

MASTER THESIS | MASTER'S THESIS

Titel | Title

Künstliche Intelligenz in der Corporate Governance – Rechtliche Anforderungen
und Organpflichten im Lichte der DS-GVO und KI-VO

verfasst von | submitted by

Lea Elisabeth Claus

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien | Vienna, 2026

Studienkennzahl lt. Studienblatt |
Degree programme code as it appears on the
student record sheet:

UA 999 082

Universitätslehrgang lt. Studienblatt |
Postgraduate programme as it appears on the
student record sheet:

Europäisches und Internationales Wirtschaftsrecht
[Vollzeit Deutsch]

Betreut von | Supervisor:

ao. Univ.-Prof. Mag. Dr. Siegfried Fina

Abstract (Deutsch)

Der Einsatz von Künstlicher Intelligenz (KI) transformiert unternehmerische Entscheidungsprozesse, Organisationsstrukturen und Risikoprofile grundlegend. Vor diesem Hintergrund untersucht die vorliegende Arbeit die hieraus resultierenden rechtlichen und organisatorischen Anforderungen an den Einsatz Künstlicher Intelligenz im Rahmen der Corporate Governance und analysiert das Zusammenspiel von gesellschaftsrechtlichen Organpflichten, der Datenschutz-Grundverordnung (DS-GVO) sowie der Verordnung über Künstliche Intelligenz (KI-VO).

Ausgangspunkt ist die zunehmende Verlagerung von Entscheidungsgrundlagen auf algorithmische Systeme, die trotz fortbestehender Verantwortlichkeit der Unternehmensleitung mit erheblichen Transparenz-, Kontroll- und Risikodefiziten einhergeht, insbesondere aufgrund der sogenannten Blackbox-Problematik. Während die DS-GVO ein prozedural geprägtes Governance-Regime etabliert – insbesondere durch Rechenschaftspflicht, Transparenzanforderungen sowie das Verbot ausschließlich automatisierter Entscheidungen –, verfolgt die KI-VO einen risikobasierten, systembezogenen Ansatz mit spezifischen Anforderungen an Datenqualität, Risikomanagement, menschliche Aufsicht und Dokumentation.

Diese Arbeit zeigt, dass beide Regelwerke trotz unterschiedlicher Anknüpfungspunkte funktional ineinandergreifen und ein sich ergänzendes Pflichtenregime begründen, das in den gesellschaftsrechtlichen Organisationsrahmen zu integrieren ist.

Auf dieser Grundlage wird ein integriertes KI-Governance-Modell entwickelt, das die regulatorischen Anforderungen mit den gesellschaftsrechtlichen Organisationspflichten verzahnt und den KI-Einsatz entlang strategischer, organisatorischer und operativer Ebenen strukturiert. Das Modell ermöglicht eine konsistente Steuerung, effektive Kontrolle und belastbare Dokumentation von KI-Systemen und leistet damit einen Beitrag zur rechtssicheren und verantwortungsvollen Implementierung von KI in der Unternehmenspraxis.

Abstract (English)

The use of artificial intelligence (AI) is fundamentally transforming corporate decision-making processes, organizational structures and risk profiles. Against this backdrop, this thesis examines the resulting legal and organizational requirements for the use of artificial intelligence within the framework of corporate governance and analyzes the interplay between corporate governance obligations, the General Data Protection Regulation (GDPR), and the Artificial Intelligence Act (AI Act).

The starting point is the increasing shift of decision-making bases to algorithmic systems, which, despite the continued responsibility of corporate management, is accompanied by significant deficits in transparency, control, and risk management, particularly due to the so-called “black box” problem. While the GDPR establishes a procedurally oriented governance regime – in particular through accountability, transparency requirements, and the prohibition of fully automated decisions – the AI Act pursues a risk-based, system-oriented approach with specific requirements regarding data quality, risk management, human oversight, and documentation.

This thesis demonstrates that, despite differing points of reference, both regulatory frameworks functionally interlock and establish a complementary regime of obligations that must be integrated into the corporate organizational framework.

Based on this, an integrated AI governance model is being developed that aligns regulatory requirements with organizational obligations under corporate law and structures the use of AI across strategic, organizational, and operational levels. The model enables consistent management, effective control, and robust documentation of AI systems, thereby contributing to the legally compliant and responsible implementation of AI in corporate practice.

Inhaltsverzeichnis

Inhaltsverzeichnis	III
Abkürzungsverzeichnis	VII
A. Einleitung	1
B. Grundlagen	2
I. Künstliche Intelligenz	2
1. Definition	2
2. Tatbestandsmerkmale des Art. 3 Nr. 1 KI-VO	3
a) Maschinengestützt	3
b) Autonomie	3
c) Anpassungsfähigkeit	4
d) Für explizite oder implizite Ziele	4
e) Ableiten	4
f) Beeinflussen der Umgebung	5
3. Abgrenzung KI-Systeme und regelbasierte Systeme	5
4. Funktionsweise von KI	6
5. Blackbox-Problematik	7
a) Definition	7
b) Rechtliche Auswirkungen	8
II. Corporate Governance	8
1. Compliance	9
2. Risk Management	9
3. KI-Governance	10
C. Rechtlicher Rahmen für den Einsatz von KI in Unternehmen	10
I. Datenschutz-Grundverordnung	11
1. Grundsätze der Datenverarbeitung, Art. 5 Abs. 1 DS-GVO	12
a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (lit. a)	12
b) Zweckbindung (lit. b)	12
c) Datenminimierung (lit. c)	13
d) Richtigkeit (lit. d)	14
2. Rechenschaftspflicht, Art. 5 Abs. 2 DS-GVO	14
3. Rechtmäßigkeit der Verarbeitung, Art. 6 DS-GVO	15
a) Datensammlung und Training des KI-Systems	15
b) Nutzung des KI-Systems	16
	III

4.	Transparenz- und Informationspflichten, Art. 13-15 DS-GVO	16
5.	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung, Art. 25 DS-GVO	17
6.	Datenschutz-Folgenabschätzung, Art. 35 DS-GVO	18
II.	Verordnung über künstliche Intelligenz	19
1.	Anbieter und Betreiber von KI-Systemen	20
2.	Risikoklassifizierung von KI-Systemen	20
3.	Pflichten der KI-VO	21
a)	KI-Kompetenz, Art. 4 KI-VO	21
b)	Anforderungen an Hochrisiko-KI-Systeme, Art. 8 ff. KI-VO	22
aa)	Anbieter	22
bb)	Betreiber	23
c)	Transparenzpflichten	24
aa)	Art. 13 KI-VO	25
bb)	Art. 50 KI-VO	25
III.	Zusammenspiel von DS-GVO und KI-VO	26
1.	Regelungsziele	26
2.	Funktionale Ergänzung der Pflichtenkataloge	27
3.	Überschneidungen in der Unternehmenspraxis	28
4.	Konsequenzen für die Corporate Governance	29
D.	Datenschutzrechtliche Grenzen der automatisierten Entscheidungsfindung	29
I.	Anwendungsbereich des Art. 22 DS-GVO	30
1.	Tatbestandsmerkmale, Art. 22 Abs. 1 DS-GVO	30
a)	Entscheidung	30
b)	Ausschließlich automatisiert	30
c)	Rechtliche oder erhebliche Auswirkungen	32
2.	Ausnahmen, Art. 22 Abs. 2, Abs. 3 DS-GVO	33
II.	Transparenz- und Informationspflichten bei automatisierten Entscheidungen	33
1.	Informationspflichten nach Art. 13-15 DS-GVO	33
2.	Inhaltliche Reichweite – Blackbox-Problematik	34
a)	Methodenbezogene Informationserbringung	34
b)	Subjektbezogene Informationserbringung	35
III.	Verhältnis zu anderen Vorschriften	35
1.	Datenschutz-Grundverordnung	35

2.	Verordnung über künstliche Intelligenz	36
IV.	Automatisierte Entscheidungsfindung als Governance-Herausforderung	36
E.	Organpflichten beim Einsatz von KI-Systemen in der Corporate Governance	37
I.	Organpflichten der Leitungsorgane in Bezug auf Künstliche Intelligenz	38
1.	Sorgfaltspflicht im engeren Sinne	38
a)	Maßstab der Sorgfaltspflicht	38
b)	Übertragung auf den Einsatz von KI-Systemen	38
aa)	ISION-Grundsätze und Plausibilitätskontrolle	38
bb)	Grundsatz der Datenqualität	39
2.	Überwachungspflicht	40
a)	Vertikale und horizontale Überwachungspflichten	40
b)	Überwachung des KI-Einsatzes	41
3.	Legalitätspflicht	41
4.	Legalitätskontrollpflicht	42
II.	Delegation an Künstliche Intelligenz	43
1.	Möglichkeit der Delegation und dessen Grenzen	43
a)	Allgemeine Grundsätze der Delegation	43
b)	Übertragung der Grundsätze auf KI-Systeme	43
c)	Grenzen der Delegation: Grundsatz der umfassenden Leitungsverantwortung	44
2.	Pflicht zur Delegation?	45
3.	Rechtsfolgen der Delegation	46
III.	Bedeutung der Organpflichten für die Corporate Governance	47
F.	Modell einer KI-Governance in Unternehmen	48
I.	Notwendigkeit eines Governance-Modells beim Einsatz von KI-Systemen	48
1.	Aus unternehmerischer Perspektive	48
2.	Aus regulatorischer Perspektive	48
II.	Datenschutzrechtliche Governance-Anforderungen nach der DS-GVO	49
1.	Daten als Ausgangspunkt	49
2.	Grundprinzipien der Datenverarbeitung	50
a)	Grundsätze nach Art. 5 Abs. 1 DS-GVO	50
b)	Rechenschafts- und Dokumentationspflichten nach Art. 5 Abs. 2 DS-GVO	51
3.	Transparenz und Blackbox-Problematik als Governance-Herausforderung	52
4.	Sicherung menschlicher Entscheidungsverantwortung	53
5.	Datenschutz-Folgeabschätzung als zentrales Governance-Instrument	53

III.	KI-spezifische Governance-Anforderungen nach der KI-VO	54
1.	Strukturierte Einordnungsentscheidungen	54
2.	Vermittlung von KI-Kompetenz als strukturelle Voraussetzung	55
3.	Menschliche Aufsicht als zentrales Steuerungselement	56
4.	Dokumentations- und Nachweispflichten	57
IV.	Integriertes KI-Governance Modell für Unternehmen	57
1.	Verzahnung der Anforderungen nach DS-GVO und KI-VO	57
2.	Ausgangspunkt: Gesamtverantwortung der Leitungsorgane	58
3.	KI-Governance Modell	58
a)	Ebene 1: Strategische Steuerung und Leitentscheidungen	58
b)	Ebene 2: Operative Organisation und Compliance	59
c)	Ebene 3: Risikomanagement und Kontrolle	60
d)	Dokumentation als verbindendes Governance-Instrument	61
V.	Schlussbetrachtung	61
G.	Fazit	62
	Literaturverzeichnis	IX

Abkürzungsverzeichnis

AG	Aktiengesellschaft
AI	Artificial Intelligence
AktG	Aktiengesetz
BB	Betriebs-Berater
BeckOK	Beck Onlinekommentar
BeckOGK	Beck Online-Großkommentar
BGH	Bundesgerichtshof
BKR	Zeitschrift für Bank- und Kapitalmarktrecht
CCZ	Corporate Compliance
CR	Computer und Recht
DS-GVO	Datenschutz-Grundverordnung
DSRI	Deutsche Stiftung für Recht und Informatik
ErwG	Erwägungsgrund
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
GRCh	Grundrechte-Charta
GuP	Gesundheit und Pflege
Hdb.	Handbuch
KI	Künstliche Intelligenz
KIR	Zeitschrift für Künstliche Intelligenz und Recht
KI-VO	Verordnung über künstliche Intelligenz
LTZ	Zeitschrift für die digitale Rechtsanwendung
M&A	Mergers and Acquisitions
MAH	Münchener Anwalts Handbuch Arbeitsrecht
MMR	Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT
MüKo	Münchener Kommentar
NZG	Neue Zeitschrift für Gesellschaftsrecht
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung

OLG	Oberlandesgericht
RdA	Recht der Arbeit
RD <i>i</i>	Recht Digital
RW	Rechtswissenschaft
Vgl.	Vergleiche
ZAT	Zeitschrift für Arbeitsrecht und Tarifpolitik in kirchlichen Unternehmen
ZD	Zeitschrift für Datenschutzrecht
ZfDR	Zeitschrift für Digitalisierung und Recht
ZIP	Zeitschrift für Wirtschaftsrecht
ZRP	Zeitschrift für Rechtspolitik

A. Einleitung

Die fortschreitende Digitalisierung der Wirtschaft führt zu einer zunehmenden Integration von Systemen der künstlichen Intelligenz (KI) in unternehmerischen Entscheidungsprozessen. KI wird dabei nicht mehr lediglich als unterstützendes Instrument zur Effizienzsteigerung eingesetzt, sondern übernimmt in rasant wachsendem Umfang Aufgaben, die bislang originär menschlicher Entscheidungsfindung vorbehalten waren. Insbesondere datengetriebene Analyse- und Prognoseverfahren ermöglichen es, komplexe Sachverhalte in einer bislang nicht erreichten Geschwindigkeit und Tiefe zu verarbeiten und auf dieser Grundlage Handlungsempfehlungen oder eigenständige Entscheidungen abzuleiten.

Diese Entwicklung geht jedoch mit erheblichen rechtlichen und organisatorischen Herausforderungen einher und stellt die klassische Corporate Governance vor erhebliche Herausforderungen. Während Unternehmensleitungen weiterhin für die Rechtmäßigkeit, Angemessenheit und Nachvollziehbarkeit unternehmerischer Entscheidungen rechtlich verantwortlich bleiben, verlagert sich die faktische Entscheidungsgrundlage zunehmend auf algorithmische Systeme und führt damit zu einer strukturellen Verschiebung. Dabei ist der Funktionsweise von KI-Systemen für die handelnden Organe oftmals nur eingeschränkt nachvollziehbar aufgrund von Intransparenz und einer gewissen Eigenständigkeit in der Entscheidungsfindung. Daraus resultieren spezifische Risiken, insbesondere im Hinblick auf Diskriminierung, Fehlentscheidungen sowie Verletzungen von Datenschutz- und Persönlichkeitsrechten.

Parallel zu dieser technologischen Entwicklung hat der europäische Gesetzgeber begonnen, den Einsatz von KI umfassend und mehrschichtig zu regulieren. Zentrale Bedeutung kommt dabei der Datenschutz-Grundverordnung (DS-GVO) zu, die bereits seit 2018 einen verbindlichen Rechtsrahmen für die Verarbeitung personenbezogener Daten schafft. Hinzu tritt aber mit der Verordnung über künstliche Intelligenz (KI-VO) auch ein neues unionsrechtliches Instrument, das spezifisch auf KI-Systeme zugeschnitten ist.

Diese Regelwerke verfolgen unterschiedliche Regelungsziele, greifen jedoch vielfach ineinander und werfen komplexe Abgrenzungs- und Koordinationsfragen auf. Während die DS-GVO den Schutz personenbezogener Daten und die Rechte betroffener Personen in den Mittelpunkt stellt, verfolgt die KI-VO einen risikobasierten Ansatz zur Gewährleistung eines sicheren und verantwortungsvollen Einsatzes von KI-Systemen. Beide Verordnungen bilden ein komplexes, sich überlagerndes Normgefüge, das in der Unternehmenspraxis zu kumulativen Anforderungen führt.

Die Einhaltung dieser Anforderungen kann nicht durch punktuelle Einzelmaßnahmen gewährleistet werden. Vielmehr bedarf es einer strukturierten Einbettung des KI-Einsatzes in die bestehende Corporate Governance. Insbesondere die gesellschaftsrechtlichen Organpflichten –die Legalitäts-, Sorgfalts- und Überwachungspflichten – verlangen, dass der Einsatz von KI-Systemen in eine ordnungsgemäße Unternehmensorganisation integriert wird. Gerade die Schnittstelle von Datenschutzrecht, Gesellschaftsrecht und KI-Regulierung ist Gegenstand aktueller juristischer Diskussionen.

Somit stellt sich die zentrale Frage, welche datenschutzrechtlichen Grenzen für den Einsatz von KI in unternehmerischen Entscheidungsprozessen bestehen, welche Pflichten die Leitungsorgane in der Corporate Governance hierzu treffen und wie hier DS-GVO und KI-VO zusammenwirken. Ziel der vorliegenden Arbeit ist es daher, die rechtlichen Anforderungen an den Einsatz von KI-Systemen systematisch aufzuarbeiten und deren Auswirkungen auf die Pflichten der Leitungsorgane zu analysieren. Aufbauend darauf wird ein integriertes KI-Governance-Modell entwickelt, das die Vorgaben der DS-GVO und der KI-VO mit den gesellschaftsrechtlichen Organisationspflichten verzahnt und als praxisorientierter Ordnungsrahmen für Unternehmen dient.

B. Grundlagen

I. Künstliche Intelligenz

1. Definition

Der Begriff der „Künstlichen Intelligenz“ war lange Zeit weder technisch noch rechtlich einheitlich bestimmt und wurde in Wissenschaft und Praxis unterschiedlich verwendet. Das beruht maßgeblich darauf, dass KI kein homogenes Phänomen darstellt, sondern eine Vielzahl unterschiedlicher Systeme, Methoden und Einsatzformen umfasst, die sich nur begrenzt verallgemeinern lassen.¹

Mit dem Erlass der KI-VO hat der europäische Gesetzgeber erstmals eine rechtsverbindliche Legaldefinition von KI-Systemen geschaffen. Eine klare Definition soll für Rechtssicherheit, mehr internationale Konvergenz und hohe Akzeptanz sorgen und gleichzeitig Flexibilität bieten, um mit den raschen technologischen Entwicklungen dieser Zeit mitzuhalten (ErwG 12 KI-VO).

¹ *Recktenwald* in Bernzen/Fritzsche/Heinze/Thomsen, DSRI Herbstakademie 2023, S. 387.

Art. 3 Nr. 1 KI-VO definiert KI-Systeme „als 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.“

Diese orientiert sich inhaltlich in großen Teilen an einer von der OECD in ihren KI-Leitlinien² entwickelten Definition und verfolgt bewusst seinen funktionalen und technologieoffenen Ansatz.³ Ziel ist es, die Regulierung nicht auf bestimmte technische Methoden zu beschränken, sondern vielmehr an die tatsächlichen Wirkungen und Risiken von KI-Systemen anzuknüpfen und so gleichzeitig eine Anpassung an die stetig fortschreitenden technologischen Entwicklungen zu ermöglichen.

2. Tatbestandsmerkmale des Art. 3 Nr. 1 KI-VO

Auf den ersten Blick erscheint die Definition sehr weit gefasst, jedoch werden die einzelnen Tatbestandsmerkmale in der Erwägungsgründen der KI-VO näher präzisiert. Erst im Zusammenspiel von Normtext und Erwägungsgrund lässt sich der Regelungsgegenstand der KI-VO hinreichend konturieren.

a) Maschinengestützt

Erstbenanntes Merkmal ist, dass es sich um ein maschinengestütztes System handeln muss. Dies bedeutet nur, dass das System von Maschinen betrieben wird, mithin rechnergestützt operiert (ErwG 12 S. 7 KI-VO).

b) Autonomie

Bedeutender ist das Merkmal, wonach ein KI-System mit unterschiedlichen Graden an Autonomie arbeiten soll. Das System muss bis zu einem gewissen Grad unabhängig von menschlichem Zutun agieren und ohne menschliches Eingreifen arbeiten können (ErwG 12 S. 11 KI-VO). Das ist jedoch nicht mit einer bloßen Automatisierung gleichzustellen.⁴ Denn Systeme, die ausschließlich auf von natürlichen Personen definierte Regeln für das automatische Ausführen von Operationen beruhen, werden ausdrücklich ausgenommen (ErwG

² OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, 22.05.2019, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>, abgerufen am 23.04.2026.

³ Kirschke-Biller/Füllsack in BeckOK KI-Recht, KI-VO, Art. 3 Rn. 15.

⁴ Vgl. Hacker/Berz, ZRP 2023, 226, 227.

12 S. 2 KI-VO). Der Unterschied zwischen Autonomie und Automatisierung ist, dass die autonomen Handlungen eines KI-Systems die Fortführung der durch Ableiten autonom generierten Ausgaben darstellen.⁵

c) Anpassungsfähigkeit

Ferner kann Abgrenzungsmerkmal die Anpassungsfähigkeit des KI-Systems nach Betriebsaufnahme sein. Dies bezieht sich auf seine Lernfähigkeit, die eine fortlaufende Veränderung während seiner Verwendung ermöglicht (ErwG 12 S. 12 KI-VO). So werden auch Systeme erfasst, die ihr Verhalten auf der Grundlage neuer Daten anpassen können.⁶ Jedoch ist dies keine zwingende Voraussetzung und insofern nicht fakultativ.

d) Für explizite oder implizite Ziele

KI-Systeme sollen sowohl nach expliziten als auch nach impliziten Zielen arbeiten können (ErwG 12 S. 8 KI-VO). Explizit meint dabei, dass die Ziele direkt im System programmiert wurden, wohingegen implizite Ziele solche sind, die aus den zugrundeliegenden Annahmen des Systems abgeleitet werden können.⁷

e) Ableiten

Zentrales Merkmal eines KI-Systems ist jedoch die Fähigkeit, abzuleiten. So muss es dem KI-System möglich sein, Ausgaben zu erzeugen sowie Algorithmen und Modelle aus Eingaben oder Daten zu erstellen (ErwG 12. S. 4 KI-VO). Beispielsweise werden hier Ansätze für maschinelles Lernen oder logik- und wissensgestützte Konzepte genannt (ErwG 12. S. 5 KI-VO). Die Fähigkeiten eines KI-Systems gehen dabei über die einfache Datenverarbeitung hinaus, indem Lern-, Schlussfolgerungs- und Modellierungsprozesse ermöglicht werden (ErwG 12. S. 6 KI-VO).

Das KI-System muss also nicht nur die Ausgaben selbst herleiten, sondern auch die Methode, wie es zu diesen Ausgaben gelangt.⁸ Die Ableitung fungiert wie eine „Brücke“: Aus den Eingaben wird abgeleitet, wie Ausgaben erstellt werden.⁹

⁵ Kirschke-Biller/Füllsack in BeckOK KI-Recht, KI-VO, Art. 3 Rn. 53.

⁶ Kirschke-Biller/Füllsack in BeckOK KI-Recht, KI-VO, Art. 3 Rn. 56; Wendehorst in Martini/Wendehorst, KI-VO, Art. 3 Rn. 33 f.

⁷ Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), Rn. 24 f., <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application>, abgerufen am 23.04.2026.

⁸ Wendehorst in Martini/Wendehorst, KI-VO, Art. 3 Rn. 38.

⁹ Glauner/Pieper in Bomhard/Pieper/Wende, KI-VO, Art. 3 Rn. 44.

f) Beeinflussen der Umgebung

Zuletzt müssen die Ausgaben die physische oder digitale Umgebung beeinflussen können. Umgebungen sind dabei als Kontexte, in denen KI-Systeme betrieben werden, zu verstehen (ErwG 12 S. 10 KI-VO).

Das Beeinflussen setzt dabei keine übermäßig hohen Anforderungen voraus.¹⁰ Eine physische Umgebung wird dann beeinflusst, wenn die Ausgabedaten des Systems eine mechanische Reaktion des maschinengestützten Systems auslösen; eine digitale Umgebung wird beeinflusst, wenn Ausgaben wiederum als Eingabedaten für ein anderes algorithmisches System dienen.¹¹

3. Abgrenzung KI-Systeme und regelbasierte Systeme

Die zentrale Frage besteht darin, wie KI-Systeme von klassischen regelbasierten Softwaresystemen abzugrenzen sind.

Letztere beruhen auf fest programmierten Entscheidungsregeln, bei denen das System lediglich vorab definierte Anweisungen ausführt.¹² Das Ergebnis ist vollständig durch den menschlichen Programmierer determiniert. Demgegenüber zeichnen sich KI-Systeme im Sinne der KI-VO dadurch aus, dass sie einen eigenständigen Ableitungsprozess zwischen Eingabe und Ausgabe vollziehen.

Daher sind die wichtigsten Tatbestandsmerkmale zur Abgrenzung der geforderte Grad an Autonomie¹³ und die Fähigkeit, abzuleiten¹⁴ sowie sich anzupassen.¹⁵ Während regelbasierte Systeme auf fest programmierten Entscheidungsregeln beruhen, zeichnen sich lernende Systeme – die KI-Systeme – durch ihre Fähigkeit aus, ihr Verhalten auf Grundlage neuer Daten fortlaufend anzupassen.

Die Abgrenzung hat erhebliche rechtliche Konsequenzen, da für KI-Systeme mit der KI-VO besondere Anforderungen für Transparenz und Verantwortung geschaffen werden. Gerade im Kontext automatisierter Entscheidungsfindung kann die zunehmende Intransparenz der Entscheidungslogik dazu führen, dass menschliche Entscheidungsträger faktisch entmachtet werden, obwohl sie rechtlich verantwortlich bleiben.

¹⁰ *Kirschke-Biller/Füllsack* in BeckOK KI-Recht, KI-VO, Art. 3 Rn. 39.

¹¹ *Wendehorst* in Martini/Wendehorst, KI-VO, Art. 3 Rn. 47.

¹² *Vasel*, LTZ 2023, 179, 182.

¹³ *Bomhard/Siglmüller*, RDt 2024, 45.

¹⁴ *Glauner/Pieper* in Bomhard/Pieper/Wende, KI-VO, Art. 3 Rn. 66.

¹⁵ *Kirschke-Biller/Füllsack* in BeckOK KI-Recht, KI-VO, Art. 3 Rn. 20 f.

4. Funktionsweise von KI

Die Funktionsweise von KI unterscheidet sich grundlegend von klassischen Softwaresystemen, da KI maßgeblich auf Verfahren des maschinellen Lernens beruht.

