definitionen werden in der Literatur bereits erste Versuche eigener Systematisierungen vorgenommen, was zu einer zunehmenden Unsicherheit bei den Unternehmen führt, insbesondere im Hinblick auf die praktische Umsetzung der Anforderungen der KI-VO.²⁸⁵

Eine zentrale Herausforderung liegt zudem in der fehlenden Konkretisierung von technischen Standards und Rechtsbegriffen. Die KI-VO formuliert grundlegende Anforderungen – insbesondere im Hinblick auf Hochrisiko-KI-Systeme – lässt aber in vielen Fällen konkrete und klar definierte Vorgaben aus. Als Beispiel hierfür lässt sich Art. 9 KI-VO und das damit einhergehende Risikosystem benennen. Da der Gesetzgeber auf die Verpflichtung zur Einhaltung spezifischer Standards

²⁸² Vgl. Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung) v. 28.9.2022, COM (2022) 496 final.

²⁸³ Vgl. *Wybitul*, BB 2024, 2179, 2182.

²⁸⁴ Vgl. *Chibanguza/Steege*, NJW 2024, 1769, 1775; Martini/Wendehorst/*Wendehorst*, Art. 3 Rn. 21.

²⁸⁵ Vgl. Martini/Wendehorst/*Wendehorst*, Art. 3 Rn. 51 f.

verzichtet, erhalten Anbieter einen größeren Ermessensspielraum bei der Umsetzung der Anforderungen an das Risikomanagement.²⁸⁶ Auch Art. 13 KI-VO stellt hinreichende Anforderungen an das Maß der Transparenz von Hochrisiko-KI-Systemen. Die Umsetzung der Anforderungen wird den Unternehmen jedoch dadurch erschwert, dass die Norm aus einer Vielzahl von unbestimmten Rechtsbegriffen besteht (z.B. „hinreichend“, „angemessen“, oder „geeignete Art“).²⁸⁷ Ein ähnliches Problem tritt bei Art. 10 KI-VO auf, der beschreibt, dass Trainings-, Validierungs- und Testdatensätze „so weit wie möglich fehlerfrei und vollständig“²⁸⁸ sein müssen, jedoch keine klaren Grenzen für diese Anforderungen ausführt.²⁸⁹

Auch in Bezug auf den Adressatenkreis der Verordnung bestehen weiterhin Unklarheiten. Durch den Umstand bedingt, dass die Anforderungen an die Risikoklassen und die Akteure gebunden sind, ist eine Abgrenzung zwischen den verschiedenen Akteuren im Rahmen der KI-VO notwendig. Die Eigenschaften von Anbietern und Betreibern schließen sich jedoch nicht gegenseitig aus, so dass sich in einigen Fällen Abgrenzungsschwierigkeiten ergeben können.²⁹⁰

Der Gesetzgeber führt an, dass gemäß Art. 111 Abs. 2 KI-VO für KI-Systeme, die bereits vor dem Inkrafttreten der KI-VO in den Verkehr gebracht oder Betrieb genommen worden sind, eine Ausnahmeregelung gilt. Dieser Ausnahmetatbestand entfällt jedoch, wenn die Systeme nach dem Inkrafttreten der KI-VO „erheblich verändert wurden“²⁹¹. Wann diese Schwelle überschritten ist, wird jedoch vom Gesetzgeber nicht weiter präzisiert.²⁹²

Diese unbestimmten Formulierungen zeigen, dass eine Vielzahl der Vorgaben der KI-VO zukünftig von Rechtsprechung, Praxisleitfäden und den Leitlinien der Kommission konkretisiert werden müssen. Mit Blick auf die ersten Umsetzungsfristen im Februar 2025 agieren Unternehmen aktuell in einer Phase der Unsicherheit.²⁹³

²⁸⁶ Vgl. Martini/Wendehorst/Braun Binder/Egli, Art. 9 Rn. 11.

²⁸⁷ Vgl. Martini/Wendehorst/Braun Binder/Egli, Art. 9 Rn. 77.

²⁸⁸ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 57.

²⁸⁹ Vgl. Ulbricht *et al.*, Praxishandbuch KI und Recht, S. 178.

²⁹⁰ Vgl. Martini/Wendehorst/Wendehorst, Art. 3 Rn. 86.

²⁹¹ Verordnung (EU) 2024/1689 vom 13. Juni 2024, S. 121.

²⁹² Vgl. Binder/Egli, MMR 2024, 626, 627.

²⁹³ Vgl. Ulbricht *et al.*, Praxishandbuch KI und Recht, S. 209.

4.3.5 Kosten- und Ressourcenaufwand

Die zuvor dargelegten Herausforderungen der KI-VO verdeutlichen, dass mit der Erfüllung der Anforderungen für Unternehmen ein hoher Ressourcen- und Kostenaufwand verbunden ist.

Auch wenn es sinnvoll erscheint, die neuen Anforderungen in bereits bestehende Prozesse zu integrieren, zieht die Erweiterung der Governance-Strukturen um die KI-spezifischen Risiken einen hohen organisatorischen Aufwand mit sich.²⁹⁴ Neben der Integration in bestehende Prozesse wird es für Unternehmen unerlässlich sein, qualifiziertes Fachpersonal einzusetzen. Der Umstand, dass Unternehmen sämtliche technische Entwicklungen und Updates berücksichtigen und sicherstellen müssen, dass diese mit den Anforderungen der KI-VO in Einklang stehen, erfordert eine kontinuierliche Überwachung und führt somit zu einem hohen Ressourcenaufwand.

