SCHÜRMANN
ROSENTHAL
DREYER
RECHTSANWÄLTE

DIGITALES BUSINESS · TECHNOLOGIE · MEDIEN

BUJ
Bundesverband
der Unternehmensjuristen

Die KI-Verordnung kommt: Leitfaden für Unternehmen

Jetzt ist der richtige Zeitpunkt mit der Umsetzung zu beginnen

Whitepaper — Stand: November 2022

Inhaltsverzeichnis

Vorwort 4

1 Einführung 5

2 KI in Unternehmen – Bestandsaufnahme und Potentiale 7

3 Einführung in die KI-VO 10

3.1 Gründe und Ziele der KI-VO 10

3.2 Aktuelles zum Gesetzgebungsverfahren 11

3.3 An wen richtet sich die KI-VO? – Anwendungsbereich der Verordnung 12

3.3.1 Sachlicher Anwendungsbereich 12

3.3.2 Persönlicher Anwendungsbereich 13

3.3.3 Räumlicher Anwendungsbereich 14

3.4 Regelungssystematik der KI-VO – Risikobasierter Ansatz 15

3.4.1 Verbotene KI-Praktiken 15

3.4.2 Hochrisiko-KI 15

3.4.3 Geringes und minimales Risiko 16

3.5 Die KI-VO und die DSGVO 18

4 Herausforderungen aus der KI-VO für Unternehmen 19

4.1 Risikomanagementsysteme (Art. 9 KI-VO-E) 21

4.2 Daten und Data-Governance (Art. 10 KI-VO-E) 21

4.3 Dokumentationspflichten (Art. 11 KI-VO-E) 22

4.4 Aufzeichnungspflichten (Art. 12 KI-VO-E) 23
4.5 Transparenz- und Instruktionspflichten (Art. 13 KI-VO-E) 23
4.6 Menschliche Aufsicht (Art. 14 KI-VO-E) 24
4.7 Genauigkeit, Robustheit und Cybersicherheit (Art. 15 KI-VO-E) 24
4.8 Qualitätsmanagementsystem (Art. 17 KI-VO-E) 25
4.9 Konformitätsbewertungsverfahren (Art. 19 KI-VO-E) 25
4.10 Weitere Verpflichtungen für Hochrisiko-KI 27
4.11 Transparenzpflichten für bestimmte KI-Systeme (Art. 52 KI-VO-E) 27
4.12 Freiwillige Verhaltenskodizes für Systeme ohne hohes Risiko (Art. 69 KI-VO-E) 27
4.13 Folgen von Verstößen (Art. 71 KI-VO-E) 28

5 Lösungsansätze und Synergien zum Datenschutzrecht 29
5.1 Was Unternehmen jetzt schon tun sollten 29
5.2 Lösungsansätze bezüglich einzelner Anforderungen 30
5.2.1 Bestehende Prozesse nutzen 30
5.2.2 Zur Produktivsetzung von KI 32
5.3 KI und datenschutzrechtliche Anforderungen 32

6 Fazit 34

7 Weitere rechtliche Herausforderungen – Exkurs ins Patent- und Urheberrecht 35

Rechtsanwälte für Digitales Business, Technologie & Medien 38

Ihre Ansprechpartner 38

Vorwort

Die geplante KI-Verordnung (KI-VO) ist ein Prestigeprojekt der EU. Es ist zu erwarten, dass das groß angelegte Regulierungsvorhaben die Verbreitung und den Einsatz von künstlicher Intelligenz (KI) in der Union und über ihre Grenzen hinaus erheblich beeinflussen wird. Unternehmen, die KI-Anwendungen bereits einsetzen, entwickeln oder sich das enorme Potenzial von KI noch zunutze machen möchten, sollten sich unbedingt schon jetzt mit der KI-VO auseinandersetzen. Auch wenn das Gesetzgebungsverfahren noch nicht beendet ist, lohnt die sorgfältige Vorbereitung, um zu verhindern, dass für gegenwärtig schon in der Entwicklung befindliche KI-Anwendungen zum späteren Zeitpunkt aufwendige Nach-Dokumentationen erfolgen müssen.

Das vorliegende Whitepaper bietet dabei eine Hilfestellung. Zunächst wird aufgezeigt, an welchen Stellen in Unternehmen bereits KI-Anwendungen im Einsatz sein können und für welche Teams und Abteilungen das Thema üblicherweise bereits relevant ist. Anschließend erfolgt eine Einführung in den aktuellen Entwurf der KI-VO. Der Fokus liegt dabei vor allem auf dem Anwendungsbereich der geplanten Verordnung. Denn es ist wichtig, dass Unternehmen frühzeitig erkennen, ob und inwiefern sie von den künftigen Vorgaben der KI-VO betroffen sein werden, um dementsprechend Maßnahmen zu planen und zu ergreifen. Zudem wird ein Einblick in den Regulierungsansatz, die Struktur und den derzeitigen Stand des Gesetzgebungsverfahrens des KI-VO-Entwurfes (KI-VO-E) gegeben. Im Anschluss werden die absehbaren konkreten Herausforderungen für Unternehmen im Hinblick auf die KI-VO skizziert. Zuletzt sollen Lösungsansätze vorgestellt werden, um diese Herausforderungen zu meistern. Dafür wird insbesondere auch auf bewährte Strategien im Umgang mit anderen Compliance-Vorgaben, beispielsweise der DSGVO, zurückgegriffen.

1 Einführung

KI-Anwendungen sind inzwischen branchenübergreifend in Unternehmen verbreitet. Für das enorme Potenzial und die Vorteile, die KI für Unternehmensabläufe mit sich bringen kann, entsteht ein immer ausgeprägteres Bewusstsein. Neben Bereichen wie smarte Prognosen in der Logistik für Einkauf und Warenhaltung (Demand Forecasting, Supply Planning), intelligente Routenplanungen und Echtzeit-Bilderkennung für das autonome Fahren, Wartungsvorhersagen (Predictive Maintenance) oder KI-gestützte Ressourcenplanung und Sicherheitsanwendungen im Cloud Computing werden zunehmend klassische Teilprozesse durch KI-basierte Assistenzsysteme unterstützt. Beispielsweise werden nunmehr Risikoprognosen und Scoring im Bank- und Versicherungswesen durch Einsatz von KI ergänzt und in der Kundenbetreuung lässt sich mithilfe von KI-betriebenen Chatbots durch schnelle Antworten und ständige Erreichbarkeit die Kundenzufriedenheit effizient steigern.