Grundlage für die Leistungsfähigkeit moderner KI-Systeme ist der Zugriff auf große und heterogene Datenmengen („Big Data“).¹⁶ Mit diesen Datenmengen – den sogenannten Trainingsdaten – wird ein Algorithmus trainiert, der selbstständig aus den Daten relevante Merkmale sowie Muster erfassen können soll.¹⁷

Aufgrund der durch das Training gewonnenen Erkenntnisse erstellt das KI-System sodann selbstständig ein geeignetes Modell, auf dessen Basis Lösungen für die eigentliche Entscheidungsfindung entwickelt und eigenständig Ausgabeentscheidungen erzeugt werden.¹⁸

Dieser Prozess soll menschlichem Handeln möglichst nahekommen und ein solches simulieren.¹⁹ Um das zu ermöglichen, werden dem KI-System künstliche neuronale Netze zugrunde gelegt, die denen des menschlichen Gehirns nachempfunden sind.²⁰ Diese zahlreichen Schichten miteinander verbundener Netze durchlaufen Mengen an Daten und wirken dabei ähnlich wie ein Filter.²¹

Zwar beruhen klassische Softwaresysteme ebenso auf Algorithmen, jedoch können „selbstlernende Algorithmen“ im Rahmen des maschinellen Lernens zu den im Vorfeld programmierten Handlungsregeln selbstständig weitere Regeln entwickeln.²² Gerade diese Möglichkeit der Selbstlernfähigkeit ist ausschlaggebend.²³ Bei klassischen Algorithmen hingegen wird der Weg zur Entscheidung schrittweise kodiert.²⁴

Zwar weisen selbstlernende Algorithmen aufgrund ihrer Funktionsweise großes Potential auf, da ihre Leistungsfähigkeit weit über die eines Menschen hinausgeht, jedoch führt dieses Vorgehen auch zu einer Entkopplung von menschlicher Einflussnahme im Rahmen der Programmierung und der konkreten Entscheidung. Diese funktionale Eigenständigkeit führt allerdings auch zu besonderen Risiken und rechtlichen Herausforderungen. Denn KI-Systeme

¹⁶ Wissenschaftliche Dienste, WD 8 – 3000 – 063/19, S. 4; *Hersemeyer/Ludolph* in Bernzen/Fritzsche/Heinze/Thomsen, DSRI Herbstakademie 2023, S. 365.

¹⁷ *Reichert/Radtke/Eske*, ZD 2024, 483, 484.

¹⁸ *Niederée/Nejdl* in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 2 Rn. 24; *Gausling*, ZD 2019, 335.

¹⁹ *Hoeren/Niehoff*, RW 2018, 47, 49.

²⁰ *Minihold* in Ifsits/Minihold/Roubik, Haftungsfragen beim Einsatz Künstlicher Intelligenz, S. 6.

²¹ *Gausling*, ZD 2019, 335.

²² *Minihold* in Ifsits/Minihold/Roubik, Haftungsfragen beim Einsatz Künstlicher Intelligenz, S. 5 f.

²³ *Hoeren/Niehoff*, RW 2018, 47, 49.

²⁴ *Niederée/Nejdl* in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 2 Rn. 24

suchen nur nach zufälligen Übereinstimmungen, nicht jedoch nach den dem zugrunde liegenden Ursachen zwischen den relevanten Parametern – sie arbeiten allein auf Basis von induktivem Wissen und Korrelationen.²⁵ Werden aus diesen zufälligen Übereinstimmungen sodann kausale Zusammenhänge abgeleitet, obwohl solche nicht bestehen, kommt es zu sogenannten Scheinkorrelationen.²⁶

Die Funktionsweise von KI beeinflusst daher maßgeblich rechtliche Problemkreise um Informationspflichten und Transparenz, Kontrolle und Überwachung sowie Verantwortungszuweisungen, die es aufzulösen gilt.

5. Blackbox-Problematik

a) Definition

Eines der größten von KI-Systemen ausgehenden Probleme besteht in ihrer begrenzten Erklärbarkeit. Zwar sind regelmäßig sowohl Eingabe- als auch Ausgabedaten bekannt, jedoch kann der konkrete Entscheidungsweg, der von Eingabe zu Ausgabe führt, selbst von Experten oftmals nicht mehr nachvollzogen werden.²⁷

Je schneller das KI-System komplexe Schritte ausführt, desto schwieriger wird es für den Menschen, das System während des Ablaufs zu überwachen.²⁸ Es sind zwar die Verarbeitungsergebnisse der KI theoretisch mathematisch nachvollziehbar, jedoch fallen sie in einer derartigen Menge an, dass sie von Menschen nicht mehr bearbeitet werden können, sondern wiederum nur von einem KI-System.²⁹ Dies gilt insbesondere für komplexe Modelle, die auf Basis neuronaler Netze arbeiten, etwa im Bereich des Deep Learning.³⁰

Diese fehlende Rekonstruierbarkeit der Entscheidungslogik wird als Blackbox-Problematik bezeichnet. Zwar liefert das KI-System konsistente Ergebnisse, jedoch sind die internen Abwägungen und Entscheidungsparameter einer vollständigen externen Kontrolle entzogen³¹. Die Blackbox-Problematik betrifft daher nicht das Fehlen von Daten, sondern die fehlende Transparenz des algorithmischen Entscheidungsprozesses selbst.

Dieses Problem ist nicht nur in Rechtskreisen bekannt, sondern stellt seit Jahren ein nachhaltig

²⁵ Ebers in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 3 Rn. 16.

²⁶ Ebers in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 3 Rn. 20

²⁷ Baumgartner/Brunnbauer/Cross, MMR 2023, 543, 544; Merkle, RD i 2024, 414, 415.

²⁸ Ebers in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 3 Rn. 11.

²⁹ Minihold in Ifsits/Minihold/Roubik, Haftungsfragen beim Einsatz von KI, Kap. V S. 99.

³⁰ Kumkar in Hilgendorf/Roth-Isigkeit, KI-VO, § 6 Rn. 3; Mainzer, Künstliche Intelligenz, S. 245.

³¹ Kumkar in Hilgendorf/Roth-Isigkeit, KI-VO, § 6 Rn. 3.

wachsendes Forschungsfeld auch in der Informatik dar. Um dieser Intransparenz zu begegnen, wird daher zu einer erklärbaren KI geforscht („Explainable AI“).³²

b) Rechtliche Auswirkungen

In rechtlicher Hinsicht hat die fehlende Erklärbarkeit vor allem Auswirkungen auf die Überwachung der KI-Systeme. So verhindern die opaken Strukturen regelmäßig sowohl eine vorgängige als auch eine nachträgliche Kontrolle der Vorgänge.³³ Ein besonderes Spannungsverhältnis besteht auch zu zentralen datenschutzrechtlichen Anforderungen, insbesondere zu Transparenz-, Informations- und Rechenschaftspflichten (Art. 12 ff. DSGVO). Wie noch zu zeigen sein wird, genügt eine bloße Offenlegung der verwendeten Trainingsdaten der Erfüllung dieser Anforderungen regelmäßig nicht.³⁴

Die Blackbox-Problematik gewinnt vor allem auch Bedeutung im Hinblick auf Diskriminierungsrisiken.³⁵ Lernende KI-Systeme übernehmen statische Muster aus den Trainingsdaten, sodass sich bestehende Verzerrungen oder Benachteiligungen zulasten bestimmter Personengruppen in der Ausgabeentscheidung fortsetzen oder gar verstärkt werden können.³⁶ Diese Fehler können nicht vom KI-System aufgedeckt werden, da es keine wertende Ursachenanalyse vornehmen kann.³⁷ Erfolgt der Entscheidungsprozess nicht hinreichend transparent, können diskriminierende Effekte weder erkannt noch korrigiert werden.

Transparenz ist daher hier nicht als bloße Informationspflicht zu verstehen, sondern als Voraussetzung effektiver Kontrolle und Verantwortungszuweisung. Die Blackbox-Problematik wirkt daher über das Datenschutzrecht hinaus und berührt grundlegende Fragen der Corporate Governance. Unternehmen müssen die Transparenzanforderungen schon bei der Entwicklung der KI-Systeme beachten, um dem Mindestmaß an Nachvollziehbarkeit und Kontrolle gerecht zu werden.³⁸ Bei der Blackbox-Problematik sind daher weitere Maßnahmen erforderlich, um zu einer möglichst hohen Transparenz zu gelangen.³⁹

II. Corporate Governance

Corporate Governance bezeichnet den rechtlichen und faktischen Ordnungsrahmen für die Lei-

³² Krügel/Pfeifferbring in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 11 Rn. 72.

³³ Scholz in Simitis/Hornung/Spiecker gen. Döhmman, DS-GVO, Art. 22 Rn. 10.

³⁴ Wilmer in Jandt/Steidle, Datenschutz und Internet, Kap. V Rn. 666.

³⁵ Kumkar in Hilgendorf/Roth-Isigkeit, KI-VO, § 6 Rn. 3; Wilmer in Jandt/Steidle, Datenschutz und Internet, Kap. V Rn. 666; Baumgartner/Brunnbauer/Cross, MMR 2023, 543, 544.

³⁶ Kumkar in Hilgendorf/Roth-Isigkeit, KI-VO, § 6 Rn. 3.

³⁷ Ebers in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 3 Rn. 20

³⁸ Baumgartner/Brunnbauer/Cross, MMR 2023, 543, 544.

³⁹ Dienes, MMR 2024, 456, 460.

tung, Steuerung und Überwachung von Unternehmen.⁴⁰ Dieser Ordnungsrahmen bestimmt, wie in Unternehmen Entscheidungen getroffen werden, und umfasst ein übergreifendes Konzept, das sowohl gesetzliche Vorgaben als auch unternehmensinterne Regelwerke einbezieht.⁴¹

Die Corporate Governance lässt sich in Bezug auf KI grundsätzlich in die Verfolgung zweier eng miteinander verknüpfter Zielrichtungen unterteilen. Zum einen dient sie der Einhaltung gesetzlicher Vorgaben (Compliance), zum andern zielt sie auf die Steuerung und Abmilderung der mit dem Einsatz von KI verbundenen unternehmerischen Risiken (Risk Management).⁴²

1. Compliance

Compliance ist die Pflicht des Unternehmens und seiner Organe, Rechtsverletzungen aus seinem Unternehmen heraus zu verhindern.⁴³ Sie ist Ausprägung der allgemeinen Unternehmenssorgfaltspflicht, da derjenige, der eine Gefahrenquelle unterhält, die ihm zumutbaren Maßnahmen zu ergreifen hat, um Schädigungen Dritter möglichst zu vermeiden.⁴⁴

Diese Pflicht ergibt sich aus den zentralen Pflichten der leitenden Organe. Diese müssen nicht nur sich selbst gesetzeskonform verhalten (Legalitätspflicht), sondern auch dafür Sorge tragen, dass das Unternehmen so organisiert ist, dass auch die Mitarbeiter die einschlägigen Rechtsnormen einhalten (Legalitätsthroughsetzungs- oder Legalitätskontrollpflicht).⁴⁵ Die Pflicht zur ordnungsgemäßen Unternehmensorganisation bildet insoweit den normativen Kern der Corporate Governance.

2. Risk Management

Mit zunehmender Komplexität der Geschäftsmodelle steigen regelmäßig auch die damit verbundenen unternehmerischen Risiken und insofern auch die Anforderung an die Ausgestaltung der Corporate Governance.⁴⁶ Das Risikomanagement umfasst die systematische Identifikation, Analyse und Steuerung dieser Risiken.⁴⁷

In diesem Zusammenhang werden die bestehenden Organpflichten konkretisiert. Erforderlich sind insbesondere eindeutig zugewiesene Verantwortlichkeiten, umfassende Dokumentations- und Transparenzpflichten sowie wirksame Überwachungspflichten, um Risiken – etwa

⁴⁰ *Fleischer* in MüKo/GmbHG, Einl. Rn. 339; *Möslein* in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 13 Rn. 5.

⁴¹ *Stephan/Tieves* in MüKo/GmbHG, § 37 Rn. 40.

⁴² *Sassenberg*, RDt 2025, 346.

⁴³ *Dieckmann* in Chibanguza/Kuß/Steega, KI-Hdb., 2. Teil: § 5 I. Rn. 2.

⁴⁴ *Dieckmann* in Chibanguza/Kuß/Steega, KI-Hdb., 2. Teil: § 5 I. Rn. 3.

⁴⁵ *Fleischer* in BeckOGK/AktG, § 91 Rn. 62; *Sassenberg*, RDt 2025, 346.

⁴⁶ *Moosmayer/Lösler* in Moosmayer/Lösler, Corporate Compliance, § 1 Rn. 7.

⁴⁷ *Moosmayer/Lösler* in Moosmayer/Lösler, Corporate Compliance, § 1 Rn. 7.

Rechtsverstöße durch fehlerhafte Eingaben oder Ausgaben – durch die Implementierung wirksamer Kontrollmechanismen zu erkennen und zu vermeiden.⁴⁸

Bei der Wahrnehmung dieser Pflichten bietet die Business Judgement Rule (§ 93 Abs. 1 S. 2 AktG) den Leitungsorganen einen gewissen Haftungsschutz.⁴⁹ Sie schützt unternehmerische Ermessensentscheidungen, sofern sie auf einer angemessenen Informationsgrundlage beruhen und zum Wohl des Unternehmens getroffen werden. Damit markiert sie zugleich auch die Grenze zulässiger Entscheidungsfreiheit: Sobald es an einer hinreichenden Informationsbasis fehlt oder gesetzliche Vorgaben missachtet werden, entfällt ihr Schutz. Gerade im Kontext des KI-Einsatzes gewinnt dies hinsichtlich der bestehenden Transparenz- und Nachvollziehbarkeitsprobleme besondere Bedeutung.

3. KI-Governance

Corporate Governance wirkt damit sowohl repressiv durch die Umsetzung rechtlicher Vorgaben und die damit verbundene Vermeidung von Normverstößen als auch präventiv hinsichtlich Risikovorsorge und -management. Diese Doppelfunktion gewinnt besondere Bedeutung hinsichtlich des Einsatzes neuer Technologien.

Künstliche Intelligenz stellt Unternehmen vor neue rechtliche und organisatorische Herausforderungen, insbesondere hinsichtlich der beschriebenen Diskriminierungsrisiken infolge verzerrter Trainingsdaten. Zur Bewältigung dieser Herausforderungen genügt es nicht, nur punktuelle Compliance-Maßnahmen zur Mitigation der mit der KI-Nutzung einhergehenden Risiken zu schaffen. Vielmehr bedarf es einer Einbettung des KI-Einsatzes in den bereits bestehenden Governance-Rahmen.⁵⁰

In diesem Zusammenhang hat sich der Begriff der „AI Policy“ beziehungsweise „KI-Governance“ etabliert.⁵¹ Sie dient als unternehmensinternes Steuerungselement, das sowohl die regulatorischen Anforderungen als auch die unternehmensspezifischen Risiken beim Einsatz von KI-Systemen adressiert und einen Rahmen für eine kontrollierte Verwendung schafft.

C. Rechtlicher Rahmen für den Einsatz von KI in Unternehmen

KI-Systeme sind häufig mit verborgenen Risiken für die Rechte und Freiheiten der betroffenen Personen verbunden. Diese Risiken resultieren insbesondere aus der Komplexität

⁴⁸ Hoeren/Pinelli, KIR 2026, 5, 6 f.

⁴⁹ Müller/Masson in Chibanguza/Kuß/Steega, KI-Hdb., 2. Teil: § 5 J. Rn. 4.

⁵⁰ Hoeren/Pinelli, KIR 2026, 5, 8.

⁵¹ Sassenberg, RD 2025, 346, 347.

algorithmischer Entscheidungsprozesse, der daraus folgenden Intransparenz sowie der potentiellen Verstärkung diskriminierender Strukturen. Vor diesem Hintergrund ist daher ein erhöhter Bedarf an rechtlicher Regulierung entstanden, um diesen Gefahren entgegenwirken zu können.⁵² Auf europäischer Ebene hat sich so zunehmend ein Rechtsrahmen für den Einsatz von KI-Systemen in Unternehmen entwickelt.

Zentrale Bedeutung kommt hierbei sowohl der DS-GVO als auch der KI-VO zu. Beide Regelwerke verfolgen jeweils eigenständige, aber miteinander verflochtene Regelungsziele. Während die DS-GVO nach Art. 1 Abs. 1 DS-GVO maßgeblich den Schutz personenbezogener Daten regelt und daraus folgend die Rechte betroffener, natürlicher Personen, hat die KI-VO die Gewährleistung eines sicheren, transparenten und verantwortungsvollen Einsatzes von KI-Systemen zum Gegenstand, Art. 1 Abs. 1 KI-VO. Ergänzt wird dieser unionsrechtliche Rahmen durch nationale Vorschriften, insbesondere solche zur Umsetzung europäischer Vorgaben sowie durch allgemeine zivilrechtliche Regelungen.

Das Zusammenspiel beider Regelwerke führt zu einem komplexen Regelungsgefüge, in dem sich die Normen gegenseitig ergänzen, jedoch auch Überschneidungen aufweisen. Der daraus entstehende kumulative Pflichtenkreis stellt Unternehmen vor die Herausforderung, ihre KI-Governance strukturiert zu entwickeln, um Doppelregulierungen zu vermeiden.

I. Datenschutz-Grundverordnung

Die leichte Zugänglichkeit und Verfügbarkeit großer Datenmengen sorgt aktuell für die rasche Fortentwicklung von KI-Systemen, da so ein umfassendes Training ermöglicht werden kann.⁵³ Allerdings entsteht dort, wo KI-Systeme personenbezogene Daten im Sinne von Art. 4 Nr. 1 DS-GVO verarbeiten, ein Spannungsverhältnis zwischen KI und Datenschutz. Denn die DS-GVO zielt darauf ab, natürliche Personen bei der Verarbeitung personenbezogener Daten zu schützen (Art. 1 Abs. 1 DS-GVO, Art. 8 Abs. 1 GRCh).

Zwar adressiert die DS-GVO nicht ausdrücklich KI-Systeme, jedoch ist sie technologieneutral und unabhängig von einer verwendeten Technologie ausgestaltet (ErwG 15 S. 1 DS-GVO), sodass sie auch auf KI-Systeme Anwendung findet. Die Verordnung schafft so einen rechtlichen Rahmen für die Entwicklung und Gestaltung von KI-Systemen, um betroffene Grundrechte zu

⁵² Schürmann, ZD 2022, 316.

⁵³ Ebers in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 3 Rn. 81.

schützen und gleichzeitig die Weiterentwicklung innovativer Technologien – wie KI – zu fördern. Die DS-GVO bringt beide Interessen in ein ausgewogenes Verhältnis.⁵⁴

1. Grundsätze der Datenverarbeitung, Art. 5 Abs. 1 DS-GVO

KI-Systeme verarbeiten regelmäßig große Mengen an personenbezogenen Daten und das über ihren gesamten Lebenszyklus hinweg – von der Datenerhebung über das Training bis hin zur produktiven Nutzung.⁵⁵ Hierfür normiert Art. 5 Abs. 1 DS-GVO die grundlegenden Prinzipien der Datenverarbeitung. Besonders relevant sind hierbei die Grundsätze der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben sowie Transparenz (lit. a), Zweckbindung (lit. b), Datenminimierung (lit. c) und Richtigkeit (lit. d).

Diese stehen aber regelmäßig in Konflikt mit der Nutzung von KI-Systemen.

a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (lit. a)

Der Rechtmäßigkeitsgrundsatz erfordert, dass die Datenverarbeitung auf einer Rechtsgrundlage erfolgen muss, was in Art. 6 DS-GVO näher konkretisiert ist.

Im Widerspruch zum Transparenzgrundsatz steht vor allem die technische Komplexität von KI-Systemen. Betroffene Personen müssen nachvollziehen können, wie und zu welchem Zweck ihre Daten verarbeitet werden.⁵⁶ Die dem KI-System zugrundeliegenden Algorithmen und Datenverarbeitungsprozesse müssen in gewissem Maße offengelegt werden, um dem zu genügen.⁵⁷

Insbesondere im Hinblick auf die Blackbox-Problematik ist dies fraglich. Damit im Zusammenhang steht auch das im Grundsatz von Treu und Glauben verankerte Diskriminierungsverbot, wonach die nicht nachvollziehbaren Entscheidungswege auch in dieser Hinsicht datenschutzrechtlich problematisch sind.⁵⁸

b) Zweckbindung (lit. b)

Auch hinsichtlich des Zweckbindungsgrundsatzes, der besagt, dass Daten nur zu einem eindeutig festgelegten, legitimen Zweck erhoben werden dürfen, bestehen Zweifel. Dies hat

⁵⁴ *Bolek-Fügl* in Windholz, KI-VO, Praxishandbuch, Kap. 4 S. 185.

⁵⁵ *Ebers* in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 3 Rn. 88; *Schäfer*, ZD 2025, 12, 13.

⁵⁶ *Minihold* in Ifsits/Minihold/Roubik, Haftungsfragen beim Einsatz von KI, Kap. V S. 111.

⁵⁷ *Bolek-Fügl* in Windholz, KI-VO, Praxishandbuch, Kap. 4 S. 184.

⁵⁸ *Wilmer* in Jandt/Steidle, Datenschutz und Internet, Kap. V Rn. 666.

den Hintergrund, dass durch eine Zweckbegrenzung die betroffenen Personen selbst bestimmen können sollen, wofür ihre Daten genutzt werden.⁵⁹

Bei der Analyse von großen Datenmengen (Big Data-Analysen) bedingt die Mehrdimensionalität der Datenverarbeitung, dass oftmals gar keine Zweckbegrenzung vorgesehen werden kann. Die Analysen sollen vielmehr gerade auf die Gewinnung neuer Erkenntnisse abzielen, woraus sich neue Verwendungszwecke ergeben können und sollen.⁶⁰ Um diesem Problem abzuhelpfen, wird daher vielfach dafür argumentiert, dass bereits die Mustererkennung und das Trainieren selbst einen hinreichenden Zweck darstellen.⁶¹

Aber auch im Laufe der Nutzung von KI bereitet ihr polyvalenter Charakter Probleme, da das KI-System neue Erkenntnisse generieren kann, die über den ursprünglichen Verarbeitungszweck hinausgehen.⁶² Das ergibt sich gerade aus der Fähigkeit des Selbstlernens. Eine nachträgliche Zweckänderung ist jedoch nur unter den engen Voraussetzungen des Art. 6 Abs. 4 DS-GVO zulässig, der eine sorgfältige Abwägung erfordert.

c) Datenminimierung (lit. c)

Das KI- Training könnte auch im Widerstreit zum Grundsatz der Datenminimierung stehen, wonach die Verarbeitung auf das notwendige Maß reduziert sein muss.⁶³ Das technische System muss so gestaltet sein, dass es seine Funktion mit möglichst wenig personenbezogenen Daten erfüllen kann („privacy by design“ bzw. „data protection by design“).⁶⁴

Ein KI-System benötigt jedoch regelmäßig große Mengen an Daten. Wortlautgemäß wird allerdings keine vollständige Reduzierung verlangt, wodurch auch Big-Data-Analysen möglich werden.⁶⁵ Vielmehr ist dieser Konflikt über das Verhältnismäßigkeitsprinzip zu lösen, wodurch diese Datenmengen gerechtfertigt werden können.⁶⁶ Der aus der Datennutzung resultierende Nutzen muss die möglichen Risiken für die betroffenen Personen übersteigen.⁶⁷ Zugunsten des KI-Einsatzes ist dabei anzubringen, dass eine möglichst große Datenmenge notwendig ist, um die Qualität eines KI-Systems zu sichern.⁶⁸

⁵⁹ *Holthausen*, RdA 2021, 19, 24.

⁶⁰ *Ebers* in *Ebers/Heinze/Krügel/Steinrötter*, KI und Robotik, § 3 Rn. 89; *Holthausen*, RdA 2021, 19, 24.

⁶¹ *Krügel/Pfeiffenbring* in *Ebers/Heinze/Krügel/Steinrötter*, KI und Robotik, § 11 Rn. 24.

⁶² *Krügel/Pfeiffenbring* in *Ebers/Heinze/Krügel/Steinrötter*, KI und Robotik, § 11 Rn. 24.

⁶³ *Kloos/Schmidt-Bens* in *Hartmann*, KI & Recht kompakt, Kap. 5, S. 183.

⁶⁴ *Holthausen*, RdA 2021, 19, 24.

⁶⁵ *Schäfer*, ZD 2025, 12, 15.

⁶⁶ *Bolek-Fügl* in *Windholz*, KI-VO, Praxishandbuch, Kap. 4 S. 188.

⁶⁷ *Bolek-Fügl* in *Windholz*, KI-VO, Praxishandbuch, Kap. 4 S. 188.

⁶⁸ *Wilmer* in *Jandt/Steidle*, Datenschutz und Internet, Kap. V Rn. 668.

d) Richtigkeit (lit. d)

Nach Art. 5 Abs. 1 lit. d DS-GVO müssen personenbezogene Daten richtig sein und erforderlichenfalls auf den neuesten Stand gebracht werden. Unrichtige Daten müssen dementsprechend unverzüglich gelöscht oder berichtigt werden. Den Verantwortlichen trifft die Pflicht, eine bestimmte Datenqualität hinsichtlich der personenbezogenen Daten zu gewährleisten.⁶⁹

Gerade im Rahmen der großen Datenmengen, die in KI-Systemen regelmäßig verarbeitet werden, stellt dies eine ernstzunehmende Herausforderung dar. Die Richtigkeit der Trainingsdaten ist bedeutend, um die Gefahr fehlerhafter, diskriminierender und verzerrter Entscheidungen zu minimieren.⁷⁰ Vor allem vor dem Hintergrund, dass ein nachträgliches Löschen der unrichtigen Daten praktisch oft nicht möglich ist. Dies wäre aufgrund der technologischen Besonderheiten von KI-Systemen ohnehin nicht zielführend, da auch gelöschte Trainingsdaten weiterhin Einfluss auf später generierte Ausgaben haben können.⁷¹ Das Problem kann daher nur über ein vollständiges Löschen des gesamten KI-Systems gelöst werden. Das KI-System ist sodann mit neuen – korrigierten – Trainingsdaten erneut zu trainieren.⁷²

Probleme ergeben sich aber auch dann, wenn zwar die Trainingsdaten bzw. Rohstoffdaten richtig sind, jedoch die daraus generierten Ausgaben nicht.⁷³ Dieses Risiko besteht vor allem bei großen, generativen Sprachmodellen („Large Language Models“), die Texte auf Grundlagen reiner Wahrscheinlichkeiten ausgeben.⁷⁴

Dementsprechend sind technische und organisatorische Maßnahmen vorzunehmen, um eine Richtigkeits- bzw. Qualitätskontrolle durchführen zu können – etwa durch das positive Definieren von „unrichtigen“ Ergebnissen.⁷⁵

2. Rechenschaftspflicht, Art. 5 Abs. 2 DS-GVO

Die in Art. 5 Abs. 2 DS-GVO normierte Rechenschaftspflicht verpflichtet den Verantwortlichen nicht nur dazu, die in Art. 5 Abs. 2 DS-GVO geregelten Prinzipien einzuhalten, sondern ihre Einhaltung auch nachweisen zu können. Die Vorschrift transformiert so die materiellen Anfor-

⁶⁹ Krügel/Pfeifferbring in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 11 Rn. 26.

⁷⁰ Krügel/Pfeifferbring in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 11 Rn. 28.

⁷¹ Paal, ZfDR 2024, 129, 142; Pesch/Böhme, MMR 2023, 917, 921.

⁷² Paal, ZfDR 2024, 129, 142.

⁷³ Minihold in Ifsits/Minihold/Roubik, Haftungsfragen beim Einsatz von KI, Kap. V S. 114.

⁷⁴ Golland, EuZW 2024, 846, 851.

