



## MANAGEMENT SUMMARY

Künstliche Intelligenz (KI) kann für viele Zwecke genutzt werden. Sie ist dabei wie jede andere Technologie zunächst wertneutral und kann - falsch eingesetzt - auch für Mensch und Umwelt schädliche Effekte hervorrufen. Die Europäische Union arbeitet daher an Regularien für Entwicklung und Einsatz von KI. Diese haben das Potential - ähnlich wie bereits im Bereich Datenschutz passiert - durch globale Vernetzung und Übernahme in Länder außerhalb der EU zum weltweiten De-Facto-Standard für ethische KI zu werden. Wir fassen den aktuellen Stand (März 2022) kompakt zusammen



## FAKTEN

### Entwicklung der KI-Gesetzgebung in der EU

Während KI in den USA von großen Konzernen und in China von staatlicher Seite gelenkt vorangetrieben wird, hinkt Europa in diesem Bereich bisher hinterher. Die Ursachen hierfür sind vielfältig. Moralische Vorbehalte, rechtliche Bedenken und daraus resultierendes Misstrauen gegenüber der Technologie tragen in jedem Fall dazu bei, dass öffentliche und privatwirtschaftliche Initiativen nur gebremst oder gar nicht voranschreiten und KI nur sehr zögerlich Eingang in Produkte und Prozesse findet.

Die EU möchte die Entwicklung von KI fördern, gleichzeitig aber auch öffentliche Interessen schützen und Vertrauen in KI schaffen. Zu diesem Zweck sollen Standards definiert werden, die rechtliche und ethische Klarheit schaffen und KI-Entwicklern sinnvolle Rahmenbedingungen geben. Zu diesem Zweck erarbeitete eine internationale, unabhängige Expertengruppe eine 2019 veröffentlichte Leitlinie für vertrauenswürdige

KI, die als Basis für einen offiziellen Entwurf für ein europäisches KI-Gesetz<sup>1</sup> diene. Der aktuelle Gesetzentwurf vom April 2021 soll - nach Überarbeitung und endgültiger Verabschiedung - voraussichtlich ab 2023 den Rechtsrahmen zu KI in der EU bilden (als Teil des sogenannten „Koordinierten Plans für KI“<sup>2</sup>). Der Entwurf beinhaltet Verbote bestimmter KI-Anwendungen, Anforderungen und Pflichten für KI-Systeme mit hohem Risiko, sowie darüber hinaus Transparenzpflichten für KI-Systeme. Außerdem wurden vor dem Hintergrund des Green Deal der EU ökologische und soziale Nachhaltigkeitsaspekte gestärkt. Ergänzt wird der vorgeschlagene Gesetzentwurf für KI durch eine Maschinenrichtlinie<sup>3</sup>.

Ebenfalls 2019 erschienen auch seitens der OECD ähnliche Grundsätze für Künstliche Intelligenz als Empfehlung für Regierungen, Investoren und Entwickler von KI. Rechtlich bindend sind diese OECD-Grundsätze jedoch nicht. Das europäische KI-Gesetz hingegen wird die EU-Mitgliedsstaaten weitgehend zur Umsetzung verpflichtet. Aufgrund der wirtschaftlichen Bedeutung Europas und der globalen Verflechtung von Märkten hat das zukünftige EU-Recht für KI das Potential, sich zum weltweiten Standard zu entwickeln (ähnlich wie dies z.B. im Bereich Datenschutz durch GDPR geschehen ist).



### Grundsätzliche Vorgaben für vertrauenswürdige KI

Leitlinie und Gesetzentwurf der EU machen einige grundlegende Vorgaben. So müssen KI-Systeme alle geltenden Gesetze, aber auch ethische Grundsätze befolgen, Menschenrechte achten und Schäden – speziell für Menschen – vermeiden. Sie müssen zuverlässig gesichert gegen nachteilige Effekte sein, egal ob diese aus unbeabsichtigten Fehlern des Systems oder aus Angriffen von außen resultieren. Sicherheit und Robustheit gegenüber Fehlern beinhalten auch Aspekte wie Genauigkeit, Zuverlässigkeit und Reproduzierbarkeit.

Fairnessgebot und Diskriminierungsverbot mögen selbstverständlich klingen, waren aber in den letzten Jahren bereits in der öffentlichen Diskussion, da sich in manche KI bereits menschliche Vorurteile eingeschlichen haben. Algorithmen lernen auf der Basis von eingespeisten Daten. Sind diese unausgewogen oder beinhalten sie Zusammenhänge, die sich aus faktischer Diskriminierung in der analogen Welt ergeben, dann führt dies zum vieldiskutierten KI Bias (Voreingenommenheit der KI).

Die geforderte Menschenzentrierung für KI findet auch darin Ausdruck, dass KI erklärbar sein muss. Transparente Rückverfolgbarkeit, Nachvollziehbarkeit, Überprüfbarkeit und Verständlichkeit von Empfehlungen und Entscheidungen sind essentiell. Entsprechende Kommunikation, z.B. mit Behörden und Betroffenen, muss gewährleistet

<sup>1</sup> <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52021PC0206&from=DE>

<sup>2</sup> <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review>

<sup>3</sup> <https://ec.europa.eu/docsroom/documents/45508?locale=de>

sein. Dies gilt auch für das Auftreten und die Wiedergutmachung von Schadensfällen (Rechenschaftspflicht).