Unabhängig davon, ob sich ein Unternehmen dazu entscheidet, das KI-Risiko durch bereits bestehendes Governance-Personal abzudecken oder neues Fachpersonal zu schaffen, ist einer der wesentlichen zu beachtenden Aspekte die KI-Kompetenz gemäß Art. 4 KI-VO. Bei der Vermittlung der KI-Kompetenz müssen die Unternehmen anwenderspezifisch und zielgruppengerecht vorgehen. Es ist erforderlich, dass das Personal nicht nur über ausreichende Fachkenntnisse im Bereich der KI verfügt, sondern auch ständig auf dem neuesten Stand bezüglich rechtlicher und technologischer Entwicklungen bleibt.²⁹⁵ Neben den Investitionen in neue technische Ausstattung und der Einführung neuer Systeme stellt somit auch der Einsatz von KI-Personal und die Weiterbildungsmaßnahmen einen nicht unerheblichen Kostenfaktor dar.

Trotz der vorgesehenen Erleichterungen für KMU und Start-ups an zahlreichen Stellen der Verordnung könnte diese Regelung in der Praxis schnell zu einer erheblichen Belastung führen.

²⁹⁴ Vgl. *Protschky et al.*, WuM 2024, o.S.

²⁹⁵ Vgl. *Klos/Taylan*, CCZ 2024, 205, 210.

5 Handlungsempfehlungen und Ausblick

Mit Blick auf die ersten Umsetzungsfristen im Februar 2025 wird deutlich, dass der Handlungsbedarf für Unternehmen bereits seit Veröffentlichung der KI-VO im Amtsblatt besteht. Die Gliederung des Kapitels C verdeutlicht die Schritte, die von den Unternehmen zur Erfüllung der Anforderungen der KI-VO erforderlich sind. Diese lassen sich im Wesentlichen in drei Abschnitte unterteilen.

Als erstes sollten Unternehmen eine Vorabprüfung durchführen. Im Rahmen dieser Vorabprüfung wird die Eröffnung des Anwendungsbereichs geprüft, um somit festzustellen, ob das Unternehmen als Adressat der KI-VO gilt. Kann dies bejaht werden, sind im Anschluss hieran vorbereitende Maßnahmen zu treffen. Hierzu zählt, dass ein Unternehmen die Rollen und Verantwortlichkeiten im Hinblick auf die Implementierung der KI-VO festlegt, eine Einbindung des BR/ IT-Ausschusses erfolgt, Melde- und Überwachungsmaßnahmen definiert werden (u.a. in Form einer KI-Richtlinie) und angemessene Schulungs- sowie Sensibilisierungsmaßnahmen getroffen werden.

Im Anschluss an die vorbereitenden Maßnahmen sollten sodann die Umsetzungsmaßnahmen und somit die tiefergehenden Pflichten in Bezug auf KI-Systeme ergriffen werden. Hierbei empfiehlt es, sich zunächst ein KI-Verzeichnis zu erstellen, an das sich die Identifizierung der Rollen und Systemverantwortlichen sowie eine Risikoklassifizierung der Systeme anschließen. Aus der KI-VO sollten die für die Akteure geltenden Pflichten herausgearbeitet und in einem Pflichtenkatalog niedergeschrieben werden. Abschließend müssen diese Pflichten den jeweiligen KI-Systemen im KI-Verzeichnis zugeordnet werden.

Unter Berücksichtigung der Umsetzungsfristen sind der Ausbau der KI-Kompetenz sowie die Identifizierung verbotener KI-Praktiken im Unternehmen vorrangige Maßnahmen.²⁹⁶

Für den Austausch zwischen den verschiedenen Branchen bietet sich für Unternehmen der Beitritt zum sogenannten KI-Pakt an. Dieser wurde von der Bundesregierung ins Leben gerufen und zielt darauf ab, die frühzeitige Umsetzung der KI-Anforderungen zu fördern. Zudem ermöglicht er Unternehmen, sich hinsichtlich ihrer Vorgehensweise auszutauschen und bewährte Verfahren sowie etablierte Richtlinien zu teilen.²⁹⁷

Unternehmen können sich zudem darauf einstellen, dass in naher Zukunft Leitlinien durch die EU-Kommission erlassen werden. Diese sollen gemäß Art. 96 KI-

²⁹⁶ Vgl. *Klos/Taylan*, CCZ 2024, 205, 211; *Ulbricht et al.*, Praxishandbuch KI und Recht, S. 209; *Wybitul*, BB 2024, 2179, 2182.

²⁹⁷ Vgl. *Vertretung in Deutschland*, AI Pact, o.S.

VO die in der Verordnung getroffenen Anforderungen praxisnah ausführen und den Unternehmen als Hilfestellung dienen. Die Leitlinien sollen als Orientierungshilfe fungieren und könnten in Form von Checklisten und Schritt-für-Schritt-Anleitungen bereitgestellt werden.²⁹⁸ Da es sich bei den Leitlinien um kein in Art. 288 AEUV benannten Rechtsakt handelt, entfalten die Leitlinien keine Rechtsverbindlichkeit.²⁹⁹ Aufgrund der zahlreichen Unklarheiten bezüglich der Begrifflichkeiten und Anforderungen ist jedoch davon auszugehen, dass diese von vielen Unternehmen als hilfreich erachtet und bei der Implementierung berücksichtigt werden.