Dennoch ist auch in Unternehmen nach wie vor eine gewisse Skepsis gegenüber „intelligenten" Systemen zu beobachten. Diese Skepsis ist mitunter auf schwer zu überblickende juristische Risiken zurückzuführen, die mit dem Einsatz von KI einhergehen. Insbesondere im Bereich der Datenverarbeitung ergeben sich strenge rechtliche Anforderungen – KI-Systeme benötigen oft große Datenmengen, um modelliert und angelernt zu werden – und nutzen im operativen Betrieb Daten, um den Algorithmus autonom weiterzuentwickeln. Hauptregelungswerk ist dafür bisher die EU-Datenschutzgrundverordnung (DSGVO). Darüber hinaus haben Kritiker ethische Bedenken oder sehen das Risiko der Verwendung qualitativ ungeeigneter Daten. Nicht zuletzt sind auch Personen in Entscheidungspositionen mit den möglichen Anwendungsbereichen und Vorgaben des Einsatzes von KI schlicht nicht vertraut.

Um Anreiz für Investitionen in die KI-Entwicklung zu geben und ihre Verbreitung in der EU zu fördern, hat es sich die EU-Kommission zur Aufgabe gemacht, einen Rechtsrahmen für ‚vertrauenswürdige' künstliche Intelligenz in der Europäischen Union zu entwickeln.

Zur Schaffung harmonisierter Vorschriften für KI hat sie deshalb am 21. April 2021 einen Vorschlag für eine Verordnung zu einem „Gesetz über künstliche Intelligenz" vorgelegt. Gegenwärtig ergänzen der Ministerrat und das EU-Parlament den Vorschlag der Kommission. Es ist zu erwarten, dass die Verordnung schon im Jahr 2023 in Kraft tritt; darauf wird voraussichtlich noch eine dreijährige Umsetzungsfrist bis zur tatsächlichen Anwendbarkeit folgen.

Für den Begriff ‚künstliche Intelligenz' existiert (bisher) keine einheitliche Definition. Hauptmerkmale für ein KI-System sind ein gewisses Maß an autonomer Funktionsweise und ein sich anpassender Verarbeitungsprozess.

KI lässt sich also grob als ein Phänomen selbstlernender Software-Algorithmen beschreiben, die meist Aufgaben übernehmen, die traditionell von Menschen ausgeführt werden. Die geplante KI-VO bietet erstmals eine Legaldefinition des KI-Begriffs und legt damit ihren Geltungsbereich fest. In dem Kommissionsentwurf wurde dabei noch ein äußerst weiter Begriff zugrunde gelegt, was von vielen Seiten kritisiert wurde. In dem nun vorliegenden Kompromissvorschlag des EU-Ministerrats vom 15. Juli 2022 wurde die Definition deshalb enger gefasst. Die aktuelle Definition von KI laut dem Kompromissvorschlag des Rats ist Grundlage für dieses Whitepaper. Im Kapitel 3 wird auf die Begrifflichkeiten der KI-VO genauer eingegangen.

2 KI in Unternehmen – Bestandsaufnahme und Potentiale

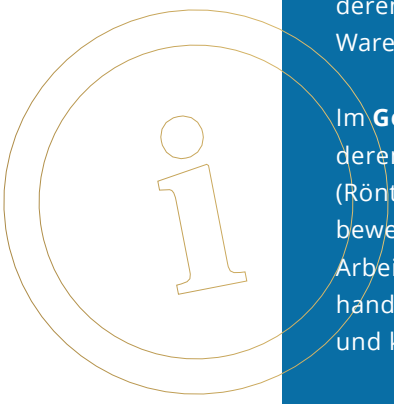
Künstliche Intelligenz ist eines der zentralen Zukunftsthemen für deutsche Unternehmen. So ergab eine Studie des Fraunhofer-Instituts für Arbeitswirtschaft und Organisation, dass sich 75 Prozent der im Jahr 2019 befragten Betriebe mit Fragestellungen zum Thema KI beschäftigten (Künstliche Intelligenz in der Unternehmenspraxis, Fraunhofer IAO, 2020, S. 28). Das zeigt, dass trotz des vermeintlich noch überschaubaren Einsatzes von KI-Anwendungen das Interesse an dem Thema bereits äußerst groß ist. So bereiteten laut der Fraunhofer-Studie 14 Prozent der befragten Unternehmen die Einführung von künstlicher Intelligenz bereits vor. 45 Prozent beschäftigten sich ausführlicher mit der Thematik oder analysierten konkret die Potenziale für den eigenen Betrieb. Dies manifestiert sich auch darin, dass der Anteil von Unternehmen, die KI einsetzten, seit Durchführung der **Studie des Fraunhofer-Instituts stetig gestiegen ist** (Künstliche Intelligenz kommt in Unternehmen allmählich voran, Bitkom e. V., Branchenverband der deutschen Informations- und Telekommunikationsbranche). Dabei wird die generelle Bedeutung von künstlicher Intelligenz für die Zukunft der Unternehmen in nahezu allen Bereichen als hoch eingeschätzt. Bemerkenswert ist, dass vor allem Studienteilnehmer der Zukunft von KI einen besonders hohen Stellenwert beimaßen, in deren Unternehmen KI bereits im Einsatz war. Dies spiegelt wider, wie gewinnbringend die KI-Systeme für die nutzenden Betriebe sind, und verdeutlicht, dass sich Investitionen und Risiken lohnen. Die Anwendungsbeispiele für KI sind dabei vielfältig und branchenübergreifend:

So spielt KI eine zentrale Rolle in der umfassenden Digitalisierung der **industriellen Produktion** (Industrie 4.0). Beispielsweise können mithilfe von Sensoren gesammelte Messwerte und Daten von KI-Systemen vorausschauend ausgewertet werden, um Maschinen und Anlagen autonom und proaktiv zu warten (Predictive Maintenance). Dadurch kann eine schnellere Entscheidungsfindung und effizientere Auslastung auf allen Wertschöpfungsstufen garantiert werden. Mittels KI können selbstlernende Fabriken so ihre Produktionsprozesse optimieren (Cognitive Maintenance). Unter Verwendung von KI-Systemen und 3D-Druckern ermöglichen „Speed-Factories" Produktion mit hoher Geschwindigkeit. ↓

Im Bereich des **Unternehmensmanagements** kann KI bei der Datenanalyse unterstützen und so Markttrends aufgreifen und bei Innovationsentscheidungen Hilfestellung leisten. Auch ermöglicht sie eine automatisierte Buchhaltung oder Recruiting mittels Chatbots. Mithilfe von „Predictive Analytics" können zukünftige Geschäftsentwicklungen analysiert werden, so können KI-Systeme bei der Entwicklung von Unternehmensstrategien assistieren.