⁷⁵ Minihold in Ifsits/Minihold/Roubik, Haftungsfragen beim Einsatz von KI, Kap. V S. 114.

derungen zu prozeduralen Organisationspflichten.

Die Nachweisverpflichtung verleiht der Rechenschaftspflicht eine eigenständige rechtliche Qualität, indem die Gesamtverantwortung auf das datenverarbeitende Unternehmen selbst verlagert wird.⁷⁶ Damit schafft die DS-GVO zusätzliche umfangreiche Dokumentations- und Nachweispflichten und begründet so ein eigenes präventives Governance-Modell beruhend auf Eigenverantwortung und Nachweisbarkeit.⁷⁷

Dabei wird die Rechenschaftspflicht durch verschiedene Instrumente der DS-GVO konkretisiert, etwa die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 24, 25 und 32 DS-GVO oder die Durchführung der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO.⁷⁸

3. Rechtmäßigkeit der Verarbeitung, Art. 6 DS-GVO

Der Grundsatz der Rechtmäßigkeit aus Art. 5 Abs. 1 lit. a DS-GVO, wonach jede Datenverarbeitung auf einer Rechtsgrundlage beruhen muss, wird durch die Erlaubnistatbestände des Art. 6 Abs. 1 lit. a-f DS-GVO konkretisiert.

Der Einsatz von KI umfasst mehrere Verarbeitungsvorgänge. Daher sollte bei der Bestimmung der Rechtsgrundlage auch strikt nach diesen verschiedenen Verarbeitungen unterschieden werden.⁷⁹

a) Datensammlung und Training des KI-Systems

Insbesondere bei den anfänglichen Verarbeitungen – Datensammlung und Training des KI-Systems – kommt eine Einwilligung als Rechtsgrundlage nach Art. 6 Abs. 1 lit. a DS-GVO kaum in Betracht, da dies aufgrund der fehlenden Informationsgrundlage praktisch nahezu unmöglich ist.⁸⁰ Es fehlt vor allem an einer Interaktion und Beziehung zwischen dem Anbieter des KI-Systems und der betroffenen Person.⁸¹

In diesen Phasen wird der Einsatz von KI-Systemen regelmäßig vor allem aufgrund berechtigter Interessen nach lit. f gerechtfertigt werden können.⁸² Dabei sind die berechtigten Interessen des

⁷⁶ Heberlein in Ehmann/Selmayr, DS-GVO, Art. 5 Rn. 39.

⁷⁷ Pötters in Gola/Heckmann, DS-GVO, Art. 5 Rn. 34.

⁷⁸ Frenzel in Paal/Pauly, DS-GVO, Art. 5 Rn. 52.

⁷⁹ Schäfer, ZD 2025, 12, 14.

⁸⁰ Wilmer in Jandt/Steidle, Datenschutz und Internet, Kap. V Rn. 671; Reichert/Radtke/Eske, ZD 2024, 483, 484; Schäfer, ZD 2025, 12, 14.

⁸¹ Reichert/Radtke/Eske, ZD 2024, 483, 484.

⁸² Wilmer in Jandt/Steidle, Datenschutz und Internet, Kap. V Rn. 671; Schäfer, ZD 2025, 12, 14.

Verantwortlichen – sofern die Datenverarbeitung zur Wahrnehmung dieser Interessen erforderlich ist – mit den Interessen der betroffenen Personen abzuwägen.⁸³

Als berechtigte Interessen kommen überwiegend wirtschaftliche Interessen in Betracht, vor allem die Entwicklung innovativer Projekte zum Erhalt der Wettbewerbsfähigkeit und zur Anpassung an den technischen Fortschritt.⁸⁴ Aber auch Interessen wie Effizienzsteigerung oder Kosteneinsparung sind berücksichtigungsfähig.⁸⁵ Um darzulegen, warum die Datenverarbeitung zur Wahrnehmung dieser Interessen konkret notwendig ist, kommt es auf den jeweiligen Einzelfall an. Regelmäßig wird es genügen, wenn der Grund der Datenerhebung erläutert wird.⁸⁶

Bezüglich der Interessen der betroffenen Personen ist besonders zu beachten, ob weitere Verarbeitungen ihrer Daten zu erwarten sind⁸⁷, ob die Daten, freiwillig im Internet veröffentlicht wurden⁸⁸ und inwiefern dem Betroffenen Widerspruchsrechte zustehen.⁸⁹ Je nach Intensität des Eingriffs in die Rechte der betroffenen Personen, sind ihre Interessen stärker zu gewichten. Aus diesem Grund müssen technische Maßnahmen zur Verringerung von Art und Umfang der verarbeiteten Daten ergriffen werden, um ein positives Abwägungsergebnis zu erreichen.⁹⁰

b) Nutzung des KI-Systems

Die Datenverarbeitung während des Einsatzes eines KI-Systems ist vor allem dann relevant, wenn hierbei personenbezogene Daten „unbeteiligter“ Personen betroffen sind.⁹¹ In diesen Fällen kommt wiederum nur Art. 6 Abs. 1 lit. f DS-GVO als Rechtsgrundlage in Betracht. Auch hier kommt es also auf eine umfassende Interessenabwägung an.

4. Transparenz- und Informationspflichten, Art. 13-15 DS-GVO

Findet eine Datenverarbeitung statt, ist die betroffene Person grundsätzlich umfassend hierüber vom Verantwortlichen zu informieren, Art. 13 und 14 DS-GVO. Dabei unterscheiden sich die Anforderungen danach, ob die Daten bei der betroffenen Person erhoben wurden (Art. 13 DS-

⁸³ Schulz in Gola/Heckmann, DS-GVO – BDSG, DS-GVO, Art. 6 Rn. 59.

⁸⁴ Kloos/Schmidt-Bens in Hartmann, KI & Recht kompakt, Kap. 5, S. 176 f.; Reichert/Radtke/Eske, ZD 2024, 483, 484.

⁸⁵ Golland, EuZW 2024, 846, 849.

⁸⁶ Reichert/Radtke/Eske, ZD 2024, 483, 484.

⁸⁷ Kloos/Schmidt-Bens in Hartmann, KI & Recht kompakt, Kap. 5, S. 178.

⁸⁸ Schulz in Gola/Heckmann, DS-GVO, Art. 6 Rn. 63.

⁸⁹ Bolek-Fügl in Windholz, KI-VO, Praxishandbuch, Kap. 4 S. 193.

⁹⁰ Kloos/Schmidt-Bens in Hartmann, KI & Recht kompakt, Kap. 5, S. 178; Reichert/Radtke/Eske, ZD 2024, 483, 484.

⁹¹ Wilmer in Jandt/Steidle, Datenschutz und Internet, Kap. V Rn. 673.

GVO) oder nicht (Art. 14 DS-GVO). Zugleich wird dem Betroffenen auch ein Auskunftsrecht nach Art. 15 DS-GVO gewährt.

Diese Pflichten sind eng mit dem Transparenzgrundsatz aus Art. 5 Abs. 1 lit. a DS-GVO verknüpft, da sie gerade Durchsichtigkeit bei der Verarbeitung personenbezogener Daten gewährleisten sollen, um es den betroffenen Personen zu ermöglichen, ihre Rechte aus Art. 15-21 DS-GVO effektiv wahrzunehmen.⁹² Das ergibt sich schon daraus, dass es betroffenen Personen im Rahmen des Auskunftsrechts möglich sein soll, die Rechtmäßigkeit der Verarbeitung überprüfen zu können (ErwG 63 S. 1 DS-GVO). Durch Übermittlung von Existenz, Umständen und Zweck der Verarbeitung soll den Betroffenen ein möglichst fairer und transparenter Einblick gewährt werden (ErwG 60 S. 1 DS-GVO).⁹³ Dem dient auch Art. 12 Abs. 1 DS-GVO, wonach die Informationserteilung in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen hat (ErwG 58 S. 1 DS-GVO).

Eine besondere Verpflichtung besteht bei ausschließlich automatisierten Entscheidungen im Sinne des Art. 22 DS-GVO. Werden solche Verfahren verwendet, muss nach Art. 13 Abs. 2 lit. f DS-GVO bzw. Art. 14 Abs. 2 lit. g DS-GVO sowohl über das Bestehen automatisierter Entscheidungsfindung als auch über die „involvierte Logik“ sowie Tragweite und Ausweitungen der Verarbeitungen informiert werden.

Sofern das KI-System öffentlich zugängliche Daten verarbeitet, ist die Informationserteilung dementsprechend erschwert. In diesen Fällen ist eine Informationspflicht ausnahmsweise abzulehnen, wenn deren Erfüllung mit einem unverhältnismäßigen Aufwand einhergehen würde (Art. 14 Abs. 5 lit. b DS-GVO).⁹⁴ Je nach KI-System wird das Unternehmen nicht imstande sein, alle Personen, deren Daten verarbeitet wurden, zu kontaktieren – vor allem wenn das KI-System Zugriff auf große Datenbestände hat.⁹⁵

5. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung, Art. 25 DS-GVO

Nach den Grundsätzen des Art. 25 DS-GVO unterliegt eine Datenverarbeitung schon in ihrer Entwicklungsphase bestimmten Anforderungen, da im Fall von KI-Systemen schon dessen Entwickler dazu gezwungen werden, Datenschutzmaßnahmen in ihre Systeme zu integrieren.

⁹² *Bolek-Fügl* in Windholz, KI-VO, Praxishandbuch, Kap. 4 S. 193.

⁹³ *Hoeren/Niehoff*, RW 2018, 47, 54 f.

⁹⁴ *Conrad* in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 34 Rn. 582.

⁹⁵ *Golland*, EuZW 2024, 846, 851.

Art. 25 Abs. 1 DS-GVO verlangt eine datenschutzgerechte Systemgestaltung („privacy by design“) – Datenschutz muss schon bei Entwicklung und Konzeption von Verarbeitungsprozessen berücksichtigt werden.⁹⁶ Das soll gewährleisten, dass die in Art. 5 DS-GVO niedergeschriebenen Datenschutzprinzipien eingehalten werden können.⁹⁷ Für KI-Systeme bedeutet das, dass Hard- und Software, Plattformen sowie Dienstleistungen so ausgewählt werden müssen, dass eine datenschutzgerechte Datenverarbeitung möglich ist.⁹⁸

Das Erfordernis datenschutzfreundlicher Voreinstellungen nach Art. 25 Abs. 2 DS-GVO verpflichtet den Verantwortlichen dazu, geeignete technische und organisatorische Maßnahmen zu treffen, die die Zweckbindung der Datenverarbeitung sicherstellen („privacy by default“). Es dürfen nur die für den Zweck erforderlichen Daten verarbeitet werden.

Gerade im Hinblick auf die großen Datenmengen, die verarbeitet werden, ergeben sich hier gewichtige Probleme. Diese von KI-Systemen ausgehenden Risiken können jedoch durch die vorzeitige Implementierung verschiedener Elemente – etwa Verschlüsselung, Anonymisierung und Pseudonymisierung oder die Identitätsverschleierung sowie sichere Datenfreigabe-Tools – verringert werden und gewährleisten so die Einhaltung der Datenschutzanforderungen.⁹⁹

Art. 25 DS-GVO unterstreicht daher die Wichtigkeit von vorbeugendem und vorausschauendem Datenschutz.¹⁰⁰

6. Datenschutz-Folgenabschätzung, Art. 35 DS-GVO

Die Datenschutz-Folgenabschätzung ist zentrales Instrument, um zu prüfen, ob der Einsatz von KI-System zur Datenverarbeitung geeignet ist.¹⁰¹

Dabei wird eine Erforderlichkeitsprüfung vorgenommen, Art. 35 Abs. 1 S. 1 DS-GVO. Hier soll festgestellt werden, ob die Form der Datenverarbeitung aufgrund Art, Umfang oder Zweck der Verarbeitung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt. Dies ist häufig bei Profiling, automatisierten Entscheidungen oder umfangreicher Verarbeitung sensibler Daten der Fall.¹⁰² Die Risiken können zu Schäden für die Betroffenen führen, insbesondere wenn die Verarbeitung etwa zu Diskriminierung, Identitätsdiebstahl oder Rufschädigung führt (ErwG 75 S. 1 DS-GVO).

⁹⁶ *Bolek-Fügl* in Windholz, KI-VO, Praxishandbuch, Kap. 4 S. 197.

⁹⁷ *Richter* in Jandt/Steidle, Datenschutz und Internet, Kap. VI Rn. 11; *Roßnagel*, MMR 2023, 64, 66.

⁹⁸ *Roßnagel*, MMR 2023, 64, 66.

⁹⁹ *Schürmann*, ZD 2022, 316, 319.

¹⁰⁰ *Bolek-Fügl* in Windholz, KI-VO, Praxishandbuch, Kap. 4 S. 197.

¹⁰¹ *Schürmann*, ZD 2022, 316, 319.

¹⁰² *Golland*, EuZW 2024, 846, 853.

Ein besonderes Bedürfnis für die Durchführung einer Datenschutz-Folgenabschätzung besteht bei der Verarbeitung großer Mengen personenbezogener Daten (ErwG 91 S. 1 DS-GVO). Daher wird aufgrund der Unabdingbarkeit von Big Data-Analysen beim Einsatz von KI-System hier regelmäßig die Durchführung einer Datenschutz-Folgenabschätzung erforderlich sein.¹⁰³

Die Risikobewertung – und die daraus folgenden Abhilfemaßnahmen – stellen den Hauptteil der Datenschutz-Folgenabschätzung dar. Dabei ist die Eintrittswahrscheinlichkeit und Schwere des Risikos bezüglich der Datenverarbeitung zu ermitteln und anhand einer objektiven Bewertung zu beurteilen, ob die Verarbeitung ein Risiko oder ein hohes Risiko birgt (ErwG 76 S. 1, 2 DS-GVO). Geht daraus hervor, dass ein hohes Risiko vorliegt, trifft der Verantwortliche Abhilfemaßnahmen – idealerweise unter Rückgriff auf ein schon vorhandenes Schutzkonzept zur Gewährleistung von Datensicherheit.¹⁰⁴

II. Verordnung über künstliche Intelligenz

Mit der KI-VO wurde erstmals ein unionsweit einheitlicher, horizontal angelegter Rechtsrahmen geschaffen, der die Entwicklung, Bereitstellung und Nutzung von KI in ihrer gesamten Breite adressiert.¹⁰⁵ Die KI-VO verfolgt einerseits das Ziel, einen einheitlichen europäischen Rechtsrahmen für den Einsatz von KI zu schaffen und Innovation zu fördern sowie andererseits Risiken für Grundrechte, Gesundheit und Sicherheit wirksam zu begrenzen, Art. 1 KI-VO. Damit ist die KI-VO nicht nur ein lediglich sektorspezifisches Technikrecht, sondern ein eigenständiger Ordnungsrahmen für den Umgang mit KI-Systemen in Unternehmen.

Anders als die DS-GVO, die an die Verarbeitung personenbezogener Daten anknüpft und damit personenbezogen ausgestaltet ist, verfolgt die KI-VO einen primär system- und risikobezogenen Regulierungsansatz. Im Ausgangspunkt steht vor allem die Frage um das Gefährdungspotenzial, das von einem KI-System aufgrund seines Einsatzkontexts, seines Funktionsumfangs und seiner Auswirkungen auf Sicherheit und Grundrechte ausgeht. Gerade darin liegt ihre erhebliche Bedeutung für die Corporate Governance: Die KI-VO zwingt Unternehmen dazu, KI nicht nur als technisches Werkzeug, sondern als regelungsbedürftigen Organisationsgegenstand zu begreifen.

Für Unternehmen folgt daraus, dass die KI-VO einen zentralen Anknüpfungspunkt bildet zur Ausgestaltung eines unternehmensweiten KI-Governance-Modells, wobei sich der Umfang der

¹⁰³ Wilmer in Jandt/Steidle, Datenschutz und Internet, Kap. V Rn. 679.

¹⁰⁴ Kloos/Schmidt-Bens in Hartmann, KI & Recht kompakt, Kap. 5, S. 206.

¹⁰⁵ Hoeren/Pinelli, KIR 2026, 5.

einzuhaltenden Pflichten maßgeblich nach dem jeweiligen Risikopotenzial des KI-Systems bestimmt.

1. Anbieter und Betreiber von KI-Systemen

Die Pflichten der KI-VO knüpfen zunächst an die Rolle des Unternehmens im Lebenszyklus des KI-Systems an. Zu unterscheiden ist insbesondere, ob das Unternehmen Anbieter oder Betreiber ist.

Anbieter im Sinne des Art. 3 Nr. 3 KI-VO sind solche Akteure, die ein KI-System entwickeln (lassen) und es unter eigenem Namen in den Verkehr bringen oder in Betrieb nehmen. Betreiber im Sinne des Art. 3 Nr. 4 KI-VO hingegen verwenden ein KI-System in eigener Verantwortung im Rahmen einer beruflichen Tätigkeit. Sie sind bloße Nutzer.¹⁰⁶

Für die Unternehmenspraxis ist diese Abgrenzung von erheblicher Bedeutung, da die KI-VO die normierten Pflichten an dieser Rollenzuweisung ausrichtet.¹⁰⁷ Dabei kann das Unternehmen jedoch je nach Konstellation Anbieter, Betreiber oder auch beides zugleich sein.

2. Risikoklassifizierung von KI-Systemen

Zentraler Bestandteil der KI-VO ist die Einteilung von KI-Systemen nach den von ihnen ausgehenden Risiken für Gesundheit, Sicherheit oder Grundrechte für natürliche Personen. Die Verordnung unterscheidet zwischen verbotenen KI-Systemen, Hochrisiko KI-Systemen und KI-Systemen mit geringem oder minimalem Risiko. Maßgeblich ist damit nicht die Technologie als solche, sondern die konkrete Gefährdungslage ihres Einsatzes.

KI-Systeme mit inakzeptablen Risiken unterfallen den verbotenen KI-Systemen (Kapitel II der KI-VO) und definieren insofern eine rote Linie für die Unternehmens-Governance. Art. 5 KI-VO enthält einen abschließenden Katalog verbotener KI-Praktiken, die weder entwickelt noch eingesetzt werden dürfen aufgrund ihrer Gefahr für Grundrechte und Sicherheit.¹⁰⁸

Von besonderer Relevanz für die Unternehmenspraxis sind die Hochrisiko-KI-Systeme. Hieran knüpft das dichteste Pflichtenprogramm der KI-VO an. Aus diesem Grund müssen Unternehmen einen Prozess zur Risikoklassifizierung etablieren, um den Vorgaben der KI-VO gerecht werden zu können.¹⁰⁹ Sie müssen einen belastbaren Prozess schaffen, mit dem beurteilt werden kann, welchen Risikogehalt ein KI-System aufweist und in welche Risikokategorie es

¹⁰⁶ Golland, EuZW 2024, 846, 852.

¹⁰⁷ Eger/Schmuck in Wieland/Steinmeyer/Grüniger, HdB Compliance-Management, Teil I. Kap. 4.1 Rn. 11.

¹⁰⁸ Lühmann/Görgülü/Marciniak, BKR 2024, 175, 180; Teichmann, ZD 2025, 495, 496.

¹⁰⁹ Sassenberg, RD 2025, 346, 347 f.

demnach einzuordnen ist oder ob es „nur“ den allgemeinen Anforderungen unterliegt, etwa Art. 4 oder Art. 50 KI-VO.¹¹⁰

Regelungen zu den Hochrisiko-KI-Systemen finden sich in Kapitel III der KI-VO. Dabei enthält Art. 6 KI-VO detaillierte Kriterien zu der Frage, wann ein KI-System als Hochrisiko-KI gilt. Dabei werden zwei Fallgruppen erfasst: KI-Systeme, die Sicherheitsfunktionen in Produkten übernehmen und KI-Systeme, die in bestimmten Hochrisiko-Bereichen eingesetzt werden.¹¹¹ Das ist vor allem abhängig vom Zweck, den Funktionen und den Anwendungsmodalitäten des Systems.¹¹² In der Praxis betrifft diese Einstufung nur einen begrenzten Teil der KI-Anwendungen, ist jedoch mit besonders weitreichenden Pflichten verbunden.¹¹³

Im Umkehrschluss aus beiden Kategorisierungen ergibt sich, dass alles, was nicht hierunter fällt, als KI mit geringem oder minimalem Risiko einzuordnen ist. Diese sind zwar nicht gesondert definiert, dennoch verbleibt hierfür die Erfüllung der risikoneutral ausgestalteten Pflichten – insbesondere die Anforderungen an KI-Kompetenz aus Art. 4 KI-VO sowie die Transparenzpflichten aus Art. 50 KI-VO.

Daneben enthält die KI-VO in Kapitel V weitere Regelungen zu KI mit speziellen, systemischen Risiken.¹¹⁴ Dabei handelt es sich jedoch nicht um eine eigenständige Risikokategorie, sondern eine zusätzliche Regulierungsebene für besonders leistungsfähige KI-Modelle – die General-Purpose-AI-Modelle.¹¹⁵

3. Pflichten der KI-VO

a) KI-Kompetenz, Art. 4 KI-VO

Im Mittelpunkt steht die von Art. 4 KI-VO geforderte KI-Kompetenz, wonach Unternehmen verpflichtet werden, ein angemessenes Maß an KI-Kompetenz bei Mitarbeitenden und weiteren betroffenen Personen sicherzustellen. Diese Pflicht ist gerade deshalb besonders relevant, weil sie rollenübergreifend und risikoneutral ausgestaltet ist: Sie gilt nicht nur für Hochrisiko-KI und ist sowohl an Anbieter sowie Betreiber gleichermaßen gerichtet¹¹⁶. Sie gilt stattdessen prinzipiell überall dort, wo KI im Unternehmenskontext eingesetzt wird.

¹¹⁰ Sassenberg, RDi 2025, 346, 347 f.

¹¹¹ Teichmann, ZD 2025, 495, 496.

¹¹² Lüthmann/Görgülü/Marciniak, BKR 2024, 175, 180.

¹¹³ Sassenberg, RDi 2025, 346, 347.

¹¹⁴ Mackert/Ernst in Wieland/Steinmeyer/Grüniger, HdB Compliance-Management, Teil I. Kap. 1.4 Rn. 34.

¹¹⁵ Lüthmann/Görgülü/Marciniak, BKR 2024, 175, 180.

¹¹⁶ Wendehorst in Martini/Wendehorst, KI-VO, Art. 4 Rn. 3 f.

Der Begriff der KI-Kompetenz umfasst nach Art. 3 Nr. 56 KI-VO die „Fähigkeiten, die Kenntnisse und das Verständnis, die es [...] ermöglichen, KI sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden [...] bewusst zu sein.“ Damit erschöpft sich Art. 4 KI-VO nicht in einem bloßen Schulungsangebot. Verlangt wird vielmehr die Schaffung organisatorischer Voraussetzungen dafür, dass Mitarbeitende KI-Systeme kontextbezogen, verantwortungsvoll und rechtssicher einsetzen können.¹¹⁷

Die Vorschrift verlangt ein grundlegendes technisches Verständnis der Funktionsweise von KI-Systemen hinsichtlich der Wirkungsweise algorithmischer Entscheidungsmodelle sowie der zugrundeliegenden Optimierungs- und Gewichtungsmechanismen.¹¹⁸ Auch sind rechtliche Kenntnisse – Transparenzpflichten, Verbotstatbestände und Haftungsrisiken – sowie ein ethisches Grundverständnis – Vermeidung diskriminierender Auswirkungen – zu vermitteln.¹¹⁹ Die Verpflichtungen bestehen über den gesamten KI-Einsatz hinweg, sodass sie als Dauerverpflichtung nur durch institutionalisierbare Lern- und Kontrollstrukturen erfüllt werden können.¹²⁰

Als KI-kompetent gilt, wer KI-Systeme kontextbezogen, rechtskonform und verantwortungsvoll handhaben sowie ihre Risiken sachgerecht erfassen kann (ErwG 20 KI-VO).¹²¹

b) Anforderungen an Hochrisiko-KI-Systeme, Art. 8 ff. KI-VO

aa) Anbieter

Wird ein KI-System als Hochrisiko-KI eingeordnet, greift ein umfassendes Pflichtensystem ein. Anbieter müssen insbesondere ein Risikomanagementsystem etablieren, Vorgaben bezüglich Datenqualität einhalten, technische Dokumentationen erstellen, Transparenz sicherstellen, menschliche Aufsicht ermöglichen sowie Anforderungen an Genauigkeit, Robustheit und Cybersicherheit erfüllen.

Art. 9 KI-VO verlangt ein fortlaufendes Risikomanagementsystem, das über den gesamten Lebenszyklus der KI hinweg angewendet wird. Das dient der Identifikation und Bewertung von Risiken, um geeignete Maßnahmen zu deren Bewältigung zu ergreifen und Nutzer über mögliche Restrisiken zu informieren.¹²² Erfasst werden dabei nicht nur technische

¹¹⁷ *Rappenglück/Vonthien*, RD i 2025, 398, 402.

¹¹⁸ *Rappenglück/Vonthien*, RD i 2025, 398, 400.

¹¹⁹ *Cretu* in Windholz, KI-VO, Praxishandbuch, Kap. 3 S. 49 f.; *Rappenglück/Vonthien*, RD i 2025, 398, 400.

¹²⁰ *Rappenglück/Vonthien*, RD i 2025, 398, 402.

¹²¹ *Schwartmann/Köhler* in Schwartmann/Keber/Zenner, KI-VO, S. 53.

¹²² *Windholz* in Windholz, KI-VO, Praxishandbuch, Kap. 3 S. 80 f.; *Binder/Egli*, MMR 2024, 626, 628.

Modellrisiken wie Bias, Rückkopplungen oder Fehlerraten, sondern ebenso operative, regulatorische, IT-sicherheitsbezogene und grundrechtsbezogene Risiken.¹²³

Art. 10 KI-VO konkretisiert diese Steuerungsperspektive für die Daten-Governance. Es werden Anforderungen an die Daten festgelegt, mit denen die KI trainiert wird – vor allem bezüglich Datenquellen, Verarbeitungsprozessen, Speicherorten, Qualitätskriterien und Schutzmechanismen. Die Abs. 2-5 legen hierfür bestimmte Qualitätskriterien fest, die die Daten erfüllen müssen.

Hinzu tritt die Pflicht zur technischen Dokumentation nach Art. 11 KI-VO sowie weitere Nachweis- und Protokollierungspflichten. Der Anbieter muss bereits vor Inverkehrbringen des KI-Systems eine technische Dokumentation erstellen und ausführliche Unterlagen zum KI-System bereithalten.¹²⁴ Gerade das macht den Entwicklungs- und Einsatzprozess erst überprüfbar.

Ebenso zentral ist Art. 14 KI-VO zur menschlichen Aufsicht. Die Norm verlangt, dass Hochrisiko-KI so konzipiert und entwickelt werden, dass sie während ihres gesamten Lebenszyklus von natürlichen Personen wirksam beaufsichtigt werden können (sog. Mensch-Maschine-Schnittstelle).¹²⁵ Menschliche Aufsicht ist damit ein Teil des Systemdesigns.