Auch Art. 56 KI-VO sieht die Schaffung von Praxisleitfäden vor, damit die in Art. 53 und 55 KI-VO genannten Pflichten, welche GPAI-Modelle umfassen, weiter ausgeführt und konkretisiert werden. Die Leitfäden sollen dabei primär von den Anbietern der entsprechenden KI-Modelle erstellt werden. Auch Erwgr. 117 KI-VO unterstreicht die Bedeutung dieser Handreichungen.

²⁹⁸ Vgl. *Deutscher Bundestag*, Positionspapier, S. 5.

²⁹⁹ Vgl. Martini/Wendehorst/*Hartmann*, Art. 96 Rn. 1 f.

6 Fazit

Im Rahmen dieser Masterarbeit wurde die KI-VO sowie die daraus resultierenden Anforderungen für Unternehmen analysiert. Die Untersuchung hat gezeigt, dass mit der Einführung der Verordnung das erste umfassende EU-weite Regelwerk für KI geschaffen wurde. Ziel dieser Verordnung ist es, einen einheitlichen Rechtsrahmen zu etablieren, der den Binnenmarkt fördert, eine menschenzentrierte und vertrauenswürdige KI sicherstellt und ein hohes Schutzniveau in Bezug auf die Gesundheit, Sicherheit und die Grundrechte anstrebt.

Mit der Einführung der KI-VO gehen viele und – insbesondere für Hochrisiko-KI-Systeme im Sinne von Art. 6 iVm. Anhang III KI-VO – hohe Anforderungen einher. Angesichts der kurzen Umsetzungsfristen gemäß Art. 113 iVm. 111 KI-VO stehen Unternehmen bereits jetzt unter Druck, diese Vorgaben zeitnah zu erfüllen. Daher ist eine frühzeitige Vorbereitung und Implementierung unerlässlich.

Damit die Einhaltung der Vorschriften hinreichend sichergestellt werden kann, erweist es sich als entscheidend, zunächst die internen Rollen und Verantwortlichkeiten klar zu definieren. Der Aufbau einer effektiven KI-Governance erfordert, dass alle relevanten Stakeholder eingebunden sind und eine umfassende Bestandsanalyse der bestehenden Unternehmensstrukturen durchgeführt wird. Hierbei sollten zum einen die bestehenden Governance- und IT-Prozesse berücksichtigt, als auch die bestehenden KI-Systeme und geplanten KI-Initiativen identifiziert werden. Unternehmen müssen eine KI-Strategie entwickeln, die eine klare Positionierung zu den neuen Technologien bietet und für alle Mitarbeitenden zugänglich und hinreichend nachvollziehbar ist.

Mit Blick auf die Umsetzungsfristen sollte der Schwerpunkt zunächst auf der KI-Kompetenz gemäß Art. 4 KI-VO und den verbotenen Praktiken gemäß Art. 5 KI-VO liegen. Gleichzeitig ist es entscheidend, auch für alle anderen Risikokategorien die Anforderungen zu kennen. Als eine zusätzliche Herausforderung stellt sich die derzeit vorhandene Rechtsunsicherheit heraus, welche durch unbestimmte Regelungen in der KI-VO sowie der noch ausstehenden Leitlinien der Europäischen Kommission bedingt ist. Während auf weitere Handreichungen gewartet wird, sollten Unternehmen auch die Relevanz der anderen einschlägigen Gesetze sowie die rechtlichen und technologischen Entwicklungen nicht aus den Augen verlieren.

Ziel dieser Arbeit ist es, herauszuarbeiten, ob die Entwicklungen im Bereich der KI eine eigenständige Governance erfordern oder ob die Anforderungen der KI-VO in die bestehenden Strukturen integriert werden können. Die Untersuchung hat gezeigt, dass die Entwicklung einer KI-Governance zwingend erforderlich ist. Zudem setzt sich die Governance eines Unternehmens aus unterschiedlichen

Einheiten zusammen, die nur durch ein koordiniertes Zusammenspiel einen hinreichenden Schutz des Vorstands gewährleisten können (siehe Abbildung 2). Damit dieser Schutz auch weiterhin aufrechterhalten werden kann und die Synergien innerhalb des Unternehmens optimal genutzt werden können, ist die KI-Governance in bereits bestehende Strukturen zu integrieren. Bestehende Prüfungsstandards können dabei als Orientierung dienen, da sie bereits wesentliche Elemente enthalten, die auch für KI-Systeme von Relevanz sind. Zudem geht auch aus der KI-VO hervor, dass Doppelarbeiten vermieden werden sollen und bereits etablierte Maßnahmen zur Erfüllung der Anforderungen aus der KI-VO genutzt werden können (z.B. Art. 27 Abs. 2 KI-VO).

Ein weiterer Schwerpunkt der Arbeit liegt auf der Bewertung der Anforderungen, die sich aus der KI-VO für Unternehmen ergeben. Mit Hilfe der Ausführungen in dieser Arbeit konnte gezeigt werden, dass die KI-VO mit dem einheitlichen Rechtsrahmen Rechtssicherheit nach sich zieht und ein hohes Schutzniveau gewährleisten soll. Der risikobasierte Ansatz verfolgt das Ziel einer differenzierten Regulierung und einer damit einhergehenden Innovationsförderung. Jedoch konnte im Rahmen der Arbeit auch herausgearbeitet werden, dass die hohen Anforderungen die Gefahr einer Überforderung der Unternehmen bergen, die wiederum eine Hemmung der Innovationskraft nach sich ziehen kann. Auch die enge Schnittstelle zur DSGVO sowie die mit KI-Technologien einhergehenden Risiken (z.B. Verzerrungen und daraus resultierende Diskriminierungen) führen zu zusätzlichen Datenanforderungen. Verstöße gegen diese Vorgaben ziehen gemäß Art. 99 KI-VO erhebliche Sanktionen nach sich. Hierdurch bedingt und unter Berücksichtigung der kurzen Umsetzungsfristen sehen sich Unternehmen somit zunehmend einem hohen Druck ausgesetzt. Die Bemühungen, allen Anforderungen in der vorgegebenen Zeit gerecht zu werden, zieht einen hohen Kosten- und Ressourcenaufwand nach sich. Insbesondere KMU und Start-ups sehen sich hierdurch vor große Herausforderungen gestellt.