Insbesondere in **Marketing, Vertrieb und der Kundenbetreuung** hat sich KI schon heute bewährt. So können die Systeme im Internet verfügbare Informationen und Muster in Nutzerdaten auswerten, um personalisierte, relevante Werbung zu individuellen Zeitpunkten zu schalten. Zudem lässt sich Customer-Service mithilfe von Chat-Bots und Assistenzsystemen zu weiten Teilen automatisieren. Ein Paradebeispiel dafür sind Speech-to-Text- und Text-to-Speech-Lösungen, die automatisierte, personalisierte Gespräche mit Kund:innen erlauben.

Auch in **Handel und Logistik** findet KI diverse Anwendungsfelder. Unter anderem wird sie für Preisoptimierung, Vertriebsvorhersagen, Einkaufsplanung, Warendisposition, logistische Vorhersagen oder Betrugsprävention eingesetzt.



Im **Gesundheitswesen** dienen KI-Systeme zur Diagnose von Krebs oder anderen, darunter seltenen Krankheiten, bei bildgebenden Untersuchungen (Röntgen, CT, MRT etc.) können sie Muster und Abweichungen erkennen und bewerten. Ferner kann KI bei chirurgischen Eingriffen assistieren, indem sie Arbeitsabläufe überwacht und bei Therapieentscheidungen unterstützt. Anhand von KI erzeugten digitalen Patientenmodellen werden personalisierte und kostenoptimierte Behandlungen ermöglicht.

KI-Systeme werden zudem in der **IT-Sicherheit** in Zukunft eine entscheidende Rolle spielen. Angriffserkennungssysteme (Intrusion Detection System, IDS) erkennen verdächtige Vorgänge und mögliche Bedrohungen und ungewollten Abfluss von Daten. Abwehrsysteme (Intrusion Prevention System, IPS) ergreifen sodann autonom entsprechende Gegenmaßnahmen. Durch Deep Learning können auch bisher unbekannte Malware oder Cyberangriffe abgewehrt werden.

Nicht zuletzt im Bereich der **Rechtsdienstleistungen** gewinnt KI zunehmend an Bedeutung (Legal Tech). So unterstützen die Systeme bei der Vertragsüberprüfung, bei rechtlicher Recherche und in der Prozessvorbereitung. Allgemein wird durch KI der Zugang zu bestimmten Bereichen verbessert und es können Erstbearbeitungen von einfachen Rechtsproblemen geleistet werden, für die eine Anwältin oder ein Anwalt nicht konsultiert werden würden. Der Einsatz von KI hat somit eine Vergrößerung des gesamten Rechtsmarktes zur Folge. Für eine Vergrößerung des Rechtsmarktes auf andere Art sorgte hingegen Googles neuronales Sprachmodell „LaMDA", als sich dieses selbst einen Anwalt nehmen wollte, um sich als „Persönlichkeit" zu schützen (Googles umstrittene Lamda-KI soll sich einen Anwalt genommen haben, t3n – digital pioneers).

Es zeigt sich, welch immense Rolle KI in Unternehmen bereits spielt und in Zukunft spielen wird. Von den intelligenten Systemen gehen jedoch auch Risiken für die Grundrechte der EU-Bürger:innen aus: So sind Fälle bekannt, in denen KI-Anwendungen bei Jobeinstellungen oder Kreditvergabe auf Basis von ethnischer Zugehörigkeit, Geschlecht oder Alter diskriminierende Entscheidungen getroffen haben. Ein bekanntes Beispiel ist die Bewerbungs-KI von Amazon, die in ihrer Auswahl Frauen benachteiligte. Werden ungeeignete Daten für die Modellierung oder das Training verwendet, können insofern diskriminierende Annahmen verfestigt werden (Bias) (Bias in KI: Programmierte Vorurteile, Volkswagenstiftung). Haben Nutzer von KI-Anwendungen falsche Vorstellungen über den Aussagegehalt oder die Genauigkeit und Verlässlichkeit einer KI-gestützten Einschätzung, drohen unsachgemäße Entscheidungen. Auch für Privatsphäre und Datenschutz können Gefahren von KI ausgehen, beispielsweise durch Systeme zur massenhaften Echtzeit-Gesichtserkennung im öffentlichen Raum. Durch die großen Datenmengen, mit denen KI-Systeme oft arbeiten, besteht auch eine erhöhte Gefahr für Datenschutzvorfälle. Die Risiken, aber vor allem auch die Potenziale von KI hat auch die EU-Kommission erkannt und mit dem Vorschlag zur KI-VO darauf reagiert. Für Unternehmen, die sich die mannigfaltigen Vorteile von KI zunutze machen und machen wollen, ist eine Auseinandersetzung mit dem Entwurf schon jetzt unabdingbar.

3 Einführung in die KI-VO

Im Folgenden wird ein Überblick über den KI-VO-E gegeben. Dabei werden zunächst die Hintergründe zur Entstehung der Verordnung und das Gesetzgebungsverfahren beleuchtet. Im Anschluss wird dargestellt, für wen die Verordnung gelten soll. Daraufhin wird ein Einblick in die Regelungssystematik des Verordnungsentwurfs, den risikobasierten Ansatz, gegeben. Schließlich wird die Beziehung der geplanten KI-VO zum bestehenden Datenschutzrecht erläutert.

Um das eigene Unternehmen hinreichend auf die KI-VO vorzubereiten, ist es unausweichlich, sich mit der Verordnung vertraut zu machen.