Schließlich wird in Art. 15 KI-VO ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit hinsichtlich des Verwendungszwecks des Hochrisiko-KI-Systems verlangt.

Diese Pflichten weisen eine deutliche Nähe zu klassischen Corporate-Governance-Anforderungen auf. Sie konkretisieren die Pflicht zur ordnungsgemäßen Organisation und Überwachung und begründen einen eigenständigen Compliance-Bereich für KI-Systeme.

bb) Betreiber

Für den Betreiber ergeben sich aus dem Risikocharakter von KI-Systemen vor allem Beobachtungspflichten.¹²⁶ Vor allem konkretisiert Art. 26 KI-VO, wie Hochrisiko-KI organisatorisch rechtssicher eingesetzt werden müssen, um die Konformität des KI-Systems mit den Anforderungen der KI-VO sicherzustellen.¹²⁷ Insofern kommt der Norm zentrale Bedeutung zu, da sie die Ebene des operativen Einsatzes adressiert und unmittelbar an interne

¹²³ Mackert/Ernst in Wieland/Steinmeyer/Grüniger, HdB Compliance-Management, Teil I. Kap. 1.4 Rn. 34.

¹²⁴ Teichmann, ZD 2025, 495, 497.

¹²⁵ Martini in Paal/Pauly, DS-GVO, Art. 22 Rn. 7d; Lühmann/Görgülü/Marciniak, BKR 2024, 175, 180.

¹²⁶ Förster, KI-VO in der Praxis, § 2 Rn. 217.

¹²⁷ Hoeren/Pinelli, KIR 2026, 5, 8.

Zuständigkeiten und Kontrollmechanismen anschließt.

Vor allem verpflichtet Art. 26 Abs. 1 KI-VO die Betreiber dazu, Hochrisiko-KI-Systeme entsprechend der beigelegten Gebrauchsanleitung zu verwenden sowie die vorgeschriebenen menschlichen Überwachungsmaßnahmen zu befolgen, Art. 26 Abs. 2 KI-VO. Hier eignet sich vor allem die Implementierung organisatorischer Maßnahmen, wie Protokollierungs- und Überwachungspflichten, das Vier-Augen-Prinzip oder der Aufbau wirksamer Compliance-Strukturen.¹²⁸

Die tatsächliche Ausübung der menschlichen Aufsichtspflicht erfordert jedoch, dass die beaufsichtigende Person auch über die erforderliche Kompetenz und Autorität verfügt, wodurch hier Art. 26 KI-VO und Art. 4 KI-VO aufeinandertreffen.¹²⁹

Ferner verlangt Art. 26 Abs. 4 KI-VO, dass Betreiber die Eingabedaten im Hinblick auf Zweckbestimmung und Repräsentanz prüfen.¹³⁰ Das ist wiederum eng verknüpft mit den Anbieterpflichten aus Art. 10 Abs. 2 und 3 KI-VO, wonach dieser für die Qualität der Daten einzustehen hat.

Zuletzt treten hier noch hinzu Überwachungs-, Protokollierungs- und Mitwirkungspflichten, Art. 26 Abs. 5 KI-VO. Der Betreiber muss potenzielle Risiken oder Fehlfunktionen melden, die sich aus seiner Ausübung der menschlichen Aufsichtspflicht ergeben.¹³¹ Art. 26 KI-VO strukturiert damit die operative Seite des KI-Einsatzes und zwingt Unternehmen so, die Nutzung der KI-Systeme in kontrollierte Betriebsprozesse einzubetten.

c) Transparenzpflichten

Schließlich enthält die KI-VO ein eigenständiges, umfangreiches Transparenzregime. Diese Pflichten stehen in einem funktionalen Zusammenhang mit den Transparenzanforderungen der DSGVO, unterscheiden sich jedoch in ihrer Zielrichtung. Im Kontext der KI-VO bedeutet Transparenz, dass KI-Systeme so entwickelt und eingesetzt werden müssen, dass die Nachvollziehbarkeit, Erklärbarkeit sowie kontrollierte Verwendung von KI-Systemen ermöglicht wird.¹³²

¹²⁸ Denga in BeckOK KI-Recht, KI-VO, Art. 26 Rn. 26; Hoeren/Pinelli, KIR 2026, 5, 8,

¹²⁹ Hafez in Windholz, KI-VO, Praxishandbuch, Kap. 10 S. 458.

¹³⁰ Förster, KI-VO in der Praxis, § 2 Rn. 231.

¹³¹ Lüthmann/Görgülü/Marciniak, BKR 2024, 175, 180.

¹³² Cretu in Windholz, KI-VO, Praxishandbuch, Kap. 3 S. 122 f.

aa) Art. 13 KI-VO

Für Hochrisiko-KI ist dies gesondert in Art. 13 KI-VO geregelt.

Der Anbieter muss das KI-System so ausgestalten, dass dessen Betrieb für den Betreiber hinreichend transparent ist und die bereitgestellten Informationen eine sachgerechte Nutzung und Überwachung ermöglichen. Vor allem muss eine Gebrauchsanleitung bereitgestellt werden, die Angaben zu Zweck, Leistungsgrenzen, Funktionsumfang und Aufsichtsmaßnahmen enthält.¹³³ Aber auch die vom System gestellten Anforderungen an die Input-Datenqualität und bestehende Risiken bei Falschnutzung müssen erläutert werden.¹³⁴

Dies hat den Hintergrund, der fehlenden Erklärbarkeit und Intransparenz verschiedener KI-Systeme – der Blackbox-Problematik – zu begegnen.¹³⁵ Transparenz ist daher die Voraussetzung wirksamer organisatorischer Aufsicht. Ohne hinreichende Informationen kann weder eine qualifizierte menschliche Kontrolle noch eine belastbare Freigabe- und Dokumentationsentscheidung erfolgen.¹³⁶

bb) Art. 50 KI-VO

Art. 50 KI-VO betrifft demgegenüber allgemeine Transparenzpflichten für bestimmte KI-Anwendungen. Diese greifen vor allem bei solchen KI-Anwendungen ein, bei denen Menschen mit einem KI-System interagieren oder von KI-generierten bzw. manipulierten Inhalte betroffen sind.¹³⁷

Hier verschiebt sich die Zielrichtung stärker auf den Schutz der Betroffenen anstatt des Betreibers – so sollen Täuschungsgefahren reduziert und ein Mindestmaß an Aufklärung gewährleistet werden.¹³⁸ Dem Menschen muss bewusst gemacht werden, dass er mit einem KI-System interagiert. Dabei hängt die Umsetzung dieser Anforderungen maßgeblich von der Art des KI-Systems und der Form der Interaktion ab, sodass diese Vorgaben konkret in die jeweilige Unternehmens-Governance übersetzt werden müssen.¹³⁹

Dabei muss das Maß an Transparenz an dem von der KI ausgehenden Risiko gemessen werden (Grundsatz der Verhältnismäßigkeit).¹⁴⁰

¹³³ Förster, KI-VO in der Praxis, § 2 Rn. 89 ff.

¹³⁴ Teichmann, ZD 2025, 495, 496.

¹³⁵ Martini in Martini/Wendehorst, KI-VO, Art. 13 Rn. 1.

¹³⁶ Hoeren/Pinelli, KIR 2026, 5, 6.

¹³⁷ Lüthmann/Görgülü/Marciniak, BKR 2024, 175, 181; Sassenberg, RD 2025, 346, 351.

¹³⁸ Zech/Linhart, BeckOK KI-Recht, KI-VO, Art. 13 Rn. 3; Teichmann, ZD 2025, 495, 496.

¹³⁹ Merkle in Bomhard/Pieper/Wende, KI-VO, Art. 50 Rn. 40.

¹⁴⁰ Cretu in Windholz, KI-VO, Praxishandbuch, Kap. 3 S. 123.

III. Zusammenspiel von DS-GVO und KI-VO

Der Einsatz von KI-Systemen in Unternehmen unterliegt nicht einem einheitlichen Regulierungsregime, sondern einem Zusammenspiel verschiedener Regelungswerke. Dabei sind die DS-GVO und die KI-VO besonders prägend, stellen jedoch keinen konkurrierenden, sondern einen sich ergänzenden Rechtsrahmen dar. Die DS-GVO bleibt von der KI-VO unberührt, (Art. 2 Abs. 7 KI-VO, ErwG 10 S. 4 KI-VO). Vielmehr soll die KI-VO hier ergänzend fungieren.¹⁴¹

Beide Verordnungen adressieren unterschiedliche Risikodimensionen digitaler Technologien, greifen jedoch dort ineinander, wo KI-Systeme personenbezogene Daten verarbeiten oder Entscheidungen über natürliche Personen vorbereiten oder beeinflussen.

1. Regelungsziele

Während die KI-VO einen primär systembezogenen Regulierungsansatz verfolgt, ist die DS-GVO personenbezogen ausgestaltet. Ausgangspunkt der KI-VO ist das Risiko, das von einem KI-System für Gesundheit, Sicherheit oder Grundrechte ausgehen kann. Dementsprechend knüpfen ihre Regelungen vor allem an den Lebenszyklus eines KI-Systems an – von der Entwicklung über das Inverkehrbringen bis zum operativen Einsatz. Ziel ist es, sicherzustellen, dass KI-Systeme so konzipiert, implementiert und betrieben werden, dass ihre Risiken beherrschbar bleiben.

Demgegenüber ist Regelungsgegenstand der DS-GVO nicht das technische System selbst, sondern die Verarbeitung personenbezogener Daten. Sie adressiert daher vor allem Risiken für das Grundrecht auf informationelle Selbstbestimmung sowie die Rechte und Freiheiten natürlicher Personen.

Sofern KI-Systeme personenbezogene Daten verarbeiten und dementsprechend von der KI Risiken hierfür ausgehen – wie etwa mangelnde Erklärbarkeit, die daraus folgende Intransparenz, Verzerrungen in Trainingsdaten oder strukturelle Diskriminierungsrisiken – überschneiden sich DS-GVO und KI-VO. Verarbeiten KI-Systeme personenbezogene Daten, wirken deren Vorgaben ebenso grundrechtsschützend im Sinne der Zielsetzung der DS-GVO.

Die KI-VO ergänzt die DS-GVO daher vorwiegend dort, wo KI-spezifische Risiken auftreten, die nicht hinreichend durch das datenschutzrechtliche Instrumentarium allein erfasst werden können. Dies vor allem, da die DS-GVO selbst technologieneutral ausgestaltet ist.

¹⁴¹ Orssisch, EuZW 2022, 254, 256.

Demgegenüber begrenzen die Grundsätze der DS-GVO – insbesondere Transparenz, Zweckbindung, Datenminimierung und Richtigkeit – den Einsatz von KI unabhängig von der risikorechtlichen Einordnung nach der KI-VO.

Beide Regelwerke verfolgen damit unterschiedliche Regelungsansätze, greifen jedoch funktional ineinander und adressieren unterschiedliche Facetten desselben Risikopotentials. Beide Rechtsakte zielen auf Transparenz, Nachvollziehbarkeit, Risikominimierung und Verantwortlichkeit ab.

In der Unternehmenspraxis ergibt sich daraus ein kumulativer Pflichtenkreis: Unternehmen müssen sowohl die systembezogenen Anforderungen der KI-VO als auch die personenbezogenen Schutzmechanismen der DS-GVO beachten. Eine effektive KI-Governance muss daher beiden Regelungsregimen gerecht werden: es müssen Überschneidungen koordiniert, Doppelregulierungen vermieden und zugleich ein wirksamer Schutz der betroffenen Personen sichergestellt werden.¹⁴²

2. Funktionale Ergänzung der Pflichtenkataloge

Viele der von der KI-VO adressierten Risiken stehen in engem Zusammenhang mit den datenschutzrechtlichen Schutzgütern der DS-GVO.

Vor allem dient zunächst die Pflicht zur KI-Kompetenz aus Art. 4 KI-VO der Vorbeugung datenschutzrechtlicher Verstöße, etwa wenn personenbezogene Daten unbedacht in externe Systeme eingegeben oder Ausgaben ungeprüft übernommen werden. Insofern ergänzt Art. 4 KI-VO die datenschutzrechtliche Rechenschaftsstruktur.

Auch die Anforderungen der KI-VO an Datenqualität aus Art. 9 KI-VO sowie Art. 26 Abs. 4 KI-VO zielen darauf ab, verzerrte oder diskriminierende Ergebnisse algorithmischer Systeme zu vermeiden. Dies ergänzt die datenschutzrechtlichen Grundsätze der Zweckbindung, Datenminimierung oder Datenrichtigkeit aus Art. 5 Abs. 1 DS-GVO in funktionaler Hinsicht. Beide Regelwerke verfolgen damit letztlich das Ziel, Fehlentscheidungen aufgrund ungeeigneter oder verzerrter Daten zu verhindern.

Ähnliches gilt für die Anforderungen an Transparenz und Nachvollziehbarkeit. Während Art. 13, 14 DS-GVO die Information betroffener Personen verlangen, zielen die

¹⁴² Schröder in Schröder, Datenschutzrecht für die Praxis, Kap. 8 S. 268.

Transparenzpflichten der KI-VO primär auf die interne und behördliche Kontrollierbarkeit der Systeme ab – nur sekundär werden im Rahmen von Art. 50 KI-VO die Betroffenen informiert. Unternehmen müssen so Transparenz nicht nur nach außen, sondern auch nach innen gewährleisten. Sowohl DS-GVO als auch KI-VO fördern damit die Nachvollziehbarkeit algorithmischer Entscheidungsprozesse, wenn auch aus unterschiedlichen Perspektiven.

Konvergenzen zeigen sich auch bei der menschlichen Kontrolle automatisierter Systeme. Die KI-VO verlangt in Art. 14 KI-VO eine wirksame menschliche Aufsicht von KI-Systemen, die von den Betreibern nach Art. 26 Abs. 3 KI-VO ausgeübt wird. Demgegenüber verfolgt die DS-GVO ein ähnliches Ziel im Rahmen des Verbots ausschließlich automatisierter Entscheidungen aus Art. 22 DS-GVO. In beiden Fällen soll verhindert werden, dass Entscheidungen mit erheblichen Auswirkungen auf natürliche Personen vollständig automatisiert erfolgen, ohne dass eine menschliche Überprüfung möglich ist.

3. Überschneidungen in der Unternehmenspraxis

In der Unternehmenspraxis entstehen aus diesem Zusammenspiel häufig überschneidende Pflichten, was vor allem im Bereich Risikomanagement, Dokumentation und organisatorische Kontrolle deutlich wird.

Sowohl die KI-VO als auch die DS-GVO verlangen eine systematische Bewertung der Risiken digitaler Systeme. Während die KI-VO für Hochrisiko-KI-Systeme ein umfassendes Risikomanagementsystem vorsieht, verlangt die DS-GVO bei risikoreichen Datenverarbeitungen die Durchführung einer Datenschutz-Folgenabschätzung, Art. 35 DS-GVO. Beide Instrumente verlangen eine strukturierte Identifikation, Bewertung und Minimierung von Risiken. Diese Parallelität legt es nahe, Datenschutz-Folgenabschätzungsprozesse und KI-Risikomanagementsysteme systemisch gemeinsam vorzunehmen.

Auch im Bereich der Dokumentation bestehen Ähnlichkeiten. Die KI-VO verpflichtet Anbieter und Betreiber zur Erstellung technischer Dokumentationen und zur Protokollierung bestimmter Systemvorgänge, Art. 11 KI-VO. Die DS-GVO fordert ihrerseits umfangreiche Nachweispflichten im Rahmen der datenschutzrechtlichen Rechenschaftspflicht, Art. 5 Abs. 2 DS-GVO. In der Unternehmenspraxis können diese Anforderungen häufig miteinander kombiniert werden.

4. Konsequenzen für die Corporate Governance

Aus dem Zusammenspiel von KI-VO und DS-GVO ergibt sich für Unternehmen verschiedene nebeneinanderher bestehende Pflichten. Der Einsatz von KI muss den Anforderungen beider Regelungswerke entsprechen.

Hier zeigt sich die zentrale Rolle eines unternehmensinternen KI-Governance-Systems. Das Unternehmen muss die Vorgaben in konkrete Organisationsstrukturen übersetzen und eine integrierte Steuerung der unterschiedlichen regulatorischen Anforderungen ohne Überschneidungen ermöglichen. Die normativen Vorgaben beider Verordnungen müssen in unternehmensinterne Prozesse eingearbeitet, Verantwortlichkeiten klar zugewiesen und Risiken vorausschauend adressiert werden.

D. Datenschutzrechtliche Grenzen der automatisierten Entscheidungsfindung

Immer häufiger werden KI-Systeme in der Unternehmenspraxis in automatisierten Entscheidungen angewendet. Mit dem Einsatz von KI-Systemen gehen jedoch auch Probleme einher, wie der Blackbox-Effekt oder die daraus resultierenden Diskriminierungen und Verzerrungen – dem soll zumindest teilweise über Art. 22 DS-GVO abgeholfen werden.¹⁴³ Hiernach stößt der Einsatz von KI-Systemen an datenschutzrechtliche Grenzen, wo Entscheidungen erhebliche Auswirkungen auf betroffene Personen entfalten und ohne hinreichende menschliche Beteiligung getroffen werden.

Besonderes Schutzinstrument und damit zentraler Anknüpfungspunkt ist insofern das in Art. 22 DS-GVO normierte Verbot, das durch seine strengen Regeln einen wichtigen Mechanismus zum Schutz der betroffenen Personen vor den Risiken und damit verbundenen Nachteilen automatisierter Entscheidungsfindung darstellt.¹⁴⁴ Denn neben den allgemeinen Voraussetzungen der Art. 5 ff. DS-GVO – insbesondere dem Transparenzgrundsatz aus Art. 5 Abs. 1 lit. a DS-GVO – müssen ausschließlich automatisierte Entscheidungen auch der speziellen Richtigkeits- und Plausibilitätskontrolle des Art. 22 DS-GVO genügen.¹⁴⁵ Die Norm gibt den Betroffenen das Recht, nicht Entscheidungen unterworfen zu werden, die rechtliche oder jedenfalls erhebliche Auswirkungen haben, ohne dass hierbei eine menschliche Überprüfung stattgefunden hätte.

¹⁴³ Scholz in Simitis/Hornung/Spiecker gen. Döhmman, DS-GVO, Art. 22 Rn. 12 f.

¹⁴⁴ Bolek-Fügl in Windholz, KI-VO, Praxishandbuch, Kap. 4 S. 202.

¹⁴⁵ Von Lewinski in BeckOK, DS-GVO, Art. 22 Rn. 23.

Obwohl die DS-GVO technologieneutral formuliert ist, enthalten vereinzelt Vorschriften eine gesetzgeberische Wertung mit Technologiebezug, um Weiterentwicklungen in diesem Bereich gerecht zu werden.¹⁴⁶ Insbesondere im Kontext von KI-Systemen gewinnt diese Vorschrift daher an Bedeutung, da diese oftmals auf eine weitgehende Automatisierung von Entscheidungsprozessen ausgerichtet sind.¹⁴⁷

I. Anwendungsbereich des Art. 22 DS-GVO

Zweck des Art. 22 DS-GVO ist es, den Einzelnen vor dem Hintergrund der stetigen technologischen Weiterentwicklung davor zu schützen, passives Objekt der Datenverarbeitung zu werden.¹⁴⁸ Dies ist besonders gefährlich, wenn Trainingsdaten bereits verzerrt sind und so Diskriminierungspotential beinhalten, das sich dann ungeprüft in der Entscheidung fortsetzt.¹⁴⁹

1. Tatbestandsmerkmale, Art. 22 Abs. 1 DS-GVO

a) Entscheidung

Um das aus Art. 22 DS-GVO hervorgehende Verbot auszulösen, ist zunächst erforderlich, dass gegenüber einer Person eine Entscheidung getroffen wird. Nicht umfasst sind daher bloße Unterstützungs- oder Vorbereitungshandlungen.¹⁵⁰

„Entscheidung“ ist weit zu verstehen und schließt auch Maßnahmen mit ein (ErwG 71 S. 1 DS-GVO). Entscheidungsgrundlage können dabei sowohl direkt vom Betroffenen erhobene Daten sein als auch Daten, die durch Profiling generiert wurden.¹⁵¹

b) Ausschließlich automatisiert

Diese Entscheidung muss ausschließlich auf einer automatisierten Verarbeitung beruhen. Verarbeitung bedeutet dabei jeder mit Hilfe automatisierter Verfahren ausgeführter Verarbeitungsvorgang personenbezogener Daten.¹⁵² Abzugrenzen ist dies von den einfach automatisierten Entscheidungen, die nur den allgemeinen Vorschriften der DS-GVO unterworfen sind.

Als ausschließlich automatisiert gelten Verarbeitungen, die ohne jegliches menschliche Eingreifen stattgefunden haben (ErwG 71 S. 1 DS-GVO). In diesem Merkmal zeigt sich der

¹⁴⁶ Kloos/Schmidt-Bens in Hartmann, KI & Recht kompakt, Kap. 5, S. 187.

¹⁴⁷ Krügel/Pfeifferbring in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 11 Rn. 38.

¹⁴⁸ Horváth in Spindler/Schuster/Kaesling, Recht der elektronischen Medien, DS-GVO, Art. 22 Rn. 1.

¹⁴⁹ Gausling, ZD 2019, 335, 339.

¹⁵⁰ Krügel/Pfeifferbring in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 11 Rn. 44.

¹⁵¹ Minihold in Ifsits/Minihold/Roubik, Haftungsfragen beim Einsatz von KI, Kap. V S. 127.

¹⁵² Kloos/Schmidt-Bens in Hartmann, KI & Recht kompakt, Kap. 5, S. 187.

Schutzzweck der Norm, da das Verbot gezielt auf Gefahren und Risiken zugeschnitten ist, die für den Einzelnen von nicht menschlich überprüften automatisierten Verarbeitungen ausgehen.¹⁵³

Zwar können auch einfache KI-Systeme selbstständig Entscheidungen treffen und Maßnahmen ergreifen, jedoch dienen diese vielmehr lediglich als Entscheidungsvorschläge oder Bewertungen.¹⁵⁴ Auf diese Entscheidungsvorschläge darf sich sodann ein menschlicher Entscheidungsträger stützen oder ihnen komplett folgen.¹⁵⁵ Entscheidend ist, dass er die KI-generierten Angaben überprüft und einer eigenen Entscheidung zuführt.¹⁵⁶ Diese menschliche Entscheidungsbefugnis führt dazu, dass natürliche Personen – im Unterschied zu ausschließlich automatisiert getroffenen Entscheidungen – nicht unmittelbar rechtlich oder ähnlich erheblich betroffen werden. Es handelt sich daher nur um teilautomatisierte Entscheidungen.

Zur Abgrenzung kommt es maßgeblich darauf an, ob der menschliche Entscheidungsträger in relevanter Weise Einfluss auf das Ergebnis der Entscheidung genommen hat.¹⁵⁷ Dafür ist einerseits maßgeblich, dass der Entscheidungsträger über ausreichend Kenntnisse zur Bewertung des Systems verfügt und fachliche Qualifikationen mitbringt.¹⁵⁸ Andernfalls ist ihm eine fachgerechte Überprüfung der Ausgabeentscheidung gar nicht möglich. Zum anderen muss er tatsächlich befugt sein, Änderungen im Entscheidungsprozess vornehmen zu können und diese Entscheidungsbefugnis auch bewusst ausüben.¹⁵⁹

Qualitativ erfordert die Einflussnahme zunächst, dass sie gezielt der Wahrung der schutzwürdigen Interessen der Betroffenen dient. Nicht ausreichend ist dagegen ein bloßes Dazwischentreten zwecks Überprüfung des Systems, etwa von Entwicklern oder Ingenieuren während der Trainingsphase.¹⁶⁰ Denn dies dient nur der immanenten Verbesserung des Systems, nicht dem Schutz der Interessen der Betroffenen.

Auch erfüllt eine rein symbolische oder bloß formale Absegnung (sog. rubber stamping)¹⁶¹, nicht die Anforderungen der Einflussnahme, da sie keinen signifikanten menschlichen Einfluss begründen kann.¹⁶² Würde dies genügen, könnte Art. 22 DS-GVO leicht umgangen und so sein

¹⁵³ *Martini* in Paal/Pauly, DS-GVO, Art. 22 Rn. 20.

¹⁵⁴ *Minihold* in Ifsits/Minihold/Roubik, Haftungsfragen beim Einsatz von KI, Kap. V S. 102 f.

¹⁵⁵ *Krügel/Pfeiffenbring* in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 11 Rn. 45.

¹⁵⁶ *Scholz* in Simitis/Hornung/Spiecker gen. Döhmman, DS-GVO, Art. 22 Rn. 31.

¹⁵⁷ *Bolek-Fügl* in Windholz, KI-VO, Praxishandbuch, Kap. 4 S. 203.

¹⁵⁸ *Scholz* in Simitis/Hornung/Spiecker gen. Döhmman, DS-GVO, Art. 22 Rn. 30.

¹⁵⁹ *Von Lewinski* in BeckOK, DS-GVO, Art. 22 Rn. 25.

¹⁶⁰ *Von Lewinski* in BeckOK, DS-GVO, Art. 22 Rn. 23.2.

¹⁶¹ *Vasel*, LTZ 2023, 179, 183.

¹⁶² *Minihold* in Ifsits/Minihold/Roubik, Haftungsfragen beim Einsatz von KI, Kap. V S. 127.

Anwendungsbereich eingeschränkt werden.¹⁶³ Notwendig ist vielmehr eine inhaltliche Auseinandersetzung mit der Entscheidung, die über eine bloße Zustimmung hinausgeht.¹⁶⁴

Allerdings besteht vor allem bei besonders komplexen und leistungsfähigen Systemen die Gefahr, dass der menschliche Entscheidungsträger trotz seiner eigentlich vorgesehenen Funktion auf das System vertraut und die KI-Ergebnisse ungeprüft übernimmt.¹⁶⁵ In einem solchen Fall würden die bestimmenden Motive und Faktoren für die Entscheidung weiterhin von dem KI-System vorgegeben werden.¹⁶⁶ Insbesondere wird es zukünftig mit zunehmender Verbesserung und Genauigkeit der KI-Verfahren immer unwahrscheinlicher, dass sich ein Sachbearbeiter trotz Entscheidungsbefugnis und Kompetenz über die Entscheidung der KI hinwegsetzen wird.¹⁶⁷ So würden die von KI-generierten Entscheidungen ausgehenden Risiken für den Betroffenen weiterbestehen. Art. 22 DS-GVO würde so seinen Zweck verfehlen.

c) **Rechtliche oder erhebliche Auswirkungen**

Letztlich muss das Ergebnis rechtliche oder jedenfalls erhebliche Auswirkungen haben.