Angesichts der bisherigen Rechtsunsicherheit und der fehlenden Orientierungshilfen bleibt fraglich, ob die mit der KI-VO verfolgten Ziele in der Praxis realisiert werden können. Es ist nicht auszuschließen, dass das Vorgehen der Gesetzgebung die Zielerreichung selbst hemmen könnte.

Die Ergebnisse dieser Arbeit knüpfen an den bisherigen Stand der Forschung an und gehen vereinzelt über diesen hinaus. Aufgrund der erst am 12.07.2024 im Amtsblatt der EU veröffentlichten Verordnung gibt es bisher keine umfangreichen Ausarbeitungen hinsichtlich der Interpretation der Governance-Anforderungen. Diese Arbeit leistet daher einen Beitrag zur Schließung der Lücke und dient Unternehmen als Leitfaden und Orientierungshilfe für die Implementierung der KI-VO.

Aufgrund der bisher fehlenden Ausführungen seitens der Kommission und der begrenzten Literatur konnte in dieser Arbeit nur ein erster Rahmen zum Vorgehen erarbeitet werden. Da für das Jahr 2025 weitere Leitlinien und auch Kommentierungen erwartet werden, kann angenommen werden, dass Unternehmen im Laufe des Jahres weitere detaillierte Handreichungen und Praxisleitfäden zur Verfügung stehen werden. Konkrete Handlungsempfehlungen und Vorgehensweisen werden sich zudem aus zukünftiger Rechtsprechung und im Laufe der Zeit anhand von Erfahrungswerten und daraus resultierender Praxisleitfäden ergeben.

In der Gesamtschau bietet diese Arbeit eine Grundlage für die Orientierung im Umgang mit den Vorgaben aus der KI-VO. Trotz der bisherigen Unklarheiten empfiehlt es sich, dass Unternehmen bereits jetzt mit der Umsetzung beginnen, um die Einhaltung der Pflichten aus der KI-VO sicherstellen zu können. Die in dieser Arbeit herausgearbeiteten Vorgehensweisen und Empfehlungen können dabei als erste Hilfestellung dienen, da die von der Kommission angekündigten Leitlinien möglicherweise nicht rechtzeitig zur Verfügung stehen werden.

Literatur

- Ammann, Thorsten/Pohle, Jan*, KI-Verordnung – Was bisher geschah und jetzt zu tun ist, in: *CB*, 2024, S. 137-1441 (zit.: *Ammann/Pohle, CB* 2024, S.).
- Becker, Axel/Gruber, Walter/Heuter, Henning (Hrsg.)*, Handbuch MaRisk, Neue Anforderungen an das Risikomanagement in der Bankpraxis, 4. Auflage, Berlin 2024 (zit.: *Becker et al., HdB-MaRisk*, S.).
- Bierekoven, Christiane*, Die neue KI-Verordnung – Teil 1, Überblick über Systematik, Konzept, Governance und Begrifflichkeiten, in: *ITRB*, 2024, S. 264-269 (zit.: *Bierekoven, ITRB* 2024, S.).
- Braun Binder, Nadja/Egli, Catherine*, Umgang mit Hochrisiko-KI-Systemen in der KI-VO, Strenge Anforderungen der Art. 8-15 KI-VO, in *MMR*, 2024, S. 626-630 (zit.: *Binder/Egli, MMR* 2024, S.).
- Bronner, Pascal*, Risikoklassifizierung, Risikobewertung und Risikominimierung nach der KI-Verordnung, in: *KIR*, 2024, S. 55-62 (zit.: *Bronner, KIR* 2024, S.).
- Brune, Gunnar*, Künstliche Intelligenz heute, Anwendungen aus Wirtschaft, Medizin und Wissenschaft, 1. Auflage, Wiesbaden 2022 (zit.: *Brune, Künstliche Intelligenz heute*, S.).
- Buchalik, Barbara/Gehrmann, Mareike Christine*, Von Nullen und Einsen zu Paragraphen: Der AI Act, ein Rechtscode für Künstliche Intelligenz. Der horizontale und risikobasierte Ansatz für Produktsicherheitsaspekte von KI-Systemen und Allzweck-KI, in: *CR*, 2024, S. 145-153 (zit.: *Buchalik/Gehrmann, CR* 2024, S.).
- Bülchmann, Oliver*, Der KI-Act als komplexe Governance-Herausforderung, Ein proaktives Implementierungsmodell, Band 14, 2022, S. 407-414 (zit.: *Bülchmann, Der KI-Act als komplexe Governance-Herausforderung*, S.).
- Dahm, Markus H./Zehnder, Valentin*, Moderne Personalführung mit Künstlicher Intelligenz, Chancen und Risiken, 1. Auflage, Wiesbaden 2023 (zit.: *Dahm/Zehnder, Moderne Personalführung mit Künstlicher Intelligenz*, S.).
- Ebers, Martin/Streitböcker, Chiara*, Die Regulierung von Hochrisiko-KI-Systemen in der KI-Verordnung, in: *RDi*, 2024, S. 393-400 (zit.: *Ebers/Streitböcker, RDi* 2024, S.).
- Ertel, Wolfgang*, Grundkurs Künstliche Intelligenz, Eine praxisorientierte Einführung, 5. Auflage, Wiesbaden 2021 (zit.: *Ertel, Grundkurs Künstliche Intelligenz*, S.).