3.1 Gründe und Ziele der KI-VO

Die Initiative der EU-Kommission geht zurück auf wiederholte Forderungen des EU-Parlaments und Ministerrats nach einem Regelungsrahmen für KI-Systeme. Der jetzige Verordnungsentwurf verdeutlicht den Anspruch der EU, bei der Entwicklung sicherer, vertrauenswürdiger und ethisch vertretbarer KI-Anwendungen weltweit eine Führungsrolle einzunehmen. Die Kommission hat erkannt, welche Vorteile der Einsatz von KI für Gesellschaft und Umwelt hat und welche Wettbewerbsvorteile sich für europäische Unternehmen ergeben. Im Umweltschutz können KI-Systeme beispielsweise helfen, Güterverkehr effizienter und damit klimaschonender zu gestalten oder Daten zur Häufigkeit und Verbreitung gefährdeter Tier- und Pflanzenarten auszuwerten (Fünf-Punkte-Programm „Künstliche Intelligenz für Umwelt und Klima“, Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit). Als Branchen, in denen sie KI-Systemen eine besonders große Bedeutung zumisst, nennt die Kommission deshalb exemplarisch Klimaschutz, Umwelt, Gesundheit, Finanzen, Mobilität, Landwirtschaft sowie den inneren und öffentlichen Sektor.

Die Kommission benennt für den angestrebten KI-Rechtsrahmen vier zentrale Ziele:

- Gewährleistung, dass die auf dem Unionsmarkt in Verkehr gebrachten und verwendeten KI-Systeme sicher sind und die Grundrechte und Werte der Union wahren
- Schaffung von Rechtssicherheit, um Investitionen in KI und deren Innovativität zu fördern
- Stärkung von Governance und Durchsetzungsmechanismen für geltendes Recht zur Wahrung der Grundrechte sowie der Sicherheitsanforderungen an KI-Systeme
- Erleichterung der Entwicklung eines Binnenmarktes für rechtskonforme, sichere und vertrauenswürdige KI-Anwendungen sowie Verhinderung von Marktfragmentierung

3.2 Aktuelles zum Gesetzgebungsverfahren

Derzeit befindet sich die KI-Verordnung im Entwurfsstadium. Nachdem die EU-Kommission den Vorschlag zur Verordnung im April 2021 vorgelegt hat, bereiten die EU-Gesetzgebungsorgane nun den offiziellen Trilog vor. Dafür befindet sich der Entwurfstext im EU-Parlament und im EU-Ministerrat in der Diskussion. Die Positionen der beiden Organe werden Gegenstand der offiziellen interinstitutionellen Verhandlungen sein. Der Ministerrat stellte unter tschechischem Ratsvorsitz **zuletzt** im **Oktober** 2022 **einen** vollständigen Kompromissvorschlag vor. Im Parlament haben am ersten Juni 2022 die Verhandlungen begonnen und Kompromisse werden entworfen; verschiedene Ausschüsse arbeiten derzeit noch an ihren Empfehlungen. Die Abstimmung im Plenum **war** für Oktober 2022 angesetzt, **wurde jedoch auf November 2022 verschoben**. Wann die Verordnung tatsächlich in Kraft treten wird, ist momentan nicht sicher abzusehen. Ein Inkrafttreten erscheint schon 2023 durchaus denkbar, wahrscheinlicher wird dies jedoch ab 2024 geschehen. Danach wird es für Unternehmen eine dreijährige Umsetzungsfrist bis zur tatsächlichen Anwendbarkeit der KI-Verordnung geben. Die Mitgliedstaaten haben binnen eines Jahres nationale notifizierende Behörden einzurichten, die für die Durchführung von Konformitätsverfahren zuständig sind.

Auch wenn sich die Verordnung derzeitig noch in der Diskussion befindet, sind die Regelungssystematik sowie die zentralen Anforderungen bereits jetzt ersichtlich. Es ist absehbar, dass der Anwendungsbereich, die Begriffsdefinition sowie die Zuschnitte der Sektoren, in denen KI als hochrisikoreich gelten soll, wichtige Diskussionspunkte im Trilog sein werden.

3.3 An wen richtet sich die KI-VO? – Anwendungsbereich der Verordnung

Nachfolgend wird der Geltungsbereich der kommenden KI-VO beschrieben. Der sachliche Anwendungsbereich regelt, welche Systeme als KI gelten und damit Regelungsgegenstand der Verordnung sein werden. Der persönliche Anwendungsbereich umfasst alle Akteure, für die die Verordnung Regelungen enthalten wird. Im räumlichen Anwendungsbereich wird die räumliche Geltung der KI-VO bestimmt. Den Anwendungsbereich der Verordnung zu kennen, ist deshalb von maßgeblicher Bedeutung, weil es gilt zu erkennen, ob das eigene Unternehmen von den regulatorischen Anforderungen betroffen sein wird.

3.3.1 Sachlicher Anwendungsbereich

Der KI-VO-E definiert den Begriff „System der künstlichen Intelligenz“ in Art. 3 Abs. 1 wie folgt:

> *Ein System, das so konzipiert ist, dass es mit einem bestimmten Grad an Autonomie arbeitet, und das auf der Grundlage von maschinellen und/oder menschlichen Daten und Eingaben mithilfe von maschinellem Lernen und/oder logik- und wissensbasierten Ansätzen ableitet, wie eine bestimmte Reihe von vom Menschen definierten Ziele erreicht werden kann, und das systemgenerierte Ergebnisse wie Inhalte (generative KI-Systeme), Vorhersagen, Empfehlungen oder Entscheidungen erzeugt, die die Umgebung beeinflussen, mit der das KI-System interagiert.*

Damit orientiert sich der KI-VO-E in seiner aktuellen Fassung an einem klassischeren Verständnis von KI-Systemen. Umfasst sind Kernmerkmale und -fähigkeiten wie eine autonome Funktionsweise, die Fähigkeit zu lernen und Techniken wie Machine Learning. Der Verordnungsentwurf folgt damit im Wesentlichen der KI-Definition der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) (Künstliche Intelligenz in der Gesellschaft, Organisation for Economic Co-operation and Development).

Die Definition ist noch nicht final und umstritten. Sie wurde in dieser Form erst im letzten Kompromissvorschlag vom EU-Ministerrat in den Verordnungstext aufgenommen. In dem ursprünglich vorgelegten Entwurf war die Definition für KI-Systeme noch wesentlich weiter angelegt.

So waren neben Machine Learning und logik- und wissensbasierten Ansätzen diverse weitere Techniken und Konzepte vorgesehen, deren Verwendung das Vorliegen von KI im Sinne der Verordnung zur Folge gehabt hätte. Diese waren in einem Anhang I aufgeführt; der Kommission sollte die Befugnis übertragen werden, die dortige Auflistung vor dem Hintergrund von technischen und Marktentwicklungen anzupassen.