Rechtliche Wirkung wird entfaltet, wenn die Entscheidung für den Betroffenen eine Rechtsfolge nach sich zieht.¹⁶⁸ Die Entscheidung muss die Rechtsposition des Betroffenen verändern, ein Recht oder Rechtsverhältnis begründen oder aufheben oder in ein Recht eingreifen.¹⁶⁹ Nicht hierunter fällt jedoch der Nichtabschluss eines Vertrages, da dies gerade nicht die Rechtsposition des Betroffenen berührt – dafür kann dies eine erhebliche Beeinträchtigung darstellen.¹⁷⁰

Eine erhebliche Beeinträchtigung liegt demgegenüber vor, wenn der Betroffene durch die Entscheidung nachhaltig in seiner wirtschaftlichen oder persönlichen Entfaltung gestört wird.¹⁷¹ Dies ist etwa der Fall bei der Ablehnung eines Online-Einstellungsverfahrens (ErwG 71 S. 1 DS-GVO), der Kündigung eines Kredites oder einer Erhöhung von Zinssätzen.¹⁷²

Gerade im Unternehmenskontext sind zahlreiche KI-Anwendungen geeignet, solche Auswirkungen zu entfalten. Etwa bei automatisierten Bewerberauswahl- oder

¹⁶³ Hoeren/Niehoff, RW 2018, 47, 53.

¹⁶⁴ Hoeren/Niehoff, RW 2018, 47, 53.

¹⁶⁵ Vasel, LTZ 2023, 179, 183.

¹⁶⁶ Scholz in Simitis/Hornung/Spiecker gen. Döhmman, DS-GVO, Art. 22 Rn. 29.

¹⁶⁷ Gausling, ZD 2019, 335, 339.

¹⁶⁸ Krügel/Pfeiffenbring in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 11 Rn. 52.

¹⁶⁹ Buchner in Kühling/Buchner, DS-GVO, Art. 22 Rn. 24a.

¹⁷⁰ Krügel/Pfeiffenbring in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 11 Rn. 52.

¹⁷¹ Scholz in Simitis/Hornung/Spiecker gen. Döhmman, DS-GVO, Art. 22 Rn. 38.

¹⁷² Buchner in Kühling/Buchner, DS-GVO, Art. 22 Rn. 26.

Kündigungsverfahren ist insofern besondere Vorsicht geboten und zwingend eine menschliche Entscheidungsebene zu implementieren.¹⁷³

2. Ausnahmen, Art. 22 Abs. 2, Abs. 3 DS-GVO

Sofern tatsächlich eine ausschließlich automatisierte Entscheidungsfindung vorliegt, ist diese grundsätzlich verboten. Damit automatisierte Entscheidungen jedoch nicht völlig verhindert werden, wurden vom Gesetzgeber drei Ausnahmetatbestände geschaffen. Nach Abs. 2 ist eine ausschließlich automatisierte Entscheidung möglich zum Abschluss oder der Erfüllung eines Vertrags (lit. a), auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten (lit. b) oder aufgrund ausdrücklicher Einwilligung (lit. c).

Diese Ausnahmen sind jedoch restriktiv auszulegen und mit zusätzlichen Schutzmaßnahmen, konkretisiert in Abs. 3, verbunden. Hierzu zählt insbesondere das Recht auf Erwirkung des Eingreifens einer natürlichen Person, auf Darlegung des eigenen Standpunkts sowie auf Anfechtung der Entscheidung. Dabei handelt es sich um Ergänzungen der allgemeinen Informationspflichten bzw. Betroffenenrechte der DS-GVO.¹⁷⁴ Vor allem können diese zusätzlichen Rechte nur ausgeübt werden, wenn der Verantwortliche seinen Informationspflichten allgemein nachgekommen ist.¹⁷⁵

II. Transparenz- und Informationspflichten bei automatisierten Entscheidungen

1. Informationspflichten nach Art. 13-15 DS-GVO

Mit der Regelung aus Art. 22 DS-GVO gehen daher die Informationspflichten und Auskunftsrechte aus Art. 13-15 DS-GVO einher.

Konkret begründen Art. 13 Abs. 2 lit. f DS-GVO bzw. Art. 14 Abs. 2 lit. g DS-GVO Informationspflichten für die Verantwortlichen, sobald Personen von ausschließlich automatisierten Entscheidungen betroffen werden. Dem Wortlaut nach muss die Erklärung zeitgleich mit der Datenerhebung erfolgen. Parallel steht dem Betroffenen ein Auskunftsrecht nach Art. 15 Abs. 1 lit. h DS-GVO zu.

Die Informationspflichten verfolgen den Zweck, den Betroffenen frühestmöglich ein effektives Vorgehen gegen die ausschließlich automatisierten Entscheidungen zu ermöglichen.¹⁷⁶ Es ist zu gewährleisten, dass der Verantwortliche eine faire und transparente Verarbeitung bei automati-

¹⁷³ Holthausen, RdA 2021, 19, 25.

¹⁷⁴ Minihold in Ifsits/Minihold/Roubik, Haftungsfragen beim Einsatz von KI, Kap. V S. 130.

¹⁷⁵ Krügel/Pfeiffenbring in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 11 Rn. 61.

¹⁷⁶ Hoeren/Niehoff, RW 2018, 47, 54.

sierten Entscheidungen einhalten muss (ErwG 71 DS-GVO).

2. Inhaltliche Reichweite – Blackbox-Problematik

Dabei ist fraglich, in welchem Umfang der Verantwortliche Informationen über die Entscheidungsfindung erteilen muss. Dies vor allem vor dem Hintergrund des Art. 12 DS-GVO, der normiert, dass die Informationserbringung in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie leichter Sprache erfolgen muss.

Problematisch ist, dass die Technologie von KI-Systemen automatisch ein Transparenzdefizit induziert und so die Ausübung von Informationspflichten hemmt – die Blackbox-Problematik.¹⁷⁷ Erschwert wird dies zusätzlich dadurch, dass die DS-GVO nicht nur größtenteils technologieneutral ist, sondern die Komplexität von KI-Systemen gänzlich nicht bedacht hat.¹⁷⁸ Sie ist daher im Lichte des technisch überhaupt Möglichen auszulegen.¹⁷⁹

Hinsichtlich der allgemeinen Intransparenz jeglicher automatisierten Entscheidung gesteht der Gesetzgeber den Verantwortlichen schon zu, dass nur „aussagekräftige Informationen über die involvierte Logik“ zu erteilen sind. Jedoch ist es insbesondere bei selbstlernenden Systemen häufig nicht möglich, zur Erfüllung der Transparenzpflichten überhaupt aussagekräftige Informationen über die involvierte Logik zu liefern.¹⁸⁰

a) Methodenbezogene Informationserbringung

Das Problem könnte einerseits über eine methodenbezogene Informationserbringung gelöst werden. Dazu müsste die Funktionsweise des KI-Systems offengelegt werden, indem der dem KI-System zugrundeliegende Quellcode bzw. der Algorithmus mit den Betroffenen geteilt wird.¹⁸¹

Das würde allerdings wirtschaftlichen Interessen des Verantwortlichen widersprechen, da sie gegebenenfalls Geschäftsgeheimnisse aufdecken müssten.¹⁸² Diese dürfen jedoch nicht beeinträchtigt werden (ErwG 63 S. 5 DS-GVO). Auch aus ErwG 63 S. 3 DS-GVO – wohl nicht aus der deutschen, jedoch aus der französischen und niederländischen Sprachfassung¹⁸³ – ergibt

¹⁷⁷ *Krügel/Pfeiffer* in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 11 Rn. 72.

¹⁷⁸ *Hoeren/Niehoff*, RW 2018, 47, 58.

¹⁷⁹ *Gausling*, ZD 2019, 335, 340.

¹⁸⁰ *Minihold* in Ifsits/Minihold/Roubik, Haftungsfragen beim Einsatz von KI, Kap. V S. 131.

¹⁸¹ Vgl. *Minihold* in Ifsits/Minihold/Roubik, Haftungsfragen beim Einsatz von KI, Kap. V S. 131.

¹⁸² *Schürmann*, ZD 2022, 316, 318.

¹⁸³ Französisch: „la logique qui sous-tend leur éventuel traitement automatisé“; niederländisch: „welke logica er ten grondslag ligt“.

sich, dass lediglich die Logik, die die Grundlage bildet, zu offenbaren ist.¹⁸⁴

Vor allem würde eine Offenlegung des Algorithmus des KI-Systems dem Zweck der Informationspflichten gar nicht gerecht werden, da der durchschnittliche Betroffene hieraus wohl keinen Erkenntnisgewinn ableiten können wird.¹⁸⁵

b) Subjektbezogene Informationserbringung

Vielmehr soll es daher zur Erfüllung der Informationspflicht hinsichtlich ausschließlich automatisierter Entscheidungsfindung ausreichend sein, wenn lediglich das Prinzip, nicht jedoch die Algorithmus-Formel dargelegt wird.¹⁸⁶ Es soll zumindest die abstrakte Funktionsweise und Ausrichtung des KI-Systems so verständlich wie möglich dargestellt werden, um den Betroffenen die Überprüfung und ein grundlegendes Verständnis der Entscheidungsfindung zu ermöglichen.¹⁸⁷

Für Unternehmen folgt daraus die Pflicht, bereits bei der Auswahl und Implementierung von KI-Systemen darauf zu achten, dass ein Mindestmaß an Erklärbarkeit gewährleistet ist.

III. Verhältnis zu anderen Vorschriften

1. Datenschutz-Grundverordnung

Neben den Informations- und Auskunftspflichten der Art. 13-15 DS-GVO ist Art. 22 DS-GVO im Verhältnis zur DS-GVO vor allem eng mit der Rechtmäßigkeit der Verarbeitung aus Art. 5, 6 DS-GVO verknüpft.¹⁸⁸

Eine weitere Anforderung im Zusammenhang mit Art. 22 DS-GVO ist die Durchführung einer Datenschutzfolgenabschätzung nach Art. 35 Abs. 1 DS-GVO. Denn der Einsatz von KI-Systemen im Rahmen ausschließlich automatisierter Entscheidungen unterfällt regelmäßig Art. 35 Abs. 3 lit. a DS-GVO, der Art. 35 Abs. 1 DS-GVO durch Regelbeispiele konkretisiert. Dadurch soll sich der Verantwortliche in besonders sensiblen Bereichen über die möglichen Folgen der Datenverarbeitung bewusst werden.¹⁸⁹

Die Datenschutz-Folgenabschätzung bildet zugleich eine wichtige Schnittschnelle zwischen Datenschutzrecht und Corporate Governance, da sie Unternehmen dazu zwingt, den Einsatz

¹⁸⁴ Hoeren/Niehoff, RW 2018, 47, 54.

¹⁸⁵ Paal, ZfDR 2024, 129, 146.

¹⁸⁶ Hoeren/Niehoff, RW 2018, 47, 60.

¹⁸⁷ Golland, EuZW 2024, 846, 851; Hoeren/Niehoff, RW 2018, 47, 58-60; Paal, ZfDR 2024, 129, 146.

¹⁸⁸ Horváth in Spindler/Schuster/Kaesling, Recht der elektronischen Medien, DS-GVO, Art. 22 Rn. 4.

¹⁸⁹ Scholz in Simitis/Hornung/Spiecker gen. Döhmman, DS-GVO, Art. 22 Rn. 75.

von KI-Systemen zu reflektieren und Kontroll- und Risikosysteme zu etablieren.

2. Verordnung über künstliche Intelligenz

Bis zum Erlass der KI-VO war Art. 22 DS-GVO die zentrale Leitnorm für vollautomatisierte Entscheidungen von KI-Systemen.¹⁹⁰ Die Vorschriften, die in Wechselwirkung mit Art. 22 DS-GVO stehen, verdrängen diese jedoch nicht, sondern treten hinzu, da die KI-VO die DS-GVO ausdrücklich unberührt lassen soll (Art. 2 Abs. 7 KI-VO, ErwG 10 S. 4 KI-VO).

Große Überschneidungen hat die Norm insbesondere mit Art. 14 KI-VO. Beide Normen haben zum Zweck, die Entscheidungsprozesse von KI-Systemen zu überwachen, um die Betroffenen vor deren Ergebnissen zu schützen.¹⁹¹ Art. 14 KI-VO normiert hier das Gebot, Hochrisiko-Systeme unter menschliche Aufsicht zu stellen, wie auch die Schutzmaßnahmen des Art. 22 Abs. 3 DS-GVO ein menschliches Eingreifen sicherstellen. Während Art. 14 KI-VO hier jedoch mehr eine systemische Vorsorgepflicht fordert, knüpft Art. 22 DS-GVO an den individuellen Einzelfall an.

Ähnlich ist auch Art. 5 KI-VO, der bestimmte KI-Anwendungen aufgrund ihres inakzeptablen Risikos für die Rechte und Freiheiten natürlicher Personen verbietet. So verbietet auch Art. 22 DS-GVO grundsätzlich ausschließlich automatische Entscheidungen, wenn diese sich in rechtlich relevanter oder ähnlich erheblicher Weise auf die betroffenen Personen auswirken. Dies korrespondiert vor allem mit den Social-Scoring-Systemen, die natürliche Personen benachteiligen (Art. 5 Abs. 1 UAbs. 1 lit. c KI-VO), oder den biometrischen Fernidentifizierungssysteme (Art. 5 Abs. 1 UAbs. 1 lit. h KI-VO).¹⁹²

IV. Automatisierte Entscheidungsfindung als Governance-Herausforderung

Art. 22 DS-GVO markiert eine zentrale datenschutzrechtliche Grenze für den Einsatz von KI-Systemen in der Praxis von Unternehmen. Die Norm zielt nicht nur auf den Schutz einzelner Betroffener ab, sondern zwingt zeitgleich Unternehmen dazu, ihre Entscheidungsprozesse so auszugestalten, dass ein effektives menschliches Eingreifen möglich bleibt. Die Norm entfaltet insofern strukturelle Steuerungswirkung.

So verlagert sich der Fokus von der bloßen Einhaltung datenschutzrechtlicher Vorgaben hin zu der gesamtstrukturellen Organisation unternehmensinterner Prozesse. Insbesondere das Verbot rein formaler menschlicher Beteiligung macht deutlich, dass vollautomatisierte

¹⁹⁰ Martini in Paal/Pauly, DS-GVO, Art. 22 Rn. 7c.

¹⁹¹ Bomhard/Wietzke in Bomhard/Pieper/Wende, KI-VO, Art. 14 Rn. 2.

¹⁹² Martini in Paal/Pauly, DS-GVO, Art. 22 Rn. 7f.

Entscheidungsprozesse klar dokumentierte Kontrollmechanismen und qualifizierte Entscheidungsträger erfordern.

Die Norm fungiert daher als Schnittstelle zwischen Datenschutzrecht und Corporate Governance. Die datenschutzrechtlichen Vorgaben können nur eingehalten werden, wenn sie in ein funktionierendes Governance-System eingebettet werden. Vor diesem Hintergrund sind insbesondere die Pflichten der Leitungsorgane, die für Organisation, Überwachung und Steuerung des KI-Einsatzes verantwortlich sind, zu beachten.

E. Organpflichten beim Einsatz von KI-Systemen in der Corporate Governance

Der Einsatz von KI-Systemen gewinnt in der Unternehmenspraxis zunehmend an Bedeutung. KI wird insbesondere zur Prognose und Analyse der finanziellen Unternehmensentwicklung,¹⁹³ zur Untersuchung von Wertschöpfungsprozessen sowie zur Identifikation von Optimierungs- und Einsparpotenzialen eingesetzt.¹⁹⁴ Auch bei Due-Diligence-Prüfungen im Rahmen von M&A-Transaktionen kommen KI-Systeme vermehrt zum Einsatz.¹⁹⁵ Ziel ist regelmäßig eine Verbesserung der Entscheidungsgüte durch eine datenbasierte Analyse komplexer Sachverhalte.¹⁹⁶

Diese Entwicklung wirft die Frage auf, welche Anforderungen sich hieraus für die Pflichten der Leitungsorgane ergeben. Denn das wichtigste Entscheidungszentrum einer Ebene befindet sich auf Leitungsebene.¹⁹⁷ Nach gesellschaftsrechtlichen Grundsätzen tragen die Mitglieder der Leitungsorgane die Gesamtverantwortung für die Geschäftsführung.¹⁹⁸ Obwohl zunehmend Entscheidungen faktisch durch algorithmische Systeme vorbereitet oder gar getroffen werden, verbleibt die rechtliche Verantwortung hierfür uneingeschränkt bei den Organen.¹⁹⁹

Da mit der Größe des Unternehmens regelmäßig auch das Ausmaß der Gefahrenquelle steigt, werden größere Unternehmen zumeist als Kapitalgesellschaften, vor allem als Aktiengesellschaft (AG) betrieben.²⁰⁰ Die Organpflichten werden daher im Folgenden exemplarisch anhand der Leitungsorgane einer Aktiengesellschaft – dem Vorstand – dargestellt.

¹⁹³ Fraunhofer IAIS, Big Data – Vorsprung durch Wissen, Innovationsanalyse, 2012, S. 31 ff.

¹⁹⁴ Fraunhofer Gesellschaft, Maschinelles Lernen, Eine Analyse zu Kompetenzen, Forschung und Anwendung, 2018, S. 25 ff.; *Weber/Kiefner/Jobst*, NZG 2018, 1131.

¹⁹⁵ *Weber/Kiefner/Jobst*, NZG 2018, 1131.

¹⁹⁶ *Plagemann*, NZG 2025, 684, 685.

¹⁹⁷ *Möslein* in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 13 Rn. 17.

¹⁹⁸ *Fleischer* in BeckOGK, AktG, § 77 Rn. 51.

¹⁹⁹ Vgl. *Möslein*, ZIP 2018, 204, 208.

²⁰⁰ *Dieckmann* in Chibanguza/Kuß/Steega, KI-Hdb., 2. Teil: § 5 I. Rn. 4; *Möslein* in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 13 Rn. 9.

Der maßgebliche rechtliche Rahmen wird dabei insbesondere durch die §§ 76 Abs. 1, 77 Abs. 1 S. 1, 93 Abs. 1 und Abs. 2 AktG geprägt.

I. Organpflichten der Leitungsorgane in Bezug auf Künstliche Intelligenz

1. Sorgfaltspflicht im engeren Sinne

a) Maßstab der Sorgfaltspflicht

Die Sorgfaltspflicht der Leitungsorgane ergibt sich für den Vorstand einer Aktiengesellschaft aus § 93 Abs. 1 S. 1 AktG. Danach haben Leitungsorgane bei der Führung der Geschäfte des Unternehmens die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Hierzu zählt auch die Pflicht zur ordnungsgemäßen Organisation der Gesellschaft.²⁰¹

Dem Leitungsorgan steht dabei ein weiter Handlungsspielraum zu, ohne den eine unternehmerische Tätigkeit kaum möglich wäre.²⁰² Dieses Geschäftsleiterermessen umfasst sowohl das bewusste Eingehen wirtschaftlicher Risiken als auch die Inkaufnahme von Fehlbeurteilungen und Fehleinschätzungen.²⁰³ Ausdruck dieses Grundsatzes ist die Business Judgement Rule des § 93 Abs. 1 S. 2 AktG, die Vorstandsmitglieder einer AG vor persönlicher Haftung schützt, sofern sie ihre Entscheidung auf einer angemessenen Informationsgrundlage treffen und zum Wohl der Gesellschaft handeln.

b) Übertragung auf den Einsatz von KI-Systemen

aa) ISION-Grundsätze und Plausibilitätskontrolle

Die Entscheidung über den Einsatz von KI-Systemen im Unternehmen ist als Geschäftsführungsmaßnahme der Verantwortung und dem unternehmerischen Ermessensspielraum des Vorstandes zuzuordnen.²⁰⁴ Der Vorstand kann daher grundsätzlich entscheiden, ob und inwieweit KI-Anwendungen im operativen Geschäft eines Unternehmens oder unterstützend bei Vorbereitung und Ausführung von Leitungsentscheidungen eingesetzt werden.²⁰⁵

Allerdings darf sich ein Leitungsorgan nicht unkritisch auf externe Expertise verlassen. Um seiner Sorgfaltspflicht nachzukommen, muss nach den ISION-Grundsätzen ein fachkundiger

²⁰¹ Ritter, ZAT 2025, 11, 13.

²⁰² BGH v. 10.02.2022 – 3 StR 329/21, NZG 2022, 1293.

²⁰³ BGH v. 10.02.2022 – 3 StR 329/21, NZG 2022, 1293.

²⁰⁴ Lücke, BB 2019, 1986, 1989-1991.

²⁰⁵ Plagemann, NZG 2025, 684, 689.

und unabhängiger Berater gewählt, dieser mit umfassenden Informationen versorgt und die Ergebnisse abschließend einer eigenen Plausibilitätskontrolle unterzogen werden.²⁰⁶ Diese Grundsätze sind auf den Einsatz von KI-Systemen übertragbar.

Auch beim Einsatz von KI ist sicherzustellen, dass das System für den vorgesehenen Zweck geeignet und fachlich qualifiziert ist, auf einer hinreichenden Informationsbasis operiert und zudem eine unabhängige Analyse gewährleistet wird.²⁰⁷ Eine unabhängige Analyse ist vor allem gefährdet, wenn die Informationsverarbeitung und Entscheidungsfindung vom Vorstand beeinflusst wird durch positives oder negatives Feedback.²⁰⁸

Abschließend ist eine Plausibilitätsprüfung durchzuführen, um untaugliche Entscheidungen auszuschließen.²⁰⁹ Dabei sind die Anforderungen an die Überprüfung am Kenntnisstand des Vorstandes zu messen; ein vollständiges technisches Verständnis des Systems ist nicht erforderlich.²¹⁰ Es ist ausreichend, wenn der Vorstand überprüft, ob alle erforderlichen Informationen zur Verfügung standen, keine erkennbaren Auslassungen vorlagen und die Entscheidung in sich schlüssig ist.²¹¹

Gleichwohl sorgt der Blackbox-Charakter von KI-Systemen dafür, dass es dem Vorstand dennoch verschlossen bleibt, wie das KI-System sein Ergebnis begründet und ob es alle Informationen in die Entscheidung einbezogen hat oder die Entscheidung gar auf Widersprüchen beruht.²¹² Vor diesem Hintergrund darf KI nicht zur alleinigen Entscheidungsgrundlage werden. Vielmehr sind die dadurch gewonnen Informationen stets mit weiteren Erkenntnisquellen und eigenem Erfahrungswissen abzugleichen.²¹³

bb) Grundsatz der Datenqualität

Besondere Bedeutung kommt der Qualität der dem KI-System zugrunde liegenden Daten zu. Hierbei sind hohe Anforderungen einzuhalten. Werden KI-Systeme im Rahmen der Entscheidungsvorbereitung oder -findung eingesetzt, verlagert sich der Schwerpunkt der Sorgfaltspflicht auf die Verlässlichkeit der zugrundeliegenden Entscheidungsgrundlagen. Um den Schutz der Business Judgement Rule in Anspruch nehmen zu können, müssen

²⁰⁶ BGH v. 20. 09. 2011 – II ZR 234/09, NZG 2011, 1271.

²⁰⁷ Dilling/Musiol, CCZ 2024, 257, 264; Ritter, ZAT 2025, 11, 13.

²⁰⁸ Weber/Kiefner/Jobst, NZG 2018, 1131, 1133.

²⁰⁹ Müller/Masson in Chibanguza/Kuß/Steega, KI-Hdb., 2. Teil: § 5 J. Rn. 17.

²¹⁰ BGH v. 28.04.2015 – II ZR 63/14, NZG 2015, 792 Rn. 35; Weber/Kiefner/Jobst, NZG 2018, 1131, 1133.

²¹¹ Müller/Masson in Chibanguza/Kuß/Steega, KI-Hdb., 2. Teil: § 5 J. Rn. 17.

²¹² Weber/Kiefner/Jobst, NZG 2018, 1131, 1133.

²¹³ Plagemann, NZG 2025, 684, 690.

Leitungsorgane sicherstellen, dass die dem KI-System zugeführten Informationen zuverlässig, plausibel und für den jeweiligen Entscheidungszweck geeignet sind.²¹⁴

Diese gesellschaftsrechtliche Sorgfaltspflicht korrespondiert mit den Anforderungen der KI-VO, insbesondere Art. 26 Abs. 4 KI-VO. Dieser normiert qualitative Anforderungen an die Eingabedaten, vor allem das Erfordernis der Repräsentation. Fehlerhafte, verzerrte oder nicht repräsentative Daten können zu systematisch fehlerhaften Prognosen und Entscheidungen führen und damit die Entscheidungsgrundlage entwerten.²¹⁵

Vor diesem Hintergrund stellt sich die Sicherstellung der Datenqualität als zentraler Bestandteil pflichtgemäßen Handelns dar. Leitungsorgane müssen besonders gewährleisten, dass die eingesetzten KI-Systeme mit Daten trainiert und betrieben werden, die diesen Anforderungen genügen.²¹⁶ Dies können sie durch eine geeignete und qualifizierte Aufsicht erreichen, die wiederum in der KI-VO – in Art. 14 Abs. 4 lit. a-e KI-VO – konkretisiert und gesetzlich normiert ist.

2. Überwachungspflicht

Die Sorgfaltspflicht wird durch eine eigenständige organschaftliche Überwachungspflicht ergänzt, die insbesondere bei der Delegation von Aufgaben Bedeutung erlangt.

a) Vertikale und horizontale Überwachungspflichten

Eine Überwachungspflicht besteht zum einen in vertikaler Hinsicht bezüglich der nachgeordneten Mitarbeiter als auch in horizontaler Hinsicht bezüglich der anderen Mitglieder des jeweiligen Leitungsorgans.

Die vertikale Überwachungspflicht verpflichtet die Leitungsorgane, die Tätigkeit nachgeordneter Mitarbeiter so zu überwachen, dass unter normalen Umständen mit einer ordnungsgemäßen Geschäftsführung gerechnet werden kann.²¹⁷ Sobald sich Anhaltspunkte für ein Fehlverhalten ergeben, muss das Leitungsorgan sofort eingreifen können.²¹⁸ Insofern haftet der Vorstand dabei nicht für fremdes, sondern für eigenes Verschulden wegen unzureichender Organisation, Anleitung oder Kontrolle, das Fehlhandlungen ermöglicht oder erleichtert.²¹⁹

²¹⁴ *Weber/Kiefner/Jobst*, NZG 2018, 1131, 1132.

²¹⁵ *Kumkar* in Hilgendorf/Roth-Isigkeit, KI-VO, § 6 Rn. 3.

²¹⁶ *Weber/Kiefner/Jobst*, NZG 2018, 1131, 1133.

²¹⁷ *Ritter*, GuP 2025, 53, 56.

²¹⁸ *Fleischer* in BeckOGK, AktG, § 93 Rn. 141.

²¹⁹ *Ritter*, ZAT 2025, 11, 13.