- Heinze, Christian/Sorge, Christoph/Specht-Riemenschneider, Louisa*, Das Recht der Künstlichen Intelligenz, Eine Skizze, in: KIR, 2024, S. 11-15 (zit.: *Heinze et al.*, KIR 2024, S.).
- Herbst, Fabian/Panic, Stefan*, KI-Recht praktisch erklärt, Der Leitfaden zum AI-Act und zu sonstigen Regelungen, 1. Auflage, Wien 2024 (zit.: *Herbst/Panic*, KI-Recht praktisch erklärt, S.).
- Horstmann, Jan*, KI-VO und Datenschutz: Überblick und ausgewählte Fragen, in: ZD-Aktuell, 2024, 01580 (zit.: *Horstmann*, ZD-Aktuell 2024, 01580).
- Kindshofer, Aurea*, KI-VO als datenschutzrechtliche Herausforderung, Theoretische und praktische Einführung mit Lösungsmöglichkeiten für DSB, in: ZD, 2024, S. 673-678 (zit.: *Kindshofer*, ZD 2024, S.).
- Klos, Christian/Taylan, Ramazan*, Von der Theorie zur Praxis: Die EU-KI-Verordnung effektiv umsetzen, in: CCZ, 2024, S. 205-211 (zit.: *Klos/Taylan*, CCZ 2024, S.).
- Knappertsbusch, Inka/Gondlach, Kai (Hrsg.)*, Arbeitswelt und KI 2030, Herausforderungen und Strategien für die Arbeit von morgen, 1. Auflage, Wiesbaden 2021 (zit.: *Knappertsbusch/Gondlach*, Arbeitswelt und KI 2030, S.).
- Kreipl, Claudia*, Verantwortungsvolle Unternehmensführung, Corporate Governance, Compliance Management und Corporate Social Responsibility, 1. Auflage, Wiesbaden 2020 (zit.: *Kreipl*, Verantwortungsvolle Unternehmensführung, S.).
- Kreutzer, Ralf T.*, Künstliche Intelligenz verstehen, Grundlage – Use Cases – unternehmenseigene KI-Journey, 2. Auflage, Wiesbaden 2023 (zit.: *Kreutzer*, Künstliche Intelligenz verstehen, S.).
- Krimphove, Dieter*, Die neue europäische KI-Verordnung und ihre Anforderungen an Unternehmen, in: ZWH, 2024, S. 249-253 (zit.: *Krimphove*, ZWH 2024, S.).
- Krönke, Christoph*, Das europäische KI-Gesetz: Eine Verordnung mit Licht und Schatten, in: NVwZ, 2024, S. 529-534 (zit.: *Krönke*, NVwZ 2024, S.).
- Steinrötter, Björn/Markert, Jette*, Datenbezogene Vorgaben der KI-Verordnung, in: RDi, 2024, S. 400-405 (zit.: *Steinrötter/Markert*, RDi 2024, S.).
- Martini, Mario/Wendehorst, Christiane*, KI-VO Kommentar, Verordnung über künstliche Intelligenz, 1. Auflage, München 2024 (zit.: *Martini/Wendehorst/Bearbeiter*, Art. Rn.).

- Müller, Angela*, Der Artificial Intelligence Act der EU: Ein risikobasierter Ansatz zur Regulierung von Künstlicher Intelligenz – mit Auswirkungen auf die Schweiz, in: *EuZ*, 2022, S. A 1-A 25 (zit.: *Müller*, *EuZ* 2022, S.).
- Müller-Peltzer, Philipp/Schneider, Sebastian*, Die geplante KI-Verordnung der EU, Rechtliche Herausforderungen für regulierte Branchen im B2C Bereich, in: *REL*, 2022, S. 9-12 (zit.: *Müller-Peltzer/Schneider*, *REL* 2022, S.).
- Münchener Kommentar zum Aktiengesetz, Münchener Kommentar zum Aktiengesetz, Band 2, *Goette, Wulf/ Habersack, Mathias/ Kalss, Susanne (Hrsg.)*, 6. Auflage, München 2024 (zit.: *MüKoAktG/Bearbeiter*, § Rn.).
- Münchener Kommentar zum Aktiengesetz, Münchener Kommentar zum Aktiengesetz, Band 3, *Goette, Wulf/ Habersack, Mathias/ Kalss, Susanne (Hrsg.)*, 6. Auflage, München 2024 (zit.: *MüKoAktG/Bearbeiter*, § Rn.).
- Pohlmann, Petra/Vossen, Gottfried/ Everding, Jan/ Scheiper, Johann*, Künstliche Intelligenz, Bias und Versicherungen – Eine technische und rechtliche Analyse, in: *ZVersWiss*, 2022, S. 135-175 (zit.: *Pohlmann et al.*, *ZVersWiss*, S.).
- Protschky, Dominik/Schüll, Moritz/ Urbach, Nils*, Governance von künstlicher Intelligenz – Eine Methode zur Transformation vorhandener Governance-Mechanismen in Unternehmen, in: *WuM*, 2024 (zit.: *Protschky et al.*, *WuM* 2024, o.S.).
- Reese, Hendrik*, KI-Governance: Implementierung im Unternehmen, in: *BB*, 2024, S. 1515-1519 (zit.: *Reese*, *BB* 2024, S.).
- Schackmann, Valentin/ Ziegler, Werner (Hrsg.)*, Praxisorientiertes Managementwissen, Die Existenz von Unternehmen in schwierigen Zeiten, 1. Auflage, Wiesbaden 2024 (zit.: *Schackmann/ Ziegler*, *Praxisorientiertes Managementwissen*, S.).
- Schneider, Moritz*, Künstliche Intelligenz am Arbeitsplatz, in: *ARP*, 2023, S. 194-197 (zit.: *Schneider*, *ARP* 2023, S.).
- Seyffarth, Malte*, Die KI-Verordnung der EU: Was KI verwendende Unternehmen nun wissen sollten, in: *GWR*, 2024, S. 173-175 (zit.: *Seyffarth*, *GWR* 2024, S.).
- Soong, Eric S.*, Die Implementierung eines KI Governance Frameworks, in: *CNL*, 2024, S. 12 (zit.: *Soong*, *CNL* 2024, S.).
- Taulli, Tom*, Grundlagen der Künstlichen Intelligenz, 1. Auflage, Monrovia 2022 (zit.: *Taulli*, *Grundlagen der Künstlichen Intelligenz*, S.).