Aufgrund der Bedenken von vielen Seiten, diese ursprüngliche Definition sei zu weit gefasst und beinhalte auch herkömmliche Softwaresysteme, sah sich der tschechische Ratsvorsitz im Sommer 2022 veranlasst, den KI-Begriff einzugrenzen. Das Resultat ist weniger zweideutig und sorgt für mehr Rechtssicherheit. Welche Definition sich in den kommenden Verhandlungen durchsetzen wird, bleibt dennoch abzuwarten. Angesichts der verbreiteten Forderung nach einem engeren KI-Begriff spricht vieles dafür, dass der Kompromissvorschlag des tschechischen Ratsvorsitzes beibehalten werden könnte.

3.3.2 Persönlicher Anwendungsbereich

Der persönliche Geltungsbereich der geplanten Verordnung ist sehr weit. Sie richtet sich an nahezu alle Akteure in der KI-Wertschöpfungskette. Insbesondere wird sie gem. Art. 2 KI-VO-E „Anbieter“ und „Nutzer“ von KI-Systemen adressieren. Beide Begriffe werden in Art. 3 KI-VO-E legaldefiniert:

> ***„Anbieter“*** *[ist] eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System entwickelt oder entwickeln lässt, um es unter ihrem eigenen Namen oder ihrer eigenen Marke – entgeltlich oder unentgeltlich – in Verkehr zu bringen oder in Betrieb zu nehmen.*

> ***„Nutzer"*** *[ist] eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet.*

Dadurch, dass Nutzer erfasst werden, wird der Anwendungsbereich stark erweitert und erstreckt sich auf zahlreiche Unternehmen, die – bewusst oder unbewusst – Softwarelösungen mit implementierten KI-Elementen einsetzen, zumal auch Nutzer unter Umständen Adressaten der Pflichten für Anbieter werden können (dazu ausführlicher in Kapitel IV). Darüber hinaus enthält die Verordnung Pflichten für „Einführer" und „Händler", also solche Akteure, die KI-Systeme aus dem Ausland in den europäischen Markt einführen oder die Systeme vertreiben.

3.3.3 Räumlicher Anwendungsbereich

Auch in räumlicher Hinsicht geht die KI-VO weit. So sollen alle Anbieter von KI verpflichtet werden, die Systeme auf dem EU-Markt bereitzustellen, unabhängig davon, ob sie in der EU niedergelassen sind oder in einem Drittland. Für Nutzer von KI-Systemen gilt die Verordnung dann, wenn sie in der EU niedergelassen oder „physisch anwesend" sind. Zudem richtet sich die KI-VO an Anbieter und Nutzer von KI, die zwar außerhalb der EU niedergelassen sind oder sich dort befinden, deren Systeme aber Ergebnisse hervorbringen, die in der Union verwendet werden. Zum Beispiel sollen Entwickler von KI-Systemen mit Sitz in den USA unter die Verordnung fallen, wenn sie diese Systeme Unternehmen in der EU zur Verwendung bereitstellen. Die KI-VO folgt damit dem Marktortprinzip aus der DSGVO, so soll eine Umgehung von EU-Recht verhindert werden.

3.4 Regelungssystematik der KI-VO – Risikobasierter Ansatz

Die KI-VO verfolgt einen risikobasierten Ansatz. Das heißt, je höher die Risiken, die von einem KI-System für die Grundrechte von EU-Bürger:innen oder andere sensible Rechtsgüter ausgehen, desto strenger die regulatorischen Anforderungen. Dort, wo keine Risiken gesehen werden, soll es im Gegenzug keine rechtlichen Belastungen geben. Die geplante Verordnung sieht vier Risikoklassen vor.

3.4.1 Verbotene KI-Praktiken

Zunächst führt die KI-VO eine Reihe von Praktiken auf, die im Bereich der künstlichen Intelligenz gänzlich verboten sein sollen. Grund dafür sind nicht hinnehmbare Risiken für die Grundrechte und Werte der Union. Dazu zählen die Entwicklung und Verwendung von KI-Systemen, die Personen manipulieren, sodass sie sich oder anderen Personen einen physischen oder psychischen Schaden zufügen können. Außerdem soll KI verboten sein, mittels derer die Schwäche oder Schutzbedürftigkeit gewisser (vulnerabler) Gruppen ausgenutzt wird und Personen in der Folge geschädigt werden können. Verboten werden zudem KI-Systeme, die zur Bewertung oder Klassifizierung der Vertrauenswürdigkeit von Personen benutzt werden sollen (Social-Scoring-Systeme). Zuletzt wird, bis auf wenige Ausnahmen, die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen durch Ermittlungsbehörden zum Zweck der Strafverfolgung untersagt. Diese Verbotsliste wird für die wenigsten Unternehmen eine praktische Bedeutung haben, da sie nur besonders kritische Systeme enthält. Im Unternehmensalltag werden diese gegenwärtig nicht eingesetzt.

3.4.2 Hochrisiko-KI

Anders sieht es bei Hochrisiko-KI aus. Hochrisiko-KI umfasst solche Systeme, von denen eine besonders hohe Gefahr für die Gesundheit und Sicherheit oder die Grundrechte von EU-Bürger:innen befürchtet wird. Sie stellen den Hauptregelungsgegenstand der KI-VO dar, der Großteil der Anforderungen aus der Verordnung bezieht sich auf diese Risikogruppe. Viele Unternehmen nutzen – möglicherweise unbewusst – bereits jetzt Anwendungen, die zukünftig als Hochrisiko-KI eingestuft sein werden.

Wann eine KI mit hohem Risiko vorliegt, ist in Artikel 6 und in den Anhängen II und III des KI-VO-E geregelt. Danach soll ein KI-System zum einen dann mit einem hohen Risiko behaftet sein, wenn es selbst oder als Sicherheitsbauteil eines anderen Produktes aufgrund bereits bestehender EU-Harmonisierungsvorschriften einer Konformitätsbewertung unterzogen werden muss (sog. „embedded AI“). Vereinfacht gesagt, handelt es sich hier um bestimmte KI-Anwendungen, die in physischen Produkten verbaut sind.