Neben den Algorithmen selbst stellt das Gesetz auch Anforderungen an die Qualität und Sicherheit der zugrundeliegenden Daten. Natürlich gelten die Prinzipien des Schutzes personenbezogener Daten (Datenschutz gemäß GDPR) in vollem Umfang. Idealerweise werden nur anonyme Daten verwendet, und wo doch personenbezogene Daten erforderlich sind, sind diese auf ein Minimum und den vorab vereinbarten Zweck zu beschränken und nach Erfüllung dieses Zwecks zu löschen.

Für das ordnungsgemäße und legale Funktionieren eines KI-Systems muss aber auch sichergestellt sein, dass die Daten korrekt sind und nicht durch schlechte Datenqualität fehlerhafte KI-Modelle und Entscheidungen entstehen. Das Thema Datenqualität hat bekanntlich über triviale Fehler hinaus viele Facetten<sup>4</sup>. Probleme fallen aufgrund des hohen Automatisierungsgrades innerhalb von KI-Systemen nicht immer sofort auf. Intensive Prüfmaßnahmen – auch und gerade im laufenden Betrieb – können erforderlich sein.

Die genannten Vorgaben gelten für alle Phasen des Lebenszyklus eines KI-Systems, also bei Konzeption und Entwicklung, während der produktiven Nutzung, aber auch danach (z.B. in Archiven). Nach Verabschiedung des Gesetzes sind sie für jegliche Nutzer und Anbieter von KI-Lösungen innerhalb der EU verbindlich, unabhängig von Herkunft und Firmensitz. Hierin liegt der potenziell weltweite Hebel der EU-Gesetzgebung.



### Konkretisierung für die Praxis

Um die obigen allgemeinen Grundsätze praktikabel zu machen, klassifizieren Richtlinie und Gesetzentwurf der EU die verschiedenen KI-Systeme hinsichtlich ihres Risikos.

Bestimmte Anwendungen werden dabei als inakzeptabel (unannehmbares Risiko) eingestuft. Hierzu gehören u.a. Social-Scoring-Applikationen und solche Systeme, die menschliches Verhalten unterbewusst manipulieren, aber auch biometrische Fernerkennung (z.B. Gesicht, Stimme, Gang) in Echtzeit. Sie sind im Geltungsbereich des EU-Gesetzes zukünftig verboten<sup>5</sup>.

Klare Anforderungen existieren an diejenigen KI-Systeme, die zwar grundsätzlich als sinnvoll, aber auch als besonders riskant eingestuft werden. Die Liste solcher Hochrisikoapplikationen ist lang: kritische Infrastruktur (wozu auch autonomes Fahren gezählt wird) und Sicherheitskomponenten innerhalb von (z.B. medizinischen) Produkten gehören genauso dazu wie jegliche Anwendungen, die Menschen bewerten und durch diese Bewertung benachteiligen können (beispielsweise Kreditrisikobewertung

<sup>4</sup> <https://de.wikipedia.org/wiki/Informationsqualit%C3%A4t>

<sup>5</sup> Für den Einsatz von Gesichtserkennung ist die gesellschaftliche und juristische Diskussion noch im Fluss.

oder automatisches Scoring von Bewerbungen oder Prüfungen). Auch hoheitliche Aufgabengebiete (z.B. in der Strafverfolgung oder bei Grenzkontrollen) und erlaubte Anwendungen für biometrische Identifizierungslösungen werden als hochriskant eingestuft. Für alle diese Applikationen gelten besonders strenge Vorschriften hinsichtlich Robustheit, Sicherheit, Risikomanagement, Transparenz, Datenqualität und anderer Kriterien. Um Risiken zu minimieren, müssen sie in angemessenem Umfang unter menschlicher Aufsicht stehen. Verstöße gegen diese Vorgaben sollen als Rechtsbruch strafrechtlich verfolgt werden können.

Bei KI-Systemen mit geringem Risiko steht Transparenz als wesentliches Gebot im Vordergrund. Nutzer von Chatbots müssen beispielsweise erkennen können, dass sie mit einer Maschine interagieren. Der Einsatz von KI-Systemen mit minimalem Risiko (z.B. Spamfilter und viele andere KI-gestützte Funktionen innerhalb von größeren Applikationen) soll auch in dieser Hinsicht weitgehend uneingeschränkt möglich sein. Hier greift letztlich die normale Produkthaftung.



### FAZIT

Trotz mancher noch offener Themen in vielen Anwendungsgebieten, z.B. nach den Rechten an den zugrundeliegenden Daten, Haftungsfragen oder auch nach den konkreten zivil- und strafrechtlichen Folgen von Verstößen, bietet der zukünftige Rechtsrahmen eine sichere Grundlage für Anbieter und Anwender von KI. Ein zeitnaher Abschluss des Gesetzgebungsverfahrens ist zu wünschen, auch um die im „Koordinierten Plan für KI“ angelegte systematische Förderung zeitnah umzusetzen und die Aufholjagd Europas in diesem Gebiet mit vollem Schwung starten zu können.



### Disclaimer

Aufgrund des noch laufenden Gesetzgebungsverfahrens sind viele der Informationen in diesem Dokument als Sach- und Diskussionsstand zum Zeitpunkt März 2022 zu verstehen. Von Veränderungen im weiteren Verlauf ist auszugehen.

### Autor

Dr. Marcus Dill ist mehrfacher erfolgreicher Unternehmensgründer und langjähriger Management Berater mit den Schwerpunkten Data, Analytics und Sustainability.

Kontakt: [Ingdilligenz GmbH](https://www.ingdilligenz.com)

[www.ingdilligenz.com](https://www.ingdilligenz.com)

[sustainability@ingdilligenz.com](mailto:sustainability@ingdilligenz.com)