- Ulbricht, Carsten/Brajovic, Danilo/Duhme, Torsten/Hawighorst, Jessica/Huber, Marco F./Iber, Varinia/Nemec, Carolin*, Praxishandbuch KI und Recht, 1. Auflage, Freiburg 2024 (zit.: *Ulbricht et al.*, Praxishandbuch KI und Recht, S.).
- Voigt, Paul/Hullen, Hils*, Handbuch KI-Verordnung, FAQ zum EU AI Act, 1. Auflage, Berlin 2024 (zit.: *Voigt/Hullen*, HdB-KI-Verordnung, S.).
- von Welser, Marcus*, Die KI-Verordnung – ein Überblick über das weltweit erste Regelwerk für künstliche Intelligenz, in: GRUP-Prax, 2024, S. 485-488 (zit.: *von Welser*, GRUP-Prax 2024, S.).
- Wennker, Phil*, Künstliche Intelligenz in der Praxis, Anwendungen in Unternehmen und Branchen: KI wettbewerbs- und zukunftsorientiert einsetzen, 1. Auflage, Wiesbaden 2020 (zit.: *Wennker*, Künstliche Intelligenz in der Praxis, S.).
- Witteler, Michael/Moll, Lucas*, Künstliche Intelligenz am Arbeitsplatz – Datenschutz und Rechte des Betriebsrats, in: NZA, 2023, S. 327-333 (zit.: *Witteler/Moll*, NZA 2023, S.).
- Wybitul, Tim*, Welche Pflichten haben Betreiber von Hochrisiko-KI-Systemen nach der EU-KI-Verordnung? Überblick, Handlungsempfehlungen und Checkliste, in: BB, 2024, S. 2179-2183 (zit.: *Wybitul*, BB 2024, S.).

Internetquellen

- Becker, Mark/Dabe, Carl Heinz/Peskes, Markus/Reinking, Ernst* (2024), Zukunft der Unternehmensdaten: Chancen und Herausforderungen von KI-Anwendungen im Spannungsfeld der Corporate Governance, IUCF Working Paper (05/2024), <https://hdl.handle.net/10419/287730> [Zugriff 20.12.2024] (zit.: *Becker et al.*, Zukunft der Unternehmensdaten, 2024, S.).
- Berwanger, Jörg* (o.J.), Business Judgement Rule, <https://wirtschaftslexikon.gabler.de/definition/business-judgement-rule-53987> (o.J.) [Zugriff 07.01.2025] (zit.: *Berwanger*, Business Judgement Rule, o.S.).