Ferner wird zum anderen dann von einer Hochrisiko-KI ausgegangen, wenn das

- *KI-System in bestimmten Bereichen eingesetzt wird (z. B. Verwaltung, Personalmanagement oder Strafverfolgung) und*
- *einem der in Anhang III abschließend aufgeführten konkreten KI-Systeme aus diesen Bereichen entspricht. (sog. „stand-alone AI“).*

Die Bandbreite der umfassten Systeme ist groß. So sind im für Unternehmen relevanten Bereich *„Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit“* solche KI-Systeme als hoch-risikobehaftet anzusehen, die bei der Einstellung oder Auswahl zukünftiger Angestellter eingesetzt wird. Zudem sind hiervon Systeme umfasst, die bei der Entscheidung über Beförderungen oder Kündigungen eines Arbeitsverhältnisses sowie zur Aufgabenzuweisung, Überwachung und Leistungsbewertung innerhalb von Beschäftigungsverhältnissen, verwendet werden sollen. Äußerst praxisrelevant ist außerdem der Bereich *„Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen.“* Wird KI beispielsweise für Kreditwürdigkeitsprüfungen oder bei der Entscheidung über den Abschluss von Verträgen eingesetzt, die den Zugang zu grundlegenden privaten und öffentlichen Diensten und Leistungen ermöglichen, kann dies zur Folge haben, dass es sich um Hochrisiko-KI handelt. Dabei ist derzeit insbesondere noch umstritten, ob dieser Sektor tatsächlich nur auf „grundlegende“ Dienste und Leistungen beschränkt wird oder ob auch Entscheidungen über die Zugänglichkeit und Inanspruchnahme von nicht-grundlegenden Diensten und Leistungen erfasst sein sollen. Welche Sektoren letztlich von der KI-VO umfasst sein werden und wie weit diese reichen werden, ist derzeit noch umstritten. Der weitere europäische Gesetzgebungsprozess bleibt also abzuwarten.

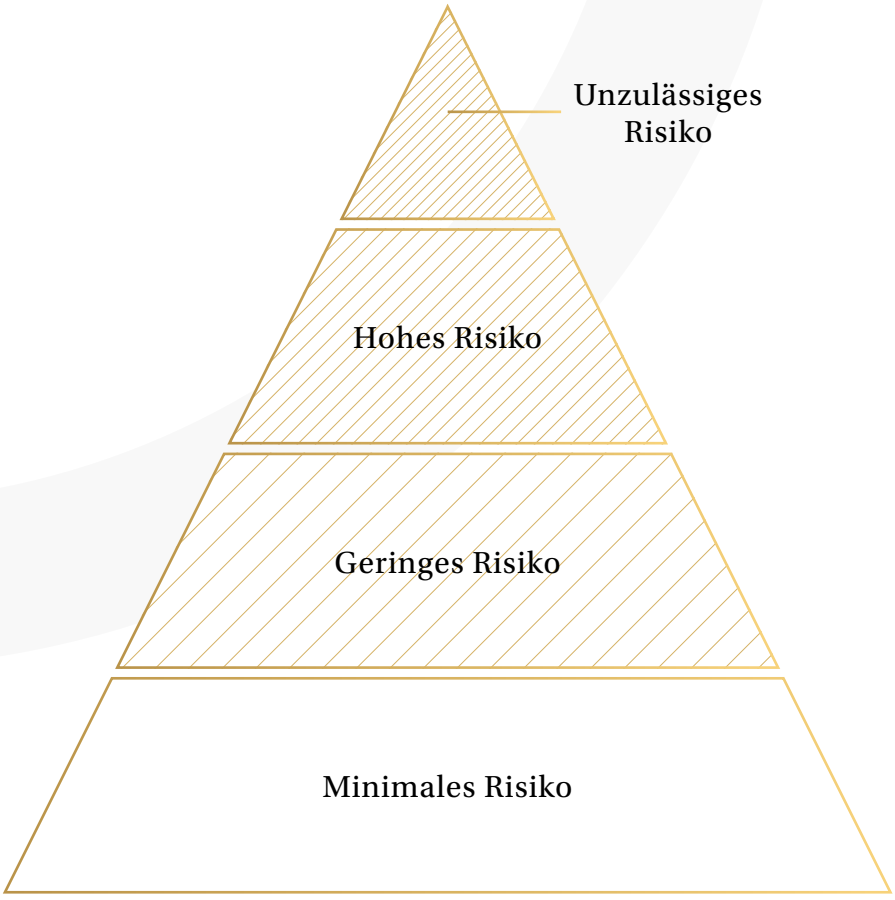
Bei der Einordnung, ob eine Hochrisiko-KI vorliegt, soll nach dem Ratsentwurf vom 15. Juli 2022 zudem entscheidend sein, ob Ergebnisse erzielt werden, die entweder gar nicht mehr von einem Menschen validiert werden oder welche die alleinige Grundlage für eine menschliche Entscheidung darstellen und daher zu einem erheblichen Risiko für die Gesundheit, die Sicherheit oder die Grundrechte führen können. Das Erfordernis, dass Hochrisiko-KI gewissermaßen eine menschliche Entscheidung ersetzen muss, wurde erst im aktuellen Ratsentwurf vom 15. Juli 2022 durch die tschechische Ratspräsidentschaft hinzugefügt, um den Begriff einzugrenzen. Zuvor hatte es genügt, wenn ein System unter die in Anhang III genannten Bereiche fiel.

Nach Art. 84 KI-VO-E soll die Europäische Kommission regelmäßig überprüfen, ob im Hinblick auf den technischen Fortschritt Änderungen an den in Anhang III aufgeführten KI-Systemen vorgenommen werden müssen. Umstritten ist jedoch noch, ob bzw. unter welchen genauen Voraussetzungen die Kommission die Möglichkeit haben soll, die Hochrisiko-Sektoren nach Inkrafttreten durch delegierte Rechtsakte anzupassen und zu ergänzen. Die aktuellen Entwürfe sehen entsprechende Befugnisse der Kommission vor, wobei die Kommission zuvor eine Risikobewertung nach festgelegten Kriterien durchlaufen soll.

3.4.3 Geringes und minimales Risiko

Ferner beschreibt der KI-VO-E Systeme mit geringem und mit minimalem Risiko. KI-Systeme mit geringem Risiko sind solche, die für die Interaktion mit Menschen bestimmt sind und nicht unter die Gruppe der verbotenen KI oder der Hochrisiko-KI fallen. Von solchen Algorithmen sollen potenziell lediglich gewisse Manipulationsrisiken ausgehen. Darunter fallen beispielsweise Chatbots, die den Anschein menschlicher Kommunikation erwecken können. Daher müssen Unternehmen, die derartige Systeme entwickeln oder verwenden, vor allem gewisse Transparenzpflichten erfüllen.