Demgegenüber entsteht aus dem Grundsatz der Gesamtverantwortung der einzelnen Vorstände die horizontale Überwachungspflicht.²²⁰ Sie verlangt von den Geschäftsleitern, die Geschäftsgänge über ihre jeweiligen Ressortgrenzen hinweg fortwährend zu beobachten.²²¹ Die Überwachung beschränkt sich hierbei regelmäßig auf eine Plausibilitätsprüfung der Handlungen der anderen Ressortverantwortlichen.²²²

b) Überwachung des KI-Einsatzes

Auch der Einsatz von KI-Systemen stellt funktional eine Delegation dar und löst entsprechende Überwachungspflichten aus.²²³ Diese können daher auch parallel zu den Überwachungspflichten bei Delegation an natürliche Personen ausgestaltet werden.

Leitungsorgane müssen zunächst prüfen, ob sich das jeweilige System zur Vorbereitung von Geschäftsführungs- bzw. Leitungsaufgaben sowie zur Erfüllung des Unternehmenszwecks eignet oder zunächst an die individuellen Verhältnisse des Unternehmens angepasst werden muss.²²⁴ Zudem ist der laufende Einsatz des KI-Systems weiter zu überwachen. Dabei sind bestimmte organisatorische Maßnahmen zu treffen, mit denen die Arbeitsweise des KI-Systems stetig evaluiert und überwacht werden kann, um falsche Entscheidungen und anderen Risiken vorzubeugen.²²⁵

Um diese Pflichten erfüllen zu können, müssen Leitungsorgane die Wirkweise und Erkenntnisgewinnung des KI-Systems zumindest im Ansatz verstehen können (sog. Algorithmusbeherrschung).²²⁶ Andernfalls wird ihnen eine effektive Wahrnehmung der Letztentscheidungs- und Kontrollverantwortung kaum möglich sein.²²⁷

3. Legalitätspflicht

Die Legalitätspflicht verpflichtet die Leitungsorgane, sich bei ihrer Amtsführung gesetzestreu zu verhalten.²²⁸ Das umfasst sowohl eine interne Pflichtenbindung, konkretisiert durch Gesetz, Gesellschaftsvertrag und Geschäftsordnung, als auch eine externe Pflichtenbindung bezüglich

²²⁰ *Lüneborg* in Hölters/Weber, AktG, § 93 Rn. 84.

²²¹ *Fleischer*, NZG 2024, 1639, 1644.

²²² *Ritter*, GuP 2025, 53, 56.

²²³ *Spindler* in MüKo/AktG, § 93 Rn. 134.

²²⁴ *Müller/Masson* in Chibanguza/Kuß/Steega, KI-Hdb., 2. Teil: § 5 J. Rn. 8; *Weber/Kiefner/Jobst*, NZG 2018, 1131, 1132.

²²⁵ *Dieckmann* in Chibanguza/Kuß/Steega, KI-Hdb., 2. Teil: § 5 I. Rn. 23; *Plagemann*, NZG 2025, 684, 690.

²²⁶ *Müller/Masson* in Chibanguza/Kuß/Steega, KI-Hdb., 2. Teil: § 5 J. Rn. 8; *Möslein*, ZIP 2018, 204, 208.

²²⁷ *Möslein* in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 13 Rn. 28.

²²⁸ *Koch*, AktG, § 93 Rn. 9.

sonstiger Rechtsnormen, insbesondere das Datenschutzrecht.²²⁹

Der Einsatz von KI-Systemen ist daher nur zulässig, soweit keine arbeitsrechtlichen oder datenschutzrechtlichen Normen verletzt werden.²³⁰ Besondere Bedeutung kommt hierbei dem Verbot ausschließlich automatisierter Entscheidungen aus Art. 22 DS-GVO zu. Daher sind entsprechende organisatorische Vorkehrungen zu treffen, um derartige Risiken zu beherrschen. Ein Verstoß gegen die Legalitätspflicht kann bereits dann vorliegen, wenn allein die Datenbasis fehlerhaft ist und so rechtswidrige Ergebnisse erzeugt werden.²³¹ Die Verantwortung hierfür verbleibt bei den Leitungsorganen. Es sollten klare Zuständigkeiten für den KI-Einsatz, definierte Entscheidungsprozesse, interne Richtlinien sowie Mechanismen zur laufenden Überwachung der Systeme geschaffen werden.²³²

4. Legalitätskontrollpflicht

Aus der Legalitätspflicht folgt weiterhin die Verpflichtung der Leitungsorgane, ebenso auf den unteren Unternehmensebenen sicherzustellen, dass nicht gegen gesetzliche Vorschriften verstoßen wird (Compliance-Pflicht).²³³ Die Leitungsorgane müssen organisatorische Vorkehrungen treffen, um die Begehung von Rechtsverstößen durch die Gesellschaft bzw. die Mitarbeiter zu verhindern – dies erfordert die Einrichtung eines Compliance-Management-Systems.²³⁴

Im Kontext des KI-Einsatzes begehen die Leitungsorgane vor allem dann eine Pflichtverletzung, wenn sie es versäumt haben, die notwendigen Maßnahmen hinsichtlich der Einhaltung der KI-VO oder der einschlägigen Normen der DS-GVO zu treffen.²³⁵ Daher müssen sich die Leitungsorgane frühzeitig mit den regulatorischen Anforderungen auseinandersetzen und klare interne Strukturen schaffen, damit deren Einhaltung sichergestellt werden kann.²³⁶ Zudem müssen die Leitungsorgane auch sofort eingreifen, sobald sich Anhaltspunkte für ein Fehlverhalten zeigen.²³⁷

Insofern greift die Legalitätskontrolle eng mit der allgemeinen Überwachungspflicht ineinander.

²²⁹ *Fleischer*, NZG 2024, 1639, 1643.

²³⁰ *Spindler* in MüKo/AktG, § 93 Rn. 131; *Ritter*, ZAT 2025, 11.

²³¹ *Weber/Kiefner/Jobst*, NZG 2018, 1131, 1135.

²³² *Plagemann*, NZG 2025, 684, 692.

²³³ *Grigoleit/Tomasic* in Grigoleit, AktG, § 93 Rn. 26.

²³⁴ OLG Nürnberg v. 30.03.2022 – 12 U 1520/19 NZG 2022, 1058.

²³⁵ *Ritter*, GuP 2025, 53, 56.

²³⁶ *Ritter*, GuP 2025, 53, 56.

²³⁷ *Fleischer* in BeckOGK, AktG, § 93 Rn. 141; *Ritter*, ZAT 2025, 11, 13.

II. Delegation an Künstliche Intelligenz

Der Einsatz von KI-Systemen wirft nicht nur die Frage nach der Verantwortung der Leitungsorgane auf, sondern auch danach, in welchem Umfang Aufgaben der Geschäftsführung oder Unternehmensleitung auf KI delegiert werden können oder gar müssen.

1. Möglichkeit der Delegation und dessen Grenzen

a) Allgemeine Grundsätze der Delegation

Nach § 77 Abs. 1 AktG führt der Vorstand die Geschäfte der Gesellschaft in Eigenverantwortung. Allerdings ist es in einer arbeitsteiligen Wirtschaft praktisch kaum möglich, dass der Vorstand alle Aufgaben selbst bewältigen kann.²³⁸ Vielmehr ist anerkannt, dass verschiedene Aufgaben nicht nur horizontal innerhalb des Vorstandes sondern auch vertikal an nachgeordnete Mitarbeiter delegiert werden können.²³⁹ Besondere Bedeutung erlangt hierbei die Auswahlpflicht der Unternehmensleitung. Die Leitungsorgane müssen dabei sicherstellen, dass die Delegationsempfänger fachlich qualifiziert sind.²⁴⁰

Dabei ist in Geschäftsführungsaufgaben und Leitungsaufgaben zu unterscheiden. Geschäftsführungsaufgaben umfassen dabei jede tatsächliche oder rechtsgeschäftliche Tätigkeit der Gesellschaft und können auf andere übertragen werden.²⁴¹ Demgegenüber sind Leitungsaufgaben solche, die das Gesetz ausdrücklich den Leitungsorganen zuweist oder zu den originären Leitungsaufgaben zählen.²⁴² Hierzu zählen grundlegende unternehmerische Entscheidungen, Zielkonzeption, Führungsgrundsätze sowie Organisation und Geschäftspolitik des Unternehmens.²⁴³ Auch die Entscheidung über den Einsatz von KI-Systemen im Unternehmen selbst ist eine Leitungsentscheidung.²⁴⁴

b) Übertragung der Grundsätze auf KI-Systeme

Überträgt man diese Grundsätze auf den Einsatz von KI-Systemen, so ist KI funktional nicht anders zu behandeln als eine natürliche Person, die mit der Informationsbeschaffung bzw. -aufbereitung betraut wird.²⁴⁵ Grundsätzlich können daher KI-Systeme zur Vorbereitung unternehmerischer Entscheidungen eingesetzt werden, etwa zur Analyse großer Datenmengen,

²³⁸ *Möslein* in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 13 Rn. 24; *Plagemann*, NZG 2025, 684, 688.

²³⁹ *Weber/Kiefner/Jobst*, NZG 2018, 1131, 1132.

²⁴⁰ BGH v. 28.04.2015 – II ZR 63/14, NZG 2015, 792 Rn. 28.

²⁴¹ *Koch*, AktG, § 76 Rn. 10.

²⁴² *Möslein* in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 13 Rn. 25.

²⁴³ *Weber* in Hölters/Weber, AktG, § 76 Rn. 8.

²⁴⁴ *Weber/Kiefner/Jobst*, NZG 2018, 1131, 1132.

²⁴⁵ *Möslein*, ZIP 2018, 204, 208; *Weber/Kiefner/Jobst*, NZG 2018, 1131, 1132.

zur Prognose wirtschaftlicher Entwicklungen oder Simulation verschiedener Handlungsoptionen.²⁴⁶ Voraussetzung ist ein ständiger Informationsfluss, eine Einflussmöglichkeit auf die KI sowie die jederzeitige Eingriffsmöglichkeit.²⁴⁷

Dagegen spricht auch nicht der Blackbox-Charakter von KI-Systemen, da probabilistische Einschätzungen ohnehin integrativer Bestandteil von unternehmerischen Entscheidungen sind.²⁴⁸

c) **Grenzen der Delegation: Grundsatz der umfassenden Leitungsverantwortung**

Während die Geschäftsführungsaufgaben grundsätzlich delegierbar sind, ist das bei Leitungsaufgaben bis auf wenige Ausnahmen nicht der Fall (Grundsatz der umfassenden Leitungsverantwortung).²⁴⁹ Allerdings besteht dennoch die Möglichkeit, vorbereitende oder ausführende Tätigkeiten im Zusammenhang mit den Leitungsaufgaben zu delegieren, sofern die Letztentscheidung beim Leitungsorgan verbleibt und dieses in eigener Verantwortung entscheidet.²⁵⁰

Um die Letztentscheidungskompetenz zu wahren, müssen die Leitungsorgane „Herren des Verfahrens“²⁵¹ bleiben und jederzeit korrigierend eingreifen können.²⁵² Hier wirkt sich wiederum die Blackbox-Problematik aus. Denn die Letztentscheidungskompetenz kann nur pflichtgemäß ausgeübt werden, wenn der Vorstand zumindest grundsätzlich nachvollziehen kann, wie algorithmisch gebildete Entscheidungen getroffen werden.²⁵³ In diese Richtung geht auch der Art. 22 DS-GVO, der ein Verbot maßgeblich von einer Letztentscheidungsverantwortlichkeit einer natürlichen Person abhängig macht.

Der Vorstand muss daher zu einer vollständig selbst getroffenen Entscheidung kommen.²⁵⁴ Dabei darf die Entscheidungsbefugnis nicht auf das KI-System übergehen, sondern diese lediglich als Hilfsmittel herangezogen werden.

²⁴⁶ *Plagemann*, NZG 2025, 684 ff.

²⁴⁷ *Calabro*, S. 104 ff.

²⁴⁸ *Langheld/Haagen*, NZG 2023, 1535, 1537.

²⁴⁹ *Möslein* in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 13 Rn. 25; *Weber* in Hölters/Weber, AktG, § 76 Rn. 8.

²⁵⁰ *Calabro*, S. 89 f.; *Möslein*, ZIP 2018, 204, 208.

²⁵¹ *Möslein*, ZIP 2018, 204, 208.

²⁵² *Plagemann*, NZG 2025, 684, 692.

²⁵³ *Spindler* in MüKo/AktG, § 76 Rn. 29.

²⁵⁴ *Calabro*, S. 90.

Vor dem Hintergrund dieser Grenze sind insbesondere Kontrollpflichten zu betonen. Dabei sind die Ergebnisse des KI-Systems gezielt zu hinterfragen und zu überprüfen, um der Letztverantwortung gerecht zu werden.²⁵⁵

Diese Wertentscheidung findet sich auch im Gesetz wieder, sofern eine menschliche Entscheidung oder Überprüfung verlangt wird. So verdeutlicht im Datenschutzrecht auch Art. 22 DS-GVO, dass ausschließlich automatisierte Entscheidungen mit rechtlichen oder erheblichen Auswirkungen nur unter engen Voraussetzungen zulässig sind. Aber auch im Rahmen der KI-VO werden hohe Anforderungen an menschliche Aufsicht gestellt, sofern es sich um eine Hochrisiko-KI handelt.

Problematisch wird die Wahrung der Letztentscheidungsverantwortung vor allem bei hochautonomen KI-Modellen, die selbst Entscheidungen treffen. Dabei könnte jedoch argumentiert werden, dass die Letztentscheidung hier schon vorher durch die Programmierung der festgelegten Grenzen stattfindet.²⁵⁶ Allerdings widerspricht das schon dem Wortlaut, wonach eine „Letzt“-entscheidung kaum vorher getroffen werden kann. Insbesondere ist es charakteristisch für intelligente Modelle, dass sie sich über die festgelegten programmierten Grenzen hinwegsetzen, wodurch eine Letztentscheidung durch Programmierung ohnehin schwer getroffen werden kann.²⁵⁷

2. Pflicht zur Delegation?

Aus der Business Judgement Rule (§ 93 Abs. 1 S. 2 AktG) könnte sich sogar eine Pflicht zum Einsatz von KI-Systemen ergeben, um eine angemessene Informationsgrundlage zu schaffen. Dazu müssten KI-Systeme unter die angemessenen Informationsquellen fallen.

Einer rechtlichen Verpflichtung wird allerdings entgegenzuhalten sein, dass auch die Einschätzung, welche Informationsquellen heranzuziehen und wie diese zu gewichten sind, selbst Teil der unternehmerischen Entscheidungsfreiheit im Einzelfall ist.²⁵⁸ Es müssen daher nicht alle verfügbaren Informationsquellen herangezogen werden, sondern vielmehr Kosten und Nutzen der Informationsbeschaffung gegeneinander abgewogen werden.²⁵⁹

Jedoch könnte sich das unternehmerische Ermessen auch auf Null reduzieren und so mindestens

²⁵⁵ *Plagemann*, NZG 2025, 684, 692.

²⁵⁶ *Weber/Kiefner/Jobst*, NZG 2018, 1131, 1134.

²⁵⁷ *Weber/Kiefner/Jobst*, NZG 2018, 1131, 1134.

²⁵⁸ Vgl. *Lüneborg* in *Hölters/Weber*, AktG, § 93 Rn. 32.

²⁵⁹ *Möslein* in *Ebers/Heinze/Krügel/Steinrötter*, KI und Robotik, § 13 Rn. 32.

eine faktische Pflicht zur Nutzung von KI-Systemen begründen.²⁶⁰ Das beruht auf der Überlegung, dass algorithmische Entscheidungen menschlichen Entscheidungen in vielen Bereichen, vor allem bei Prognoseentscheidungen oder der Verarbeitung großer Datenmengen, überlegen sind.²⁶¹ Je größer der Informationsvorsprung ist, den ein KI-System bieten kann, und je gravierender die wirtschaftlichen Entscheidungen sind, desto eher kann ein Verzicht auf den Einsatz von KI-Systemen pflichtwidrig sein.²⁶²

Das wird allerdings nur sehr ausnahmsweise angenommen werden können. Dafür muss es für die konkrete Anwendung bereits erprobte KI-Modelle auf dem Markt geben und die jeweilige Aufgabenstellung dies auch konkret erfordern.²⁶³ Eine Pflicht würde auch dem haftungserleichternden Zweck der Business Judgement Rule entgegenlaufen. Das ergibt auch ein Vergleich mit dem Heranziehen von Expertengutachten, wozu auch keine Pflicht besteht.²⁶⁴ Daher wird wohl eher nur eine Pflicht zum Erwägen eines KI-Einsatzes angenommen werden können.²⁶⁵

3. Rechtsfolgen der Delegation

Die Delegation von Aufgaben an KI-Systeme entbindet die Leitungsorgane nicht von ihren Pflichten, sondern verändert diese lediglich inhaltlich.²⁶⁶ Zunächst muss für die konkrete Entscheidung ein KI-System ausgewählt werden, das – ähnlich der Delegation an natürliche Personen – fachlich qualifiziert ist.²⁶⁷ Dabei kommt es vor allem auf die Datenqualität an.

Auch werden auch die bereits beschriebenen Überwachungs- und Überprüfungspflichten nach den ISION-Grundsätzen ausgelöst. Zusätzlich werden den Leitungsorganen Dokumentationspflichten auferlegt, um zu beweisen, dass sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben.²⁶⁸ Dokumentationspflichten sind daher elementar, da sie das Haftungsregime determinieren.²⁶⁹

Dies auch im Zusammenspiel mit den gesetzlichen Vorschriften: Die Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO verpflichtet den Verantwortlichen, die Einhaltung der

²⁶⁰ Calabro, S. 177 f.; Dieckmann in Chibanguza/Kuß/Steega, KI-Hdb., 2. Teil: § 5 I. Rn. 35; Möslin, ZIP 2018, 204, 209.

²⁶¹ Dieckmann in Chibanguza/Kuß/Steega, KI-Hdb., 2. Teil: § 5 I. Rn. 35.

²⁶² Möslin in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 13 Rn. 31.

²⁶³ Calabro, S. 177 f.; Lücke, BB 2019, 1986, 1989.

²⁶⁴ Langheld/Haagen, NZG 2023, 1535, 1537 f.

²⁶⁵ Möslin, ZIP 2018, 204, 209.

²⁶⁶ Langheld/Haagen, NZG 2023, 1535, 1538.

²⁶⁷ Calabro, S. 120 f.

²⁶⁸ Möslin, ZIP 2018, 204, 212; Weber/Kiefner/Jobst, NZG 2018, 1131, 1136.

²⁶⁹ Möslin in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 13 Rn. 38.

datenschutzrechtlichen Grundsätze nachweisen zu können. Dies erfordert eine entsprechende Dokumentation.²⁷⁰ Auch die KI-VO sieht eigene Dokumentations- und Nachweispflichten – etwa in Art. 6 Abs. 3 S. 1 KI-VO oder Art. 11 KI-VO – vor, die sich mit den gesellschaftsrechtlichen Pflichten überschneiden.

III. Bedeutung der Organpflichten für die Corporate Governance

Für die Corporate Governance erlangt vordergründig die Legalitätspflicht besondere Bedeutung, nach der der Vorstand gem. § 76 Abs. 1 AktG auf die Gesetzeskonformität des unternehmerischen Handelns einzustehen hat.²⁷¹ Diese begrenzt den Einsatz von KI-Systemen insbesondere durch datenschutzrechtliche, arbeitsrechtliche sowie diskriminierungsrechtliche Vorgaben. Zugleich verpflichtet die Legalitätskontrollpflicht die Leitungsorgane dazu, organisatorische Maßnahmen zu ergreifen, um Rechtsverstöße innerhalb der Organisation zu verhindern.

Darüber hinaus begründen auch die allgemeinen Überwachungs- und Sorgfaltspflichten sowie die Verpflichtung zur Risikovorsorge aus §§ 91, 93 AktG die Notwendigkeit einer strukturierten Governance.²⁷² Die Sorgfaltspflicht verlangt eine sorgfältige Ermittlung der Entscheidungsgrundlagen, was sich beim KI-Einsatz insbesondere in Anforderungen an Datenqualität, Systemauswahl und Plausibilitätskontrolle niederschlägt. Die Überwachungspflicht greift, sobald Aufgaben an KI-Systeme delegiert werden, und erfordert eine laufende Kontrolle der Systemleistung sowie ein Mindestmaß an Verständnis der Funktionsweise („Algorithmusbeherrschung“).

Maßgeblich ist jedoch auch § 91 Abs. 2 AktG, der die Pflicht normiert, technikimmanenten Risiken zu begegnen.²⁷³ Diese verpflichtet den Vorstand, geeignete Maßnahmen zur frühzeitigen Erkennung bestandsgefährdender Entwicklungen zu treffen. Gerade der Einsatz komplexer KI-Systeme kann solche Risiken begründen, da fehlende Erklärbarkeit, intransparente Entscheidungslogik oder Verzerrungen in Trainingsdaten erhebliche wirtschaftliche oder rechtliche Folgen nach sich ziehen können. Die Einrichtung einer KI-Governance als zentrales Steuerungselement wird daher auch aus gesellschaftsrechtlicher Perspektive erforderlich.²⁷⁴

²⁷⁰ Pötters in Gola/Heckmann, DS-GVO, Art. 5 Rn. 34.

²⁷¹ Dendorfer-Ditges in MAH ArbR, Teil P., § 75 Rn. 11.

²⁷² Conrad/Streitz in Auer-Reinsdorff/Conrad, Hdb. IT- und DatenschutzR, § 33 Rn. 39; Dendorfer-Ditges in MAH ArbR, Teil P., § 75 Rn. 18.

²⁷³ Möselein in Ebers/Heinze/Krügel/Steinrötter, KI und Robotik, § 13 Rn. 28; Sassenberg, RD 2025, 347.

²⁷⁴ Reese, BB 2024, 1515, 1516.

F. Modell einer KI-Governance in Unternehmen

I. Notwendigkeit eines Governance-Modells beim Einsatz von KI-Systemen

Der Einsatz von KI-Systemen in Unternehmen ist nicht lediglich eine technologische Frage, sondern gibt Anlass zur Entwicklung eines eigenständigen Governance-Modells. Denn KI-Systeme fungieren nicht nur als neutrale Werkzeuge zur Effizienzsteigerung oder Datenanalyse, sondern verändern Entscheidungsprozesse, Verantwortungszuordnungen und Risikostrukturen innerhalb der Unternehmensorganisation grundlegend. Damit wird der Einsatz zu einer organisationsrelevanten Gefahrenquelle, die eine gezielte Steuerung und Kontrolle durch die Leitungsorgane erfordert.

1. Aus unternehmerischer Perspektive

Bereits die vorangegangenen Kapitel haben gezeigt, dass KI-Systeme zunehmend in die Kernbereiche unternehmerischer Entscheidungsfindung vordringen. Ihre Anwendungsfelder beschränken sich nicht auf rein operative Prozesse, sondern berühren regelmäßig strategische, mitunter existenzielle Entscheidungen des Unternehmens.

Damit fällt ihr Einsatz typischerweise in den Verantwortungsbereich und Pflichtenkreis der Leitungsorgane. Vor allem aus der Legalitäts- und Legalitätskontrollpflicht sowie den allgemeinen Überwachungs- und Sorgfaltspflichten ergibt sich die Notwendigkeit zur Einrichtung einer KI-Governance. Sie ist daher auch aus gesellschaftsrechtlicher Perspektive notwendig.

Vor diesem Hintergrund lässt sich der Einsatz von KI nicht isoliert durch punktuelle Compliance-Maßnahmen beherrschen, sondern muss als eigenständiger Teil in einen übergreifenden Ordnungsrahmen eingebettet und mit den Pflichten der Leitungsorgane verzahnt werden.²⁷⁵

2. Aus regulatorischer Perspektive

Eine solche Einbettung erfolgt typischerweise im Rahmen einer unternehmensinternen Governance-Struktur, bei der neben sowohl unternehmensspezifischen Risiken auch regulatorische Anforderungen berücksichtigt werden müssen.²⁷⁶ So hat die Analyse der DSGVO und der KI-VO gezeigt, dass beide Verordnungen eigenständige, aber komplementäre Governance-Anforderungen an den Einsatz von KI formulieren.

²⁷⁵ Hoeren/Pinelli, KIR 2026, 5, 8.

²⁷⁶ Sassenberg, RD 2025, 347.

Die DS-GVO adressiert vor allem den Schutz personenbezogener Daten und statuiert mit Instrumenten wie der Datenschutz-Folgenabschätzung, dem Verbot vollautomatisierter Entscheidungen und der Rechenschaftspflicht prozedurale und organisatorische Anforderungen. Die KI-VO verfolgt demgegenüber einen risikobasierten Ansatz, der systembezogene Pflichten wie Datenqualitätsanforderungen, menschliche Aufsicht, Dokumentations- und Überwachungspflichten normiert.

Beide Regelungsregime verlangen damit in unterschiedlicher Weise eine strukturelle Verankerung von Verantwortlichkeiten, Prozessen und Kontrollmechanismen innerhalb der Unternehmensorganisation. Genau hierin auch liegt die Schnittmenge mit den gesellschaftsrechtlichen Organisationspflichten der Leitungsorgane.

Dabei fungiert KI-Governance als integratives Steuerungselement, das die normativen Anforderungen beider Verordnungen mit den gesellschaftsrechtlichen Pflichten zur ordnungsgemäßen Unternehmensorganisation verbindet. Es erfüllt dabei eine doppelte Funktion: zum einen dient es der Operationalisierung rechtlicher Pflichten, indem es rechtliche Vorgaben umsetzt, und wirkt zum anderen als Risikosteuerungselement, das es den Leitungsorganen ermöglicht, den KI-Einsatz vorausschauend, kontrolliert und haftungsadäquat zu gestalten.

II. Datenschutzrechtliche Governance-Anforderungen nach der DS-GVO

Der Einsatz von KI-Systemen in Unternehmen ist in der Praxis regelmäßig mit der Verarbeitung personenbezogener Daten verbunden, sodass die DS-GVO einen zentralen normativen Referenzrahmen für die Ausgestaltung der KI-Governance bildet.

Ihre Bedeutung erschöpft sich dabei nicht in der Einhaltung einzelner materieller Datenschutzvorschriften. Vielmehr etabliert die DS-GVO abstrakte Grundsätze wie Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung und Richtigkeit, deren Einhaltung eine organisatorische Implementierung erfordert. Unternehmen werden dazu verpflichtet, Datenschutzrisiken zu identifizieren, zu bewerten und zu kontrollieren. Damit konkretisiert die DS-GVO zugleich die gesellschaftsrechtlichen Organisationspflichten der Leitungsorgane, insbesondere im Hinblick auf die Pflicht zur Einrichtung eines wirksamen Compliance- und Risikomanagementsystems.