- Bitkom* (2024), Umsetzungsleitfaden zur KI-Verordnung (EU) 2024/1689, <https://www.bitkom.org/sites/main/files/2024-10/241028-bitkom-umsetzungsleitfaden-ki.pdf> (29.10.2024) [Zugriff 21.01.2025] (zit.: *Bitkom*, Umsetzungsleitfaden zur KI-Verordnung, 2024, S.).
- DCGK* (2022), Deutscher Corporate Governance Kodex in der Fassung vom 28. April 2022, https://www.dcgk.de/files/dcgk/usercontent/de/download/kodex/220627_Deutscher_Corporate_Governance_Kodex_2022.pdf (2022) [Zugriff 20.12.2024] (zit.: *DCGK*, 2022, S.).
- Deloitte* (2024), EU AI Act: Das KI-Gesetz der Europäischen Union, Einzelheiten und Hintergründe zu den Umsetzungsanforderungen, <https://www.deloitte.com/de/de/issues/innovation-ai/european-ai-act.html> (18.10.2024) [Zugriff 09.01.2025] (zit.: *Deloitte*, EU AI Act, 2024, o.S.).
- Die Bundesregierung* (2024), AI Act verabschiedet, Einheitliche Regeln für Künstliche Intelligenz in der EU, <https://www.bundesregierung.de/breg-de/themen/digitalisierung/kuenstliche-intelligenz/ai-act-2285944> (22.05.2024) [Zugriff 21.01.2025] (zit.: *Bundesregierung*, AI Act verabschiedet, 2024, o.S.).
- Die Bundesregierung* (o.J.), Zukunftsthema KI, Fortschritte Künstlicher Intelligenz für unser Land nutzen, <https://www.bundesregierung.de/breg-de/aktuelles/bundesregierung-staerkt-ki-2224174> (o.J.) [Zugriff 21.01.2025] (zit.: *Bundesregierung*, Zukunftsthema KI, o.S.).
- Europäische Kommission* (o.J.), Künstliche Intelligenz – Exzellenz und Vertrauen, Vertrauenswürdige künstliche Intelligenz (KI), https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_de (o.J.) [Zugriff 08.01.2025] (zit.: *Europäische Kommission*, Künstliche Intelligenz, o.S.).
- Europäisches Parlament* (2020), Was ist künstliche Intelligenz und wie wird sie genutzt?, <https://www.europarl.europa.eu/topics/de/article/20200827STO85804/was-ist-kunstliche-intelligenz-und-wie-wird-sie-genutzt> (14.09.2020) [Zugriff 24.11.2024] (zit.: *Europäisches Parlament*, Was ist künstliche Intelligenz und wie wird sie genutzt? 2020, o.S.).
- Deutscher Bundestag* (o.J.), Positionspapier, Die Forderung der deutschen Wirtschaft zur Umsetzung der KI-Verordnung, <https://www.lobbyregister.bundestag.de/media/31/bf/298808/Stellungnahme-Gutachten-SG2406110018.pdf> (o.J.) [Zugriff 02.01.2025] (zit.: *Deutscher Bundestag*, Positionspapier, S.).

- Heid* (o.J.), Daten und Datenverarbeitung als Fundament für den Einsatz von KI, <https://www.ki-wissens-und-weiterbildungszentrum.de/knowledge-pool/daten-und-datenverarbeitung-als-fundament-fur-den-einsatz-von-ki/> (o.J.) [Zugriff 06.12.2024] (zit.: *Heid*, Daten und Datenverarbeitung, o.S.).
- Heidrich Rechtsanwälte* (o.J.), KI Richtlinie erstellen, <https://ki-kanzlei.de/ki-richtlinie> (o.J.) [Zugriff 15.01.2025] (zit.: *Heidrich Rechtsanwälte*, KI Richtlinie, o.S.).
- IBM* (o.J.), Was ist maschinelles Lernen (ML)?, <https://www.ibm.com/de-de/topics/machine-learning> (o.J.) [Zugriff 24.11.2024] (zit.: *IBM*, Was ist maschinelles Lernen? o.S.).
- IBM* (2023), Was ist KI-Governance? <https://www.ibm.com/de-de/topics/ai-governance#:~:text=Die%20KI%2DGovernance%20umfasst%20Überwachungsmechanismen,gleichzeitig%20Innovation%20und%20Vertrauen%20fördern> (28.11.2024) [Zugriff 27.11.2024] (zit.: *IBM*, Was ist KI-Governance? o.S.).
- IDW* (o.J.), IDW Verlautbarungen, <https://www.idw.de/idw/idw-verlautbarungen/?tab=search&query=IDW+PS+820> (o.J.) [24.12.2024] (zit.: *IDW*, IDW Verlautbarungen, S.).
- ISO* (o.J.), Standards, <https://www.iso.org/standards.html> (o.J.) [Zugriff 06.01.2025] (zit.: *ISO*, Standards, o.S.).
- Lugowski, Raphael* (2024), Rahmen-Betriebsvereinbarung KI – Darauf ist zu achten, <https://betriebsrat-kanzlei.de/rahmen-betriebsvereinbarung-ki-darauf-ist-zu-achten/> (13.10.2024) [Zugriff 30.12.2024] (zit.: *Lugowski*, Rahmen-Betriebsvereinbarung KI, 2024, o.S.).
- OECD* (2024), G20/OECD-Grundsätze der Corporate Governance 2023, <https://doi.org/10.1787/0dc0b93c-de> (06.07.2024) [Zugriff 29.11.2024] (zit.: *OECD*, G20/OECD, 2024, S.).
- Spitznagel, Anna* (2024), Vertrauenswürdige KI und KI Governance im Finanzwesen, <https://live.handelsblatt.com/vertrauenswuerdige-ki-und-ki-governance-im-finanzwesen/> (22.08.2024) [Zugriff 29.12.2024] (zit.: *Spitznagel*, Vertrauenswürdige KI, 2024, o.S.).

Vertretung in Deutschland (2024), Mehr als einhundert Unternehmen unterzeichnen europäischen KI-Pakt, https://germany.representation.ec.europa.eu/news/mehr-als-einhundert-unternehmen-unterzeichnen-europaischen-ki-pakt-2024-09-25_de (25.08.2024) [Zugriff 20.01.2025] (zit.: *Vertretung in Deutschland*, Mehr als einhundert Unternehmen unterzeichnen europäischen KI-Pakt, 2024, o.S.).

Vertretung in Deutschland (2024), KI-Gesetz tritt in Kraft, https://germany.representation.ec.europa.eu/news/ki-gesetz-tritt-kraft-2024-08-01_de (01.08.2024) [Zugriff 20.01.2025] (zit.: *Vertretung in Deutschland*, KI-Gesetz tritt in Kraft, 2024, o.S.).