Als vierte Gruppe wird KI mit minimalem Risiko genannt. Umfasst sind Systeme, von denen keine expliziten Risiken ausgehen sollen. Für den Umgang mit diesen sieht der KI-VO-E dementsprechend auch keine besonderen Verpflichtungen vor. Die Kommission und die Mitgliedstaaten wollen jedoch gem. Art. 69 KI-VO-E fördern, dass Anbieter solcher KI-Systeme Verhaltenskodizes aufstellen.



3.5 Die KI-VO und die DSGVO

KI arbeitet in vielen Fällen mit enormen Datenmengen. Deshalb sind bei der Entwicklung, aber auch im Umgang mit KI-Systemen häufig datenschutzrechtliche Anforderungen zu beachten. Insbesondere im Rahmen des maschinellen Lernens (Machine Learning) werden KI-Algorithmen mit einer Vielzahl an Datensätzen trainiert. Beim Machine Learning lernt die Software autonom, indem sie auf Basis der Korrelation von alten und neuen Datenmustern, Arbeitsergebnisse produziert. Je nach Input und Anwendungsfeld kommt es dabei auch zur Verarbeitung von personenbezogenen Daten. In diesen Fällen sind daher die zahlreichen Vorgaben aus der DSGVO einzuhalten. Die KI-VO wird ebenfalls datenschutzrechtliche Reglungen enthalten. Die Ziele des Datenschutzes werden jedoch nicht den Fokus der Verordnung darstellen. Vielmehr soll bestehendes Datenschutzrecht von der Verordnung unberührt bleiben und durch diese ergänzt werden. Bei der Entwicklung und Nutzung von KI wird es also zu vielen Wechselwirkungen und gegebenenfalls zu „Doppelverpflichtungen“ aus den beiden Verordnungen kommen. Die beiden Regelungsmaterien liegen inhaltlich nah beieinander, zudem ähnelt sich die Natur der Verpflichtungen und Regelungsansätze aus KI-VO-E und DSGVO an vielen Stellen.

Es wird sich daher auf den umfangreichen Erfahrungsschatz aus dem Umgang mit der DSGVO und den in diesem Zusammenhang im Unternehmen etablierten Prozessen zurückgreifen lassen, wenn die KI-Verordnung umgesetzt wird. Auch wird es zu synergetischen Effekten kommen, die sich Unternehmen zunutze machen können, wenn sie KI entwickeln oder einsetzen.

4 Herausforderungen aus der KI-VO für Unternehmen

Die KI-VO wird einen umfangreichen Katalog von Anforderungen und Verpflichtungen enthalten, die sich vor allem an Anbieter von KI richten. Doch auch für Nutzer, Einführer und Händler enthält der Verordnungsentwurf Pflichten. Nach Art. 28 Abs. 1 KI-VO-E gelten auch diese Akteure als Anbieter für die Zwecke der Verordnung, wenn sie a) ein Hochrisiko-KI-System unter ihrem Namen auf den Markt bringen oder in Betrieb nehmen, b) die Zweckbestimmung eines sich bereits im Verkehr befindlichen KI-Systems ändern oder c) wesentliche Änderungen am KI-System vornehmen.

Da KI-Systeme, die in Unternehmen im Einsatz sind, oftmals auf deren Bedürfnisse maßgeschneidert sind, werden die nutzenden Unternehmen voraussichtlich in vielen Fällen selbst als Anbieter von KI gelten. Das bedeutet, dass für sie auch die umfangreichen Anbieterpflichten aus der KI-VO gelten werden.

Die Anforderungen und Pflichten beziehen sich fast ausschließlich auf Hochrisiko-KI. Soweit nicht anders beschrieben, knüpfen daher alle der in diesem Kapitel erläuterten Vorgaben an diese Risikogruppe an. Da der Begriff der Hochrisiko-KI voraussichtlich weit gefasst sein wird, wird ein Großteil der Unternehmen, die mit KI arbeiten, diese Anforderungen umsetzen müssen.

Insbesondere sind die nachfolgenden Maßnahmen vorgesehen:

Pflichten für Anbieter von Hochrisiko-KI	Pflichten für Nutzer von Hochrisiko-KI*
• Einhaltung aller Anforderungen aus Art. 8–15 KI-VO-E (Art. 16 lit. a KI-VO-E); Vornahme von Korrekturmaßnahmen, wenn die Anforderungen nicht erfüllt werden (Art. 16 lit. g KI-VO-E); gegenüber zuständiger nationaler Behörde muss dies stets nachgewiesen werden können (Art. 16 lit. j KI-VO-E) • Einrichten eines Qualitätsmanagementsystems nach Art. 17 KI-VO-E (Art. 16 lit. b KI-VO-E) • Aufbewahrung der nach Art. 12 KI-VO-E zu erstellenden Protokolle, wenn dies der Kontrolle des Anbieters unterliegt (Art. 16 lit. d KI-VO-E) • Durchführung eines Konformitätsbewertungsverfahrens nach Art. 19 KI-VO-E (Art. 16 lit. e KI-VO-E); Anbringung der CE-Kennzeichnung an KI-System nach Art. 49 KI-VO-E (Art. 16 lit. i KI-VO-E) • Registrierung des Systems in EU-Datenbank nach Art. 51 KI-VO-E (Art. 16 lit. f KI-VO-E) • Zusammenarbeit mit nationalen Behörden und notifizierten Stellen bei Nichtkonformität des Systems (Art. 16 lit. h KI-VO-E)	• Sorge tragen, dass Eingabedaten der Zweckbestimmung des KI-Systems entsprechen (Art. 29 Abs. 3 KI-VO-E) • Überwachen des Betriebes des KI-Systems entsprechend der Gebrauchsanweisung (Art. 29 Abs. 4 KI-VO-E) • Aufbewahrung der nach Art. 12 KI-VO-E zu erstellenden Protokolle, wenn dies der Kontrolle des Nutzers unterliegt (Art. 29 Abs. 5 KI-VO-E) • Verwendung der nach Art. 13 KI-VO-E bereitgestellter Informationen, um ggf. eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen

* Gem. Art. 28 KI-VO-E gelten Nutzer als Anbieter für die Zwecke der Verordnung, wenn sie ein KI-System unter ihrem Namen auf den Markt bringen oder in Betrieb nehmen, wenn sie die Zweckbestimmung eines sich bereits im Verkehr befindlichen KI-Systems ändern oder wenn sie wesentliche Änderungen am KI-System vornehmen. Das bedeutet, dass in diesen Fällen auch alle Anbieterpflichten für sie gelten.