1. Daten als Ausgangspunkt

Ausgangspunkt jeder datenschutzrechtlichen Governance ist die Frage, ob und in welchem Umfang personenbezogene Daten überhaupt verarbeitet werden. Ein vollständiger Ausschluss

der Anwendbarkeit der DS-GVO kann nur erreicht werden, wenn keine personenbezogenen Daten verwendet werden, etwa durch den Einsatz anonymisierter oder synthetischer Daten.²⁷⁷

Anonymisierte Daten unterfallen nicht dem Anwendungsbereich der Verordnung, sofern der Personenbezug dauerhaft und irreversibel – nach dem jeweils aktuellen Stand der Technik – ausgeschlossen ist (ErwG 26 S. 5 DS-GVO).²⁷⁸ Dies erfordert jedoch eine fortlaufende Überprüfung, da sich die Möglichkeiten der Re-Identifizierung mit dem technischen Fortschritt verändern können.²⁷⁹ Auch synthetische Daten, die reale Datensätze statistisch nachbilden, ohne auf konkrete Personen rückführbar zu sein, können eine datenschutzfreie Alternative darstellen.²⁸⁰

In der Unternehmenspraxis wird ein vollständiger Verzicht auf personenbezogene Daten jedoch regelmäßig nicht realisierbar sein. KI-Systeme sind typischerweise auf große und qualitativ hochwertige Datensätze angewiesen, sodass ein Spannungsverhältnis zwischen Datenminimierung und Systemleistung entsteht. Vor diesem Hintergrund gewinnt die Pseudonymisierung besondere Bedeutung (ErwG 26 S. 2 DS-GVO).²⁸¹ Durch eine funktionale Trennung von Daten und Zuordnungsinformationen kann das Risiko für betroffene Personen reduziert werden, ohne die Nutzbarkeit der Daten für KI-Anwendungen vollständig einzuschränken.²⁸²

Für die Governance bedeutet dies, dass bereits auf Datenebene strategische Grundentscheidungen zu treffen sind, die sowohl datenschutzrechtliche Anforderungen als auch funktionale Erfordernisse des KI-Einsatzes berücksichtigen. Diese Entscheidungen fallen in den Verantwortungsbereich der Leitungsorgane und sind Ausdruck ihrer Pflicht zur risikoadäquaten Organisation der Datenverarbeitung.

2. Grundprinzipien der Datenverarbeitung

a) Grundsätze nach Art. 5 Abs. 1 DS-GVO

Die in Art. 5 Abs. 1 DS-GVO normierten Grundsätze der Datenverarbeitung bilden den materiellen Kern des Datenschutzrechts und zugleich die Grundlage organisatorischer Steuerungsanforderungen. Sie definieren einerseits die materiellen Anforderungen an die

²⁷⁷ DSK, Positionspapier zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen v. 6.11.2019, S. 9, https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf, abgerufen am 23.04.2026.

²⁷⁸ Roßnagel/Geminn ZD 2021, 487, 489; Schäfer, ZD 2025, 12, 15.

²⁷⁹ Arning/Rothkegel in Taeger/Gabel, DSGVO Art. 4 Rn. 48.

²⁸⁰ Lukas, ZD 2023, 321, 322; Schäfer, ZD 2025, 12, 15.

²⁸¹ Klar/Kühling in Kühling/Buchner, DS-GVO, Art. 4 Nr. 5 Rn. 13

²⁸² Schleipfer, ZD 2020, 284, 285.

Datenverarbeitung und begründen zum anderen organisatorische Pflichten, die durch geeignete interne Prozesse umgesetzt werden müssen.

Gerade im Kontext des Einsatzes von KI-Systemen gewinnen diese Grundsätze eine ausgeprägte Governance-Dimension und erfordern, dass sie bereits in der Entwicklungs- und Beschaffungsphase bedacht werden durch geeignete organisatorische und technische Maßnahmen.

Besondere Bedeutung erlangt hierbei der Grundsatz der Rechtmäßigkeit als auch der Grundsatz der Datenminimierung. Datenverarbeitungen sind so zu konzipieren, dass nur diejenigen Daten erhoben und verarbeitet werden, die für den jeweiligen Zweck erforderlich sind, sodass auch die Eingriffsintensität für die betroffenen Personen möglichst gering gehalten wird. Dies wirkt sich auch positiv auf die im Rahmen des Art. 6 Abs. 1 lit. f. DS-GVO vorzunehmende Interessenabwägung aus, indem die datensparsame Verwendung zugunsten der verantwortlichen Unternehmen zu berücksichtigen ist.

Eng hiermit verbunden ist der Grundsatz der Zweckbestimmung. Dieser erfordert eine präzise Festlegung der Verarbeitungszwecke sowie eine klare Abgrenzung von Primär- und Sekundärnutzung.²⁸³ Gerade hinsichtlich KI ist diese Differenzierung zentral, da Trainings- und Anwendungsprozesse häufig eigenständige Zweckdimensionen aufweisen und gesondert zu bewerten sind. Eine unscharfe Zweckdefinition führt nicht nur zu datenschutzrechtlichen Risiken, sondern auch zu einer erschwerten Kontrolle im Nachhinein.

Schließlich erfordert auch der Grundsatz der Datenrichtigkeit die Implementierung ex post wirkender Sicherheitsmechanismen. So können nachträgliche Kontrollinstanzen eingerichtet werden. Aber auch im Vorfeld hilft eine strukturierte Data-Governance, die Qualität und Repräsentativität der Daten sicherstellt. Andernfalls besteht die Gefahr, dass sich diskriminierende Ergebnisse fortsetzen.

Die Umsetzung aller Grundsätze ist nur durch eine enge Verzahnung von technischen, organisatorischen und rechtlichen Funktionen innerhalb des Unternehmens auf allen Ebenen möglich.

b) Rechenschafts- und Dokumentationspflichten nach Art. 5 Abs. 2 DS-GVO

Die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO verstärkt die organisatorische Dimension der Datenschutzerfordernungen erheblich. Unternehmen müssen nicht nur rechtmäßig handeln,

²⁸³ Schäfer, ZD 2025, 12, 16; Paal, ZfDR 2024, 129, 143 f.

sondern ihre Entscheidungen und Prozesse auch nachvollziehbar dokumentieren.

Zu den wichtigsten Instrumenten der datenschutzrechtlichen Rechenschaftspflicht gehört insbesondere das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO.²⁸⁴ Aber auch interne Richtlinien dienen der Erfüllung der Dokumentationspflichten der DS-GVO. Im Kontext von KI-Systemen gewinnen diese Instrumente zusätzliche Bedeutung, da komplexe und mehrstufige Datenverarbeitungen andernfalls kaum rekonstruierbar wären.

Gleichzeitig eröffnet sich hier eine wesentliche Schnittstelle zur KI-VO: Die dort vorgesehenen Dokumentations- und Nachweispflichten – vor allem im Zusammenhang mit Hochrisiko-KI-Systemen – lassen sich funktional mit den datenschutzrechtlichen Dokumentationsanforderungen verbinden. Für die Governance ergibt sich daraus die Notwendigkeit, integrierte Dokumentationssysteme zu schaffen, die sowohl datenschutzrechtliche als auch KI-spezifische Anforderungen abdecken und so Doppelstrukturen vermeiden.

3. Transparenz und Blackbox-Problematik als Governance-Herausforderung

Ein zentrales Spannungsfeld zwischen KI-Systemen und der DS-GVO liegt in den Transparenzanforderungen der Art. 12 bis 14 DS-GVO. Betroffene Personen haben Anspruch auf verständliche Informationen über die Verarbeitung ihrer Daten sowie – im Falle automatisierter Entscheidungen – über die zugrunde liegende Logik.

Gerade hier kollidiert das Datenschutzrecht mit der technischen Realität komplexer KI-Modelle, deren Entscheidungsprozesse aufgrund der Blackbox-Problematik nur eingeschränkt nachvollziehbar sind. Die daraus resultierende Spannung kann nicht allein technisch aufgelöst werden, sondern erfordert eine bewusste organisatorische Steuerung.

Unternehmen müssen definieren, in welcher Form und Tiefe Informationen gegenüber welchen Adressaten bereitgestellt werden können und welche ergänzenden Maßnahmen erforderlich sind, um Transparenzdefizite zu kompensieren. Dies kann etwa durch standardisierte Erläuterungskonzepte, abgestufte Informationsmodelle oder zentrale Veröffentlichungen erfolgen.²⁸⁵ Transparenz wird damit zu einer organisatorischen Aufgabe.

Für die Leitungsorgane folgt daraus, dass sie im Rahmen ihrer Legalitäts- und Überwachungspflichten sicherstellen müssen, dass die eingesetzten KI-Systeme zumindest ein

²⁸⁴ Martini in Paal/Pauly, DS-GVO, Art. 30 Rn. 2b.

²⁸⁵ Vgl. Schäfer, ZD 2025, 12, 17.

Mindestmaß an erklärbarer Funktionsweise aufweisen oder durch flankierende Maßnahmen kompensiert werden. Andernfalls drohen nicht nur datenschutzrechtliche Verstöße, sondern auch ein Verlust effektiver Kontrolle über unternehmensinterne Entscheidungsprozesse.

4. Sicherung menschlicher Entscheidungsverantwortung

Besondere Bedeutung kommt im Kontext der KI Governance dem Verbot ausschließlich automatisierter Entscheidungen nach Art. 22 DS-GVO zu. Danach dürfen Entscheidungen, die rechtliche Wirkung entfalten oder betroffene Personen erheblich beeinträchtigen, grundsätzlich nicht ohne menschliche Beteiligung erfolgen.

Diese Vorgabe ist nicht nur als Individualschutzrecht zu verstehen, sondern besitzt zugleich eine organisationsrechtliche Dimension. Unternehmen sind verpflichtet, Entscheidungsprozesse so auszugestalten, dass eine tatsächliche menschliche Einflussnahme gewährleistet ist. Dies betrifft sowohl die strukturelle Einbindung menschlicher Entscheidungsträger als auch deren faktische Befähigung, KI-gestützte Ergebnisse zu überprüfen und gegebenenfalls zu korrigieren.

Damit korrespondiert Art. 22 DS-GVO unmittelbar mit den gesellschaftsrechtlichen Anforderungen an die Leitungsorgane, die die Letztverantwortung für unternehmerische Entscheidungen tragen. KI-Systeme dürfen diese Verantwortung nicht substituieren, sondern allenfalls unterstützen.

Für die Governance bedeutet dies, dass Entscheidungsprozesse so gestaltet werden müssen, dass menschliche Kontrolle nicht zur bloßen Formalität wird. Vielmehr sind klare Zuständigkeiten, effektive Eingriffsmöglichkeiten und ein hinreichendes Verständnis der eingesetzten Systeme sicherzustellen.

5. Datenschutz-Folgeabschätzung als zentrales Governance-Instrument

Eine Schlüsselrolle innerhalb der datenschutzrechtlichen Governance nimmt die Datenschutz-Folgeabschätzung nach Art. 35 DS-GVO ein. Sie ist durchzuführen, wenn eine Form der Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat – eine Konstellation, die häufig beim Einsatz von KI-Systemen vorliegt.²⁸⁶

Die Datenschutz-Folgeabschätzung stellt dabei kein bloßes Prüfungsinstrument dar, sondern

²⁸⁶ Mackert/Ernst in Wieland/Steinmeyer/Grüniger, HdB Compliance-Management, Teil I. Kap. 1.4 Rn. 35; Rappenglück/Vonthien, RD 398, 403.

fungiert als strukturierendes Governance-Element. Sie zwingt Unternehmen, Risiken frühzeitig zu identifizieren, ihre Ursachen zu analysieren und geeignete Abhilfemaßnahmen zu definieren. Zugleich dokumentiert sie den Entscheidungsprozess und macht ihn gegenüber Aufsichtsbehörden nachvollziehbar.

In dieser Funktion ähnelt die Datenschutz-Folgenabschätzung klassischen Instrumenten des Risikomanagements und knüpft unmittelbar an die gesellschaftsrechtliche Pflicht zur ordnungsgemäßen Unternehmensorganisation an. Gleichzeitig bestehen erhebliche Überschneidungen zur Risikobewertung nach der KI-VO, insbesondere im Hinblick auf die Einstufung und Regulierung von Hochrisiko-KI-Systemen.

Für eine effektive KI-Governance bietet es sich daher an, die Datenschutz-Folgenabschätzung mit den risikobasierten Bewertungsmechanismen der KI-VO in einem integrierten Prozess zusammenzuführen. Auf diese Weise lassen sich Doppelprüfungen vermeiden und eine konsistente Risikosteuerung wird gewährleistet.

III. KI-spezifische Governance-Anforderungen nach der KI-VO

Mit der KI-VO hat der europäische Gesetzgeber erstmals einen eigenständigen, systembezogenen Regulierungsrahmen für künstliche Intelligenz geschaffen. In der Governance-Perspektive entfaltet die KI-VO aufgrund ihres risikobezogenen Regelungsansatzes eine eigenständige, aber komplementäre Steuerungswirkung.

Die KI-VO wirkt als normativer Ordnungsrahmen, der in bestehende Governance-Strukturen eingreift und Unternehmen dazu zwingt, den Einsatz von KI-Systemen systematisch zu erfassen, zu klassifizieren, organisatorisch zu kontrollieren und fortlaufend zu überwachen. Sie konkretisiert damit die gesellschaftsrechtlichen Organisations- und Überwachungspflichten in Bezug auf KI-spezifische Risiken und erweitert diese um systembezogene Anforderungen. Gerade hierin liegt die zentrale Bedeutung für eine KI-Governance.

1. Strukturierte Einordnungsentscheidungen

Am Beginn jeder KI-Governance steht nicht nur eine technische, sondern eine rechtlich strukturierte Einordnungsentscheidung. Für die konkrete Ausgestaltung der Governance ist maßgeblich, welche Rolle das Unternehmen im Lebenszyklus des KI-Systems einnimmt und welchem Risikoregime das System unterliegt.²⁸⁷

²⁸⁷ Eger/Schmuck in Wieland/Steinmeyer/Grüninger, HdB Compliance-Management, Teil I. Kap. 4.1 Rn. 10 f.

Zunächst ist zu bestimmen, ob das Unternehmen als Anbieter oder als Betreiber eines KI-Systems agiert. Diese Differenzierung ist von zentraler Bedeutung, da die KI-VO unterschiedliche Pflichtenkreise an diese Rollen knüpft.

Darauf aufbauend ist eine Risikoklassifizierung vorzunehmen. Unternehmen müssen einen belastbaren Prozess schaffen, mit dem beurteilt werden kann, ob ein System unter Art. 5 KI-VO fällt, als Hochrisiko-KI nach Art. 6 KI-VO einzuordnen ist oder nur den allgemeinen Anforderungen – etwa Art. 4 oder Art. 50 KI-VO – unterliegt.²⁸⁸ Je höher das regulatorisch angenommene Risiko, desto intensiver sind die Anforderungen an Auswahl, Kontrolle und Überwachung durch die Leitungsorgane. Dies korrespondiert mit dem gesellschaftsrechtlichen Grundsatz, dass sich der Umfang der Sorgfalts- und Überwachungspflichten am Gefahrenpotential der jeweiligen Geschäftstätigkeit orientiert.

In der Praxis empfiehlt sich die Einrichtung eines unternehmensweiten „AI System Inventory“, in dem sämtliche eingesetzten KI-Systeme erfasst, klassifiziert und dokumentiert werden.²⁸⁹ So können typische Risiken identifiziert und entsprechend bewertet werden. Diese Bestandsaufnahme bildet die Grundlage für sämtliche weitere Governance-Maßnahmen und muss fortlaufend aktualisiert werden, insbesondere bei Änderungen des Systemzwecks, der Datenbasis oder des Einsatzkontextes.²⁹⁰

Für die Governance folgt daraus, dass Einordnungsentscheidungen nicht nur einmalig getroffen, sondern dauerhaft überprüft, dokumentiert und organisatorisch verankert werden müssen. Die Leitungsorgane erfüllen ihre Pflicht zur gesetzeskonformen Organisation nur dann, wenn entsprechende Verfahren zur Identifikation und Klassifizierung von KI-Systemen eingerichtet sind.

2. Vermittlung von KI-Kompetenz als strukturelle Voraussetzung

Eine effektive KI-Governance setzt voraus, dass die handelnden Personen über die erforderliche KI-Kompetenz verfügen. Art. 4 KI-VO verpflichtet Unternehmen, ein angemessenes Maß an Kenntnissen, Fähigkeiten und Verständnis im Umgang mit KI-Systemen sicherzustellen.

Diese Pflicht besitzt eine grundlegende Governance-Funktion und ist insofern zentrale Herausforderung für Unternehmen.²⁹¹ Ohne ein hinreichendes Verständnis der Funktionsweise,

²⁸⁸ Sassenberg, RDi 2025, 346, 347 f.

²⁸⁹ Mackert/Ernst in Wieland/Steinmeyer/Grüninger, HdB Compliance-Management, Teil I. Kap. 1.4 Rn. 31.

²⁹⁰ Hoeren/Pinelli, KIR 2026, 5, 6.

²⁹¹ APP AI Governance Profession Report 2025, S. 11,

https://assets.contentstack.io/v3/assets/bltd4dd5b2d705252bc/blt9bd00190c2eba136/ai_governance_profession_report_2025.pdf, abgerufen am 23.04.2026.

Risiken und regulatorischen Anforderungen von KI-Systemen können weder operative Entscheidungen noch Leitungs- und Überwachungsaufgaben sachgerecht wahrgenommen werden.

Unternehmen müssen zunächst den bestehenden Kenntnisstand ermitteln und darauf aufbauend differenzierte Schulungskonzepte entwickeln.²⁹² Dabei ist darauf zu achten, die Mitarbeitenden mit den jeweiligen Regelwerken nicht zu überfordern.²⁹³ Hierzu bietet es sich an, zwischen verschiedenen Adressatengruppen zu differenzieren. Während für alle Mitarbeitenden ein grundlegendes Verständnis erforderlich ist, bedürfen Entscheidungsträger, Entwickler und Compliance-Verantwortliche vertiefte Kenntnisse.²⁹⁴

3. Menschliche Aufsicht als zentrales Steuerungselement

Ein zentrales, verbindendes Merkmal zwischen KI-VO, DS-GVO und Gesellschaftsrecht ist das Gebot eines menschlichen Entscheidungselements. Für Hochrisiko-KI-Systeme verlangt die KI-VO ausdrücklich, dass diese unter wirksamer menschlicher Aufsicht stehen.

Hinsichtlich der Governance konkretisiert dieses Erfordernis die gesellschaftsrechtliche Pflicht der Leitungsorgane, die Kontrolle über unternehmerische Entscheidungsprozesse zu behalten. Menschliche Aufsicht darf sich nicht auf eine bloß formale Kontrolle beschränken, sondern muss tatsächlich geeignet sein, Einfluss auf das Systemverhalten zu nehmen.

Dies setzt vor allem voraus, dass klare Zuständigkeiten definiert werden, Eingriffsbefugnisse festgelegt sind und effektive Kontrollmechanismen implementiert werden. Menschliche Aufsicht funktioniert nur, wenn die beaufsichtigenden Personen das System verstehen, Abweichungen erkennen, Ergebnisse plausibilisieren und notfalls intervenieren können.²⁹⁵ Daraus folgt für die Governance die Notwendigkeit klarer Aufsichtsstrukturen, etwa in Form definierter Verantwortlicher, Vier-Augen-Prinzipien, Eskalationswege und dokumentierter Interventionsbefugnisse²⁹⁶ oder Notfallabschaltungen, wie ein „Kill Switch“.²⁹⁷

Hier zeigt sich auch die Parallele zu Art. 22 DS-GVO. Während dieser die menschliche Letztentscheidung zum Schutz der betroffenen Person fordert, zielt die KI-VO auf die strukturelle Kontrolle risikobehafteter Systeme ab. Ziel ist es, Risiken frühzeitig zu erkennen,

²⁹² Schippel, KIR 2025, 119 ff.; Fleck KIR 2024, 99, 100.

²⁹³ Sassenberg, RD i 2025, 346, 348.

²⁹⁴ Rappenglück/Vonthien, RD i 398, 402; Schippel KIR 2025, 119, 121.

²⁹⁵ Hafez in Windholz, KI-VO, Praxishandbuch, Kap. 10 S. 462.

²⁹⁶ Denga in BeckOK KI-Recht, KI-VO, Art. 26 Rn. 26; Hoeren/Pinelli, KIR 2026, 5, 8.

²⁹⁷ Spittka in BeckOK, KI-Recht, KI-VO Art. 20 Rn. 10.

Fehlfunktionen zu korrigieren und automatisierte Prozesse notfalls zu unterbrechen.

4. Dokumentations- und Nachweispflichten

Die KI-VO statuiert umfangreiche Dokumentations- und Nachweispflichten. Diese dienen nicht nur der externen Kontrolle, sondern haben eine ausgeprägte Governance-Funktion. Dokumentation macht Entscheidungsprozesse nachvollziehbar, schafft interne Transparenz und ermöglicht eine ex-post-Kontrolle auch intern durch Leitungs- und Aufsichtsorgane.²⁹⁸

Technische Dokumentation, Audit Trails und nachvollziehbare Entscheidungs- und Freigabevermerke machen den Entwicklungs- und Einsatzprozess überprüfbar und knüpfen damit an die Entscheidungsdokumentation im Sinne der Business Judgement Rule an.²⁹⁹ Die Unternehmensleitung kann ihre Leitungs- und Überwachungsentscheidungen nur dann belastbar rechtfertigen, wenn wesentliche Risikoannahmen, Freigaben, Kontrollmaßnahmen und verbleibende Restrisiken nachvollziehbar dokumentiert sind.

IV. Integriertes KI-Governance Modell für Unternehmen

1. Verzahnung der Anforderungen nach DS-GVO und KI-VO

Die vorangegangenen Kapitel haben gezeigt, dass der Einsatz von KI-Systemen in Unternehmen weder isoliert technikrechtlich noch datenschutzrechtlich zu erfassen ist. Vielmehr überlagern sich gesellschaftsrechtliche Organpflichten, datenschutzrechtliche Schutzmechanismen und die systembezogenen Anforderungen der KI-VO. Für die Unternehmenspraxis ergibt sich daraus ein komplexer, kumulativer Pflichtenkreis, der ohne eine strukturierte Governance nicht konsistent beherrscht werden kann.

In diesem Gefüge übernimmt KI-Governance die Funktion eines integrierenden Ordnungs- und Steuerungsmodells. Sie dient dazu, die normativen Vorgaben der DS-GVO und der KI-VO in die bestehenden Corporate-Governance-Strukturen einzubetten und zugleich die Verantwortung der Leitungsorgane operationalisierbar zu machen.

Dabei muss eine KI-Governance vor allem folgende Schnittstellen auflösen: die Konzipierung von Verarbeitungsprozessen, die sowohl den Datenschutz-Grundsätzen genügen als auch den Anbieterpflichten hinsichtlich Data-Governance der KI-VO; die Einführung menschlicher Aufsicht, die sowohl an Art. 14 KI-VO als auch Art. 22 DS-GVO ausgerichtet ist; die Verbindung von KI-Risikoklassifizierung und Datenschutz-Folgenabschätzung; die

²⁹⁸ Hafez in Windholz, KI-VO, Praxishandbuch, Kap. 10 S. 459; Hoeren/Pinelli, KIR 2026, 5, 6.

²⁹⁹ Hoeren/Pinelli, KIR 2026, 5, 6.

Abstimmung von Transparenzanforderungen sowie die Zusammenführung von Dokumentations- und Nachweispflichten. Ziel ist nicht die Schaffung paralleler Regelungsregime, sondern die funktionale Verzahnung bestehender Pflichten.

2. Ausgangspunkt: Gesamtverantwortung der Leitungsorgane

Zentraler Anknüpfungspunkt des KI-Governance-Modells ist die gesellschaftsrechtliche Gesamtverantwortung der Leitungsorgane. Unabhängig vom Grad der Automatisierung verbleibt die rechtliche Verantwortung stets bei den natürlichen Personen auf Leitungsebene.

Diese Verantwortung konkretisiert sich im KI-Kontext insbesondere in vier Dimensionen, die bereits herausgearbeitet wurden: die sorgfältige Ermittlung und Bewertung der Entscheidungsgrundlagen, der Wahrung der Letztentscheidungskompetenz, der Einrichtung wirksamer Organisations- und Kontrollstrukturen sowie der fortlaufenden Überwachung risikobehafteter Systeme. Die Anforderungen aus der DS-GVO und der KI-VO konkretisieren diese Pflichten jeweils aus unterschiedlicher Perspektive und machen sie operativ greifbar.

Die KI-Governance setzt genau hier an, indem sie die abstrakten Organpflichten in organisatorische Strukturen übersetzt durch rollenbasierte Zuständigkeiten, standardisierte Prozesse und dokumentierte Entscheidungsabläufe.

3. KI-Governance Modell

a) Ebene 1: Strategische Steuerung und Leitentscheidungen

Auf oberster Ebene verortet das KI-Governance-Modell die strategische Steuerung des KI-Einsatzes. Die Entscheidung über den Einsatz von KI-Systemen ist – wie gezeigt – eine originäre Leitungsaufgabe, da sie die Geschäftsausrichtung, das Risikoprofil und die Wettbewerbsfähigkeit des Unternehmens betrifft.

Hierzu gehört insbesondere die Festlegung der zulässigen Einsatzbereiche von KI. In der Praxis bietet sich die Einführung eines unternehmensinternen Freigabesystems an, etwa in Form einer Positivliste zugelassener Anwendungen.³⁰⁰ Damit wird auch dem Problem begegnet, dass Arbeitnehmer unautorisiert selbst KI verwenden (sog. Shadow AI), das insbesondere durch frei zugängliche KI-Tools im Internet erheblich an Bedeutung gewonnen hat.³⁰¹

Auf dieser Ebene sind zudem grundlegende Weichenstellungen vorzunehmen, insbesondere die initiale Risikoeinordnung. So kann die Risikoklassifizierung nach der KI-VO Anhaltspunkte

³⁰⁰ Sassenberg, RD 2025, 346, 350.

³⁰¹ Sassenberg, RD 2025, 346.

für die datenschutzrechtliche Bewertung liefern, während umgekehrt die Datenschutz-Folgenabschätzung als Ausgangspunkt für eine vertiefte KI-Risikobewertung dienen kann.³⁰²

Auch sind auf dieser Ebene strategische Leitlinien im Umgang mit Daten im Sinne der DS-GVO festzulegen. Gerade hier sind die Datenschutz-Grundsätze nach Art. 5 Abs. 1 DS-GVO als auch die Anforderungen an Data-Governance nach Art. 11 KI-VO zu bedenken. Schon hier ist an die Legalitätspflicht zu denken, die die zwingende Einhaltung der datenschutzrechtlichen und KI-rechtlichen Anforderungen erfordert.