Folgende Bände sind bisher in dieser Reihe erschienen:

Band 1 (2020)

Tim Jesgarzewski

[Wirtschaftsverwaltungsrecht: Schwerpunkt Gewerberecht und Anwendungsfälle](#)

ISBN (Print) 978-3-89275-210-3 ISSN (Print) 2748-6869

ISBN (eBook) 978-3-89275-211-0 ISSN (eBook) 2748-6877

Band 2 (2025)

Béatrice Grewer

[Kompensation von Ungleichgewichtslagen im Arbeitsrecht und im Verbraucherschutzrecht](#)

ISBN (Print) 978-3-89275-408-4 ISSN (Print) 2748-6869

ISBN (eBook) 978-3-89275-409-1 ISSN (eBook) 2748-6877

Band 3 (2025)

Barbara Mertes

[Verbraucherschützende Widerrufsrechte: Implikationen für Unternehmer](#)

ISBN (Print) 978-3-89275-419-3 ISSN (Print) 2748-6869

ISBN (eBook) 978-3-89275-420-6 ISSN (eBook) 2748-6877

Band 4 (2025)

Matthias Krause

[Interne Untersuchungen in Unternehmen: Rechtlicher Rahmen und Praxisprobleme](#)

ISBN (Print) 978-3-89275-425-1 ISSN (Print) 2748-6869

ISBN (eBook) 978-3-89275-426-8 ISSN (eBook) 2748-6877

Forschungsstark und praxisnah

FOM. Die Hochschule. Für Berufstätige.

FOM Hochschulzentrum
Düsseldorf

Rund 45.000 Studierende, mehr als 20 Forschungseinrichtungen und 500 Veröffentlichungen im Jahr – damit zählt die FOM zu den größten und forschungsstärksten Hochschulen Europas. Initiiert durch die Stiftung für internationale Bildung und Wissenschaft folgt sie einem klaren Bildungsauftrag: Berufstätige und Abiturienten durch qualitativ hochwertige und bezahlbare Studiengänge akademisch zu qualifizieren. Als gemeinnützige Hochschule ist die FOM nicht gewinnorientiert, sondern reinvestiert sämtliche Gewinne – unter anderem in die Lehre und Forschung.

Die FOM ist staatlich anerkannt und bietet mehr als 60 praxisorientierte Bachelor- und Master- Studiengänge an. Studiert wird im Campus-Studium+ mit Vorlesungen im Hörsaal und virtuellen Anteilen oder komplett ortsunabhängig im Digitalen Live-Studium.

Lehrende und Studierende forschen an der FOM in einem großen Forschungsbereich aus hochschuleigenen Instituten und KompetenzCentren. Dort werden anwendungsorientierte Lösungen für betriebliche und gesellschaftliche Problemstellungen generiert. Aktuelle Forschungsergebnisse fließen unmittelbar in die Lehre ein und kommen so den Unternehmen und der Wirtschaft insgesamt zugute.

Zudem fördert die FOM grenzüberschreitende Projekte und Partnerschaften im europäischen und internationalen Forschungsraum. Durch Publikationen, über Fachtagungen, wissenschaftliche Konferenzen und Vortragsaktivitäten wird der Transfer der Forschungs- und Entwicklungsergebnisse in Wissenschaft und Wirtschaft sichergestellt.

Alle Institute und KompetenzCentren unter
fom.de/forschung



ISBN (Print) 978-3-89275-427-5

ISSN (Print) 2748-6869

ISBN (eBook) 978-3-89275-428-2

ISSN (eBook) 2748-6877



KCW KompetenzCentrum
für Wirtschaftsrecht
der FOM Hochschule für Oekonomie & Management

FOM Hochschule

Mit rund 45.000 Studierenden ist die FOM eine der größten Hochschulen Europas und führt seit 1993 Studiengänge für Berufstätige durch, die einen staatlich und international anerkannten Hochschulabschluss (Bachelor/Master) erlangen wollen.

Die FOM ist der anwendungsorientierten Forschung verpflichtet und verfolgt das Ziel, adaptionsfähige Lösungen für betriebliche bzw. wirtschaftsnahe oder gesellschaftliche Problemstellungen zu generieren. Dabei spielt die Verzahnung von Forschung und Lehre eine große Rolle: Kongruent zu den Masterprogrammen sind Institute und KompetenzCentren gegründet worden. Sie geben der Hochschule ein fachliches Profil und eröffnen sowohl Wissenschaftlerinnen und Wissenschaftlern als auch engagierten Studierenden die Gelegenheit, sich aktiv in den Forschungsdiskurs einzubringen.

Weitere Informationen finden Sie unter **fom.de**

KCW

Das KCW KompetenzCentrum für Wirtschaftsrecht forscht in für Wirtschaftsunternehmen relevanten Rechtsbereichen. Der Fokus liegt auf Fragestellungen, die sich aus Unternehmenssicht in der wirtschaftsrechtlichen Praxis ergeben. Die im Rahmen von Forschungsprojekten aufzuwerfenden Fragestellungen weisen daher stets einen größtmöglichen Praxisbezug auf.

Neben der Forschungsarbeit legt das KCW großen Wert auf den Wissenstransfer. Es werden daher regelmäßig Fortbildungen und Schulungen für Unternehmen und Verbände angeboten. Zudem fließen die aktuellen Forschungsergebnisse in die Lehre der FOM Hochschule ein.

Weitere Informationen finden Sie unter **fom-kcw.de**



Der Wissenschaftsblog der FOM Hochschule bietet Einblicke in die vielfältigen Themen, zu denen an der FOM geforscht wird: **fom-blog.de**