Auch die Vermittlung grundlegender KI-Kompetenz wird auf der ersten Ebene verankert, um von Anfang an überhaupt eine informierte Einrichtung und Nutzung der KI-Anwendungen auf allen Organisationsebenen zu ermöglichen. Dabei ist darauf zu achten, dass es sich um Dauerverpflichtungen handelt, die eine regelmäßige Anpassung an technologische Entwicklungen und regulatorische Anforderungen erfordert.³⁰³

Die strategische Governance bildet damit das Fundament für alle nachgelagerten Prozesse.

b) Ebene 2: Operative Organisation und Compliance

Kern des Governance-Modells ist die integrierte Betrachtung von Datenschutz- und KI-Compliance – die Einhaltung des rechtlichen Ordnungsrahmens. Ein isolierter Compliance-Ansatz würde zwangsläufig zu Inkonsistenzen und ineffizienten Doppelstrukturen führen.

Ausgehend von der auf strategischer Ebene vorgenommenen Bestandsaufnahme – und den hierdurch aufgedeckten Lücken und Risiken – sind die identifizierten Anforderungen organisatorisch zu implementieren.³⁰⁴ Aus diesen Erkenntnissen können weitere interne Richtlinien entwickelt werden, die die Einhaltung der konkret durch die Risikoanalyse ausgelösten rechtlichen Pflichten – sowohl nach KI-VO als auch DS-GVO – sicherstellen und in konkrete Handlungsanweisungen für die Unternehmenspraxis übersetzen.³⁰⁵

Besonders ist dabei die Umsetzung der jeweiligen Informationspflichten und Ermöglichung der Auskunftsrechte zu beachten. Aber auch einheitliche Dokumentationsstandards, abgestimmte Kontrollmechanismen sowie klare Eskalationsprozesse sind festzulegen. Diese bilden die Grundlage für eine konsistente und rechtssichere Umsetzung der regulatorischen Anforderungen und minimieren zugleich haftungsrechtliche Risiken.³⁰⁶ Dabei sollte darauf

³⁰² Mackert/Ernst in Wieland/Steinmeyer/Grüniger, Hdb. Compliance-Management, Teil I. Kap. 1.4 Rn. 35.

³⁰³ Rappenglück/Vonthien, RD 398, 402.

³⁰⁴ Rappenglück/Vonthien, RD 398, 403.

³⁰⁵ Hoeren/Pinelli, KIR 2026, 5, 9.

³⁰⁶ Hafez in Windholz, KI-VO, Praxishandbuch, Kap. 10 S. 456; Hoeren/Pinelli, KIR 2026, 5, 7 Fn. 27.

geachtet werden, dass im gesamten Unternehmen ein gemeinsames Verständnis von Risiken und Schwellenwerten besteht, damit einheitlich festgelegt wird, wann welche Maßnahmen zu treffen sind.³⁰⁷

Zentrales Organisationsinstrument ist dabei die klare Zuweisung von Zuständigkeiten und Kontrollinstanzen. Während die Letztverantwortung bei den Leitungsorganen verbleibt, können operative Aufgaben delegiert werden. In der Praxis bietet sich vor allem die Benennung eines KI-Beauftragten an, der die Einhaltung der internen Richtlinien kontrolliert, die Schulungsmaßnahmen koordiniert und als Schnittstelle zwischen verschiedenen Unternehmensbereichen fungiert.³⁰⁸

Entscheidend ist, dass Delegation nicht zu einer Entkopplung von Verantwortung führt. Die Leitungsorgane müssen jederzeit in der Lage sein, den KI-Einsatz zu überblicken und steuernd einzugreifen.

c) Ebene 3: Risikomanagement und Kontrolle

Die dritte Ebene betrifft die fortlaufende Überwachung und Steuerung des KI-Einsatzes. KI-Systeme sind dynamische Systeme, deren Risikoprofil sich fortlaufend verändern kann – etwa durch neue Daten, veränderte Einsatzkontexte oder technische Updates. Governance darf sich daher nicht auf eine einmalige ex-ante-Bewertung beschränken.

Erforderlich ist ein kontinuierliches Monitoring, das insbesondere die Systemleistung, die Qualität und Repräsentativität der verwendeten Daten sowie die Einhaltung der vorgesehenen Kontrollmechanismen umfasst.³⁰⁹ Auch die Risikoklassifizierung ist regelmäßig zu überprüfen und bei Veränderungen anzupassen. Insofern sind auch Mitteilungspflichten und Meldeprozesse zu implementieren für den Fall, dass relevante Vorfälle oder unerwartetes Verhalten des KI-Systems entdeckt wird.³¹⁰

Diese Anforderungen entsprechen nicht nur den allgemeinen Überwachungspflichten der Leitungsorgane, sondern spiegeln auch die Vorgaben der KI-VO wider, insbesondere die Verpflichtung zur laufenden Beobachtung und Kontrolle des Systemverhaltens. Gleichzeitig ermöglichen sie es, datenschutzrechtliche Risiken frühzeitig zu erkennen und zu adressieren.

³⁰⁷ Hafez in Windholz, KI-VO, Praxishandbuch, Kap. 10 S. 455.

³⁰⁸ Knappertsbusch/Rappenglück, CR 2025, 281, 284.

³⁰⁹ Bolek-Fügl in Windholz, KI-VO, Praxishandbuch, Kap. 10 S. 480.

³¹⁰ Sassenberg, RD 2025, 346, 351.

Damit wird die operative Nutzung von KI-Systemen zu einem integralen Bestandteil des unternehmensweiten Risikomanagements.

d) Dokumentation als verbindendes Governance-Instrument

Eine zentrale Querschnittsfunktion innerhalb des Governance-Modells kommt der Dokumentation zu. Sie bildet das verbindende Element zwischen den Anforderungen der DS-GVO, der KI-VO und den gesellschaftsrechtlichen Organpflichten.

Dokumentation erfüllt dabei mehrere Funktionen zugleich: Sie dient dem Nachweis der Rechtmäßigkeit gegenüber Aufsichtsbehörden, ermöglicht interne Kontrolle und Steuerung und schafft haftungsrechtliche Absicherung der Leitungsorgane. Gleichzeitig stellt sie sicher, dass komplexe Entscheidungsprozesse nachvollziehbar bleiben.

Im integrierten KI-Governance-Modell ist Dokumentation daher keine bloße Formalie, sondern zentraler Bestandteil verantwortungsvoller Unternehmensführung. Sie macht Entscheidungsprozesse nachvollziehbar und schafft Transparenz in einem Bereich, der technisch häufig von Intransparenz geprägt ist.

V. Schlussbetrachtung

Das entwickelte KI-Governance-Modell zeigt, dass die Anforderungen der DS-GVO und der KI-VO nicht isoliert nebeneinanderstehen, sondern sich funktional ergänzen und in einem einheitlichen Organisationsrahmen zusammengeführt werden können. Während die DS-GVO die datenschutzrechtlichen Grenzen und Verfahrensanforderungen vorgibt, konkretisiert die KI-VO die systembezogenen Anforderungen an Entwicklung und Einsatz von KI-Systemen.

Erst durch ihre integrierte Umsetzung entsteht ein konsistentes Steuerungssystem, das den komplexen Risiken des KI-Einsatzes gerecht wird. Die gesellschaftsrechtlichen Organpflichten bilden dabei den übergeordneten Rahmen, innerhalb dessen beide Regelwerke operationalisiert werden.

KI-Governance erweist sich damit nicht als notwendige Konkretisierung ordnungsgemäßer Unternehmensorganisation im digitalen Zeitalter. Sie ermöglicht es, den Einsatz von KI-Systemen nicht nur rechtskonform, sondern auch strukturiert, transparent und risikoadäquat zu gestalten.

G. Fazit

Die Untersuchung hat gezeigt, dass der Einsatz von KI-Systemen in Unternehmen nicht lediglich eine technologische Innovation darstellt, sondern eine tiefgreifende organisationsrechtliche Herausforderung begründet. KI verändert Entscheidungsprozesse, verschiebt Verantwortungsstrukturen und schafft neue, systemimmanente Risiken, die sich insbesondere aus Intransparenz, Skalierbarkeit und Datenabhängigkeit ergeben.

Im Zentrum der rechtlichen Bewertung steht dabei die Erkenntnis, dass die bestehenden gesellschaftsrechtlichen Organpflichten grundsätzlich hinreichend flexibel sind, um auch den Einsatz von KI-Systemen zu erfassen. Insbesondere die Legalitätspflicht, die Sorgfaltspflicht sowie die Überwachungspflicht bilden einen tragfähigen normativen Rahmen, der durch den KI-Einsatz jedoch inhaltlich konkretisiert und verschärft wird. Die Leitungsorgane bleiben ungeachtet des Automatisierungsgrades „Herren des Verfahrens“ und tragen die Letztverantwortung für unternehmerische Entscheidungen.

Gleichzeitig hat die Analyse des unionsrechtlichen Rahmens gezeigt, dass sowohl die DS-GVO als auch die KI-VO eigenständige, aber funktional komplementäre Anforderungen an den Einsatz von KI-Systemen stellen. Die DS-GVO fokussiert auf den Schutz personenbezogener Daten und verlangt insbesondere Transparenz, Zweckbindung sowie eine strukturierte Risikobewertung durch Instrumente wie die Datenschutz-Folgenabschätzung. Demgegenüber adressiert die KI-VO die technischen und systemischen Risiken von KI-Systemen durch einen risikobasierten Regulierungsansatz, der insbesondere Klassifizierungs-, Dokumentations- und Überwachungspflichten umfasst.

Das Zusammenspiel beider Regelwerke führt zu einem kumulativen Pflichtenkreis, der ohne eine strukturierte organisatorische Einbettung kaum beherrschbar ist. Gerade an den Schnittstellen – etwa bei der Verbindung von Datenschutz-Folgenabschätzung und KI-Risikoklassifizierung, bei Transparenzanforderungen oder bei Dokumentationspflichten – zeigen sich sowohl Überschneidungen als auch wechselseitige Ergänzungen.

Vor diesem Hintergrund wurde im Rahmen der Arbeit ein integriertes KI-Governance-Modell entwickelt. Dieses Modell versteht KI-Governance als verbindendes Steuerungselement, das die normativen Anforderungen der DS-GVO und der KI-VO mit den gesellschaftsrechtlichen Organisationspflichten zusammenführt. Zentrale Elemente sind dabei eine strukturierte Einordnung von KI-Systemen, klare Zuständigkeits- und Kontrollstrukturen, ein

kontinuierliches Risikomanagement sowie eine umfassende Dokumentation als Nachweis- und Steuerungsinstrument.

Die wesentliche Erkenntnis besteht darin, dass KI-Governance keine zusätzliche, isolierte Compliance-Ebene darstellt, sondern als notwendige Konkretisierung ordnungsgemäßer Unternehmensorganisation im digitalen Zeitalter zu verstehen ist. Erst durch die Integration der unterschiedlichen regulatorischen Anforderungen in ein kohärentes Governance-System wird es möglich, den Einsatz von KI-Systemen nicht nur rechtskonform, sondern auch transparent, kontrolliert und risikoadäquat zu gestalten.

Für die Unternehmenspraxis bedeutet dies, dass der Einsatz von KI-Systemen zwingend eine Weiterentwicklung bestehender Governance-Strukturen erfordert. Unternehmen, die KI nicht lediglich als technisches Werkzeug, sondern als organisationsprägendes Element begreifen und entsprechend in ihre Corporate Governance integrieren, werden nicht nur regulatorischen Anforderungen besser gerecht, sondern können zugleich die Potenziale der Technologie effizient und verantwortungsvoll nutzen.

Abschließend lässt sich festhalten, dass die rechtliche Bewältigung des KI-Einsatzes nicht in der Schaffung immer neuer Einzelregelungen liegt, sondern in der konsequenten Verzahnung bestehender Normen und deren Überführung in funktionierende Organisationsstrukturen. Die KI-Governance bildet hierfür den zentralen Ansatzpunkt und zugleich den entscheidenden Maßstab für eine zukunftsfähige Unternehmensorganisation.

Literaturverzeichnis

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl., München 2019

Baumgartner, Ulrich/Brunnbauer, Jonas/Cross, Samuel, Anforderungen der DS-GVO an den Einsatz von Künstlicher Intelligenz – Welche Regelungen gelten für Anbieter und Anwender?, in Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT (MMR) 2023, S. 543 ff.

Binder, Nadja Braun/Egli, Catherine, Umgang mit Hochrisiko-KI-Systemen in der KI-VO – Strenge Anforderungen der Art. 8–15 KI-VO, in Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT (MMR) 2024, S. 626 ff.

Bomhard, David/Pieper, Fritz-Ulli/ Wende, Susanne, Kommentar zur Verordnung über künstliche Intelligenz, 1. Aufl., Frankfurt am Main 2025

Bomhard, David/Siglmüller, Jonas, AI Act – das Trilogergebnis, in Recht Digital (RDigital) 2024, S. 45 ff.

Calabro, Claudio, Künstliche Intelligenz und Corporate Governance – Der Einsatz Künstlicher Intelligenz im Vorstand der börsennotierten Aktiengesellschaft, Diss., Berlin 2023

Chibanguza, Kuuya J./Kuß, Christian/Steega, Hans (Hrsg.), Künstliche Intelligenz – Recht und Praxis automatisierter und autonomer Systeme – Generative KI – Rechtshandbuch, 2. Aufl., Baden Baden 2026

Dienes, Jennifer, Anforderungen an die menschliche Aufsicht über Künstliche Intelligenz – Verständnis als Kernelement des Art. 14 KI-VO, in Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT (MMR) 2024, S. 456 ff.

Dillig, Johannes/Musiol, Philip, KI-Verordnung und interne Ermittlungen, in Corporate Compliance (CCZ) 2024, S. 257 ff.

Ebers, Martin/Heinze, Christian/Krügel, Tina/Steinrötter, Björn, Künstliche Intelligenz und Robotik – Rechtshandbuch, 1. Aufl., München 2020

Ehmann, Eugen/Selmayr, Martin (Hrsg.), Beck'sche Kurz-Kommentare, Datenschutz-Grundverordnung, 3. Aufl., München 2024

Fleck, Tilmann, AI literacy als Rechtsbegriff – Anforderungen an die KI-Kompetenz nach Art. 4 KI-VO, in Zeitschrift für Künstliche Intelligenz und Recht (KIR) 2024, S. 99 ff.

Fleischer, Holger, Geschäftsleiterhaftung in der Personengesellschaft, in Neue Zeitschrift für Gesellschaftsrecht (NZG) 2024, S. 1639 ff.

Fleischer, Holger/Goette, Wulf (Hrsg.), Münchener Kommentar zum GmbHG, 5. Aufl., München 2026

Förster, Christian/Straburzynski, Julia, Die KI-Verordnung in der Praxis – Rechtliche Grundlagen und Pflichten bei der Anwendung von KI im Unternehmen, 1. Aufl., München 2025

Gausling, Tina, Künstliche Intelligenz im digitalen Marketing – Datenschutzrechtliche Bewertung KI-gestützter Kommunikations-Tools und Profiling-Maßnahmen, in Zeitschrift für Datenschutzrecht (ZD) 2019, S. 335 ff.

Goette, Wulf, Habersack, Mathias/Kalss, Susanne (Hrsg.), Münchener Kommentar zum AktG, Band 2: §§ 76-117 AktG, MitbestG, DrittelbG, 6. Aufl., München 2023

Gola, Peter/Heckmann, Dirk (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz – Kommentar, 3. Aufl., München 2022

Golland, Alexander, KI und KI-Verordnung aus datenschutzrechtlicher Sicht, in Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2024, S. 852 ff.

Grigoleit, Hans Christoph (Hrsg.), Aktiengesetz – Kommentar, 3. Aufl., München 2025

Hacker, Philipp/Berz, Amelie, Der AI Act der Europäischen Union – Überblick, Kritik und Ausblick, in Zeitschrift für Rechtspolitik (ZRP) 2023, S. 226 ff.

Hartmann, Matthias (Hrsg.), KI & Recht kompakt, 1. Aufl., Berlin 2020

Hersemeyer, Guillaume/Ludolph, Melanie, Datenschutzrechtliche Herausforderungen beim Einsatz künstlicher Intelligenz im Unternehmenskontext, in Bernzen/Fritzsche/Heinze/Thomsen, Deutsche Stiftung für Recht und Informatik, , Deutsche Stiftung für Recht und Informatik, Tagungsband Herbstakademie 2023 – Das IT-Recht vor der (europäischen) Zeitwende?, S. 365 ff.

Hilgendorf, Eric/Roth-Isigkeit, David, Die neue Verordnung der EU zur Künstlichen Intelligenz, 2. Aufl., München 2025

Hoeren, Thomas/Niehoff, Maurice, KI und Datenschutz – Begründungserfordernisse automatisierter Entscheidungen, in Rechtswissenschaft (RW) 2018, S. 47 ff.

Hoeren, Thomas/Pinelli, Stefan, KI-Compliance im Unternehmen – Anforderungen, Strukturen und Herausforderungen unter der KI-VO, in Künstliche Intelligenz und Recht (KIR) 2024, S. 5 ff.

Hölters, Wolfgang (Begr.)/Weber, Markus (Hrsg.), Aktiengesetz Kommentar, 5. Aufl., München 2025

Holthausen, Joachim, Big Data, People Analytics, KI und Gestaltung von Betriebsvereinbarungen – Grund-, arbeits- und datenschutzrechtliche An- und Herausforderungen, in Recht der Arbeit (RdA) 2021, S. 19 ff.

Hüffler, Uwe (Begr.)/Koch, Jens (Bearb.), Beck'sche Kurz-Kommentare, Aktiengesetz, 19. Aufl., München 2025

Ifsits, Clara/Minihold, Anna/Roubik, Marleen, Haftungsfragen beim Einsatz Künstlicher Intelligenz – Zivilrecht – Strafrecht – Datenschutzrecht, 1. Aufl., Wien 2020

Jandt, Silke/Steidle, Roland (Hrsg.), Datenschutz und Internet, DS-GVO, BDSG, TDDDG, KI-VO, DMA, DAS, 2. Aufl., Baden-Baden 2025

Knappertsbusch, Ina/Rappenglück, David, KI-Kompetenz und verbotene KI-Praktiken als Compliance-Pflichten für Arbeitgeber Anforderungen an die strategische Neuausrichtung der innerbetrieblichen Governance, in Zeitschrift für Computer und Recht (CR) 2025, S. 281 ff.

- Kühling, Jürgen/Buchner, Benedikt (Hrsg.)*, Datenschutz-Grundverordnung, BDSG – Kommentar, 4. Aufl., München 2024
- Langheld, Georg/Heinze, Christian*, Einsatz Künstlicher Intelligenz bei unternehmerischen Entscheidungen – Möglichkeiten, Pflichten und offene Fragen, in *Neue Zeitschrift für Gesellschaftsrecht (NZG)* 2023, S. 1535 ff.
- Lühmann, Daniel/Görgülü, Can/Marciniak, Jörg*, Einsatz von KI im Asset Management – Ein Blick auf die regulatorische Landschaft mit Fokus auf die KI-Verordnung der EU, in *Zeitschrift für Bank- und Kapitalmarktrecht (BKR)* 2024, S. 175 ff.
- Lukas, Arnold J. F.*, Privacy Enhancing Technologies im Zusammenspiel mit der DS-GVO – Beispiele aus der Praxis und rechtliche Auswirkungen, in *Zeitschrift für Datenschutzrecht (ZD)* 2023, S. 321 ff.
- Mainzer, Klaus*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, 2. Aufl., Berlin 2019
- Martini, Mario/Wendehorst, Christiane*, Kommentar zur Verordnung über künstliche Intelligenz, 2. Aufl., München 2026
- Merkle, Marieke Luise*, Transparenz nach der KI-Verordnung – von der Blackbox zum Open-Book?, in *Recht Digital (RDigital)* 2024, S. 414 ff.
- Moll, Wilhelm (Begr.)/Eckhoff, Frank/Reufels, Martin (Hrsg.)*, Münchener Anwalts Handbuch Arbeitsrecht, 6. Aufl., München 2025
- Moosmeyer, Klaus/Lösler, Thomas (Hrsg.)*, Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen, 4. Aufl., München 2024
- Möslein, Florian*, Digitalisierung im Gesellschaftsrecht: Unternehmensleitung durch Algorithmen und künstliche Intelligenz?, in *Zeitschrift für Wirtschaftsrecht (ZIP)* 2018, S. 204 ff.
- Oliver, Lücke*, Der Einsatz von KI in der und durch die Unternehmensleitung, in *Betriebs-Berater (BB)* 2019, S. 1986 ff.

- Orssich, Irina*, Das europäische Konzept für vertrauenswürdige Künstliche Intelligenz, in Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2022, S. 254 ff.
- Paal, Boris P.*, KI-Training mit öffentlich frei zugänglichen Daten im Lichte der DS-GVO-Vorgaben, in Zeitschrift für Digitalisierung und Recht (ZfDR) 2024, S. 129 ff.
- Paal, Boris P./Pauly, Daniel A. (Hrsg.)*, Beck'sche Kompakt Kommentare, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 4. Aufl., München 2026
- Pesch, Paulina Jo/Böhme, Rainer*, Verarbeitung personenbezogener Daten und Datenrichtigkeit bei großen Sprachmodellen – ChatGPT & Co. unter der DS-GVO, in Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT (MMR) 2023, S. 917 ff.
- Plagemann, Nikolaus*, Aktienrechtliche Verhaltenspflichten in Bezug auf KI, in Neue Zeitschrift für Gesellschaftsrecht (NZG) 2025, S. 684 ff.
- Rappenglück, David/Vonthien, Maximilian*, Art. 4 KI-VO operativ umsetzen – Ein Drei-Säulen-Ansatz für KI-Kompetenz, KI-Governance und KI-Compliance im Unternehmen, in Recht Digital (RDigital) 2025, S. 398 ff.
- Recktenwald, Nina*, Datenschutzrechtliche Herausforderungen bei der Einführung von KI in Unternehmen, in Bernzen/Fritzsche/Heinze/Thomsen, Deutsche Stiftung für Recht und Informatik, Tagungsband Herbstakademie 2023 – Das IT-Recht vor der (europäischen) Zeitwende?, S. 387 ff.
- Reese, Hendrik*, KI-Governance: Implementierung im Unternehmen, in Betriebs-berater (BB) 2024, S. 1515 ff.
- Reichert, Florian/Radtke, Kristina/Eske, Hermann*, KI -Verordnung: Rechtsgrundlagen für die Bereitstellung und Nutzung von KI – Betrachtung des vom LfDI BW initiierten Diskussionspapiers, in Zeitschrift für Datenschutzrecht (ZD) 2024, S. 483 ff.
- Ritter, Thomas*, KI und Weisungsrecht, in Zeitschrift für Arbeitsrecht und Tarifpolitik in kirchlichen Unternehmen (ZAT) 2025, S. 11 ff.
- Ritter, Thomas*, KI-Einsatz im Krankenhaus und Organhaftung, in Gesundheit und Pflege (GuP) 2025, S. 53 ff.

Roßnagel, Alexander, Digitale Souveränität im Datenschutzrecht – Voraussetzung für die Umsetzung datenschutzrechtlicher Anforderungen, in Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT (MMR) 2023, S. 64 ff.

Roßnagel, Alexander/Geminn, Christian L., Vertrauen in Anonymisierung – Regulierung der Anonymisierung zur Förderung Künstlicher Intelligenz, in Zeitschrift für Datenschutzrecht (ZD) 2021, S. 487 ff.

Sassenberg, Thomas, AI Governance Framework – Regelungsgegenstand der AI Policy, in Recht Digital (RD) 2025, S. 346 ff.

Schäfer, Lena, Datenschutz-Compliance im KI-Training – Datenschutzkonformes KI-Training in der Praxis, Zeitschrift für Datenschutzrecht (ZD) 2025, S. 12 ff.

Schefzig, Jens/Kilian, Robert, Beck Online Kommentar KI-Recht, 4. Edition, München
Stand: 01.11.2025

Schippel, Robert, Trainingsvorgaben: Wie kann man KI-Kompetenz nach Art. 4 KI-VO vermitteln? – Strategievorschlag zur effektiven Vermittlung von KI-Kompetenz, in Zeitschrift für Künstliche Intelligenz und Recht (KIR) 2025, S. 119 ff.

Schleipfer, Stefan, Pseudonymität in verschiedenen Ausprägungen – Wie gut ist die Unterstützung der DS-GVO?, in Zeitschrift für Datenschutzrecht (ZD) 2020, S. 284 ff.

Schröder, Georg F., Datenschutzrecht für die Praxis – Grundlagen, Datenschutzbeauftragte, Audit, Handbuch, Haftung etc., 6. Aufl., München 2026

Schürmann, Kathrin, Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz – Bewertung und Minimierung der Risiken, in Zeitschrift für Datenschutzrecht (ZD) 2022, S. 316 ff.

Schwartmann, Rolf/Keber, Tobias/Zenner, Kai (Hrsg.), KI-VO – Leitfaden für die Praxis, 3. Aufl., Heidelberg 2025

Simitis, Spiros/Hornung, Gerrit/Spiecker genannt Döhmman, Indra (Hrsg.), Kommentar zum Datenschutzrecht, DS-GVO/BDSG, 2. Aufl., Baden-Baden 2025

Spindler, Gerald/Schuster, Fabian/Kaesling, Katharina (Hrsg.), Recht der elektronischen Medien – Kommentar, 5. Aufl., München 2026

Stilz, Eberhard/Veil, Rüdiger (Hrsg.), Beck Online Großkommentar, Aktienrecht, München
Stand: 01.10.2025

Taeger, Jürgen/Gabel, Detlef (Hrsg.), DSGVO – BDSG – TDDDG, 5. Aufl., Frankfurt am Main 2026

Teichmann, Fabian, Neuer Rechtsrahmen für vertrauenswürdige KI – Risikobasierte Regulierung, Transparenzpflichten und Schnittstellen zum Datenschutzrecht, in Zeitschrift für Datenschutzrecht (ZD) 2025, S. 495 ff.

Vasel, Johann Justus, Künstliche Intelligenz in der Justiz, in Legal Tech – Zeitschrift für die digitale Rechtsanwendung (LTZ) 2023, S. 179 ff.

Weber, Robert/Kiefner, Alexander/Jobst, Stefan, Künstliche Intelligenz und Unternehmensführung, in Neue Zeitschrift für Gesellschaftsrecht (NZG) 2018, S. 1131 ff.

Wieland, Josef/Steinmeyer, Roland/Grüninger, Stephan (Hrsg.), Handbuch Compliance-Management – Konzeptionelle Grundlagen, praktische Erfolgsfaktoren, globale Herausforderungen, 4. Aufl., Berlin 2025

Windholz, Natascha, Praxishandbuch KI-VO – Künstliche Intelligenz rechtskonform im privaten und öffentlichen Bereich einsetzen, 1. Aufl., München 2024

Wolff, Heinrich Amadeus/Brink, Stefan/v. Ungern-Sternberg, Antje, Beck Online Kommentar Datenschutzrecht, 54. Edition, München Stand: 01.11.2025