4.1 Risikomanagementsysteme (Art. 9 KI-VO-E)

Wichtigster Regelungsaspekt der geplanten KI-VO ist die Mitigation von Risiken für Nutzer und betroffene Personen, also Menschen, die mit KI in Berührung kommen. So wird als erste Anforderung die Einrichtung, Anwendung, Dokumentation und Aufrechterhaltung von Risikomanagementsystemen genannt. Diese sollen als kontinuierlicher iterativer Prozess während des gesamten Lebenszyklus eines KI-Systems fortgeführt werden. Dazu gehören die Ermittlung und Analyse aller bekannten und vorhersehbaren Risiken, die von einer KI ausgehen. Ferner sollen die Risiken bewertet werden, die auftreten können, wenn das System gemäß seinem Zweck benutzt wird, oder die im Rahmen einer vorhersehbaren Fehlanwendung auftreten könnten. Außerdem müssen Anbieter gem. Art. 61 KI-VO-E auch ein System zur Beobachtung eines KI-Systems nach dessen Inverkehrbringen einrichten. Im Rahmen des Risikomanagements nach Art. 9 KI-VO-E sollen die daraus resultierenden Erkenntnisse ausgewertet und damit verbundene Risiken behandelt werden. Es sind zudem kontinuierlich geeignete Risikomanagementmaßnahmen zu ergreifen, die die verbleibenden Risiken auf ein vertretbares Maß reduzieren. Bei der Einordnung der Risiken bietet es sich an, unternehmensintern ein eigenes System zur Risikoklassifizierung einzuführen. Beispielsweise lassen sich Risikomatrizen nutzen, um Risikobeurteilungen vorzunehmen.

4.2 Daten und Data-Governance (Art. 10 KI-VO-E)

Werden für die Entwicklung des KI-Systems Daten verwendet, müssen diese die Anforderungen aus Art. 10 Abs. 3 und Abs. 4 KI-VO-E erfüllen. Dies gilt für alle Trainings-, Validierungs- und Testdaten – und zwar unabhängig davon, ob es sich bei den Daten um personenbezogene Daten handelt. Die Daten müssen insbesondere nachweisbar relevant, repräsentativ, fehlerfrei und vollständig sein (Art. 10 Abs. 3 S. 1 KI-VO-E). Durch die Erfüllung dieser Anforderungen soll eine hohe Datenqualität sichergestellt und das bestimmungsgemäße Funktionieren der KI-Anwendung gewährleistet werden. Zudem sollen auch Diskriminierungen durch die KI vermieden werden.

Darüber hinaus müssen für den Umgang mit den Daten für die KI-Anwendung Data-Governance und Datenverwaltungsverfahren eingeführt werden (Art. 10 Abs. 2 lit. a–e KI-VO-E). Diese sollen bereits bei der Konzeption von Datenverarbeitungen greifen und betreffen dann beispielsweise die Datenerfassung, die Untersuchung im Hinblick auf mögliche Verzerrungen und Vorurteile (Bias) oder die Ermittlung und Behebung möglicher Datenlücken und Mängel. Zu den Anforderungen gehört es ferner, die Beweggründe und Auswahlkriterien für Datenquellen darlegen zu können. Da sich diese Vorgaben auf die Frühphase der KI-Entwicklung beziehen – die Datenbeschaffung – und die Überlegungen im Nachhinein nicht mehr ohne Weiteres dokumentiert werden können, zeigt sich, dass die frühzeitige Beschäftigung mit den zukünftigen KI-Compliance-Pflichten und der Ausbau eines KI-Managementsystems schon vor der Anwendbarkeit der KI-VO notwendig sind.

4.3 Dokumentationspflichten (Art. 11 KI-VO-E)

Nach Art. 11 KI-VO-E werden Unternehmen, die KI-Systeme auf den Markt bringen oder nutzen, zur technischen Dokumentation verpflichtet. Diese soll vor allem gegenüber den Aufsichtsbehörden als Nachweis dienen, dass das KI-System die Anforderungen aus der KI-VO erfüllt. Im Anhang IV zum Verordnungsentwurf ist detailliert erklärt, welche Informationen die Dokumentation mindestens enthalten muss. Dazu gehören beispielsweise eine Beschreibung der Zweckbestimmung des Systems, der Methoden und der Schritte, die zu seiner Entwicklung genutzt wurden, sowie eine detaillierte Beschreibung des Risikomanagementsystems nach Art. 9 KI-VO-E. Die EU-Kommission soll gem. Art. 11 Abs. 3 KI-VO-E die Befugnis erhalten, die Vorgaben im Anhang IV in Anbetracht des technischen Fortschritts, anzupassen. Es gilt also, im Auge zu behalten, welche Änderungen die Kommission bezüglich der Anforderungen an die technische Dokumentation gegebenenfalls vornehmen wird.

4.4 Aufzeichnungspflichten (Art. 12 KI-VO-E)

Zudem sollen KI-Systeme so konzipiert und entwickelt werden, dass eine automatische Protokollierung der Vorgänge und Ereignisse während des Betriebs der KI-Systeme erfolgt (Logging). So soll die Funktionsfähigkeit der KI-Systeme über deren gesamten Lebenszyklus zurückverfolgt werden können. Die Aufzeichnungspflichten sollen die Beobachtung einer KI nach dem Inverkehrbringen erleichtern. Die Mindestanforderungen an die automatische Aufzeichnung werden in Art. 12 Abs. 4 KI-VO-E definiert.

4.5 Transparenz- und Instruktionspflichten (Art. 13 KI-VO-E)

Damit Nutzer von KI die erzeugten Ergebnisse angemessen interpretieren und verwenden können, sollen die Systeme so konzipiert und entwickelt werden, dass ihr Betrieb möglichst transparent ist. Dadurch soll vor allem gewährleistet werden, dass die Nutzer ihrerseits den Verpflichtungen aus der Verordnung nachkommen können. Zu diesem Zweck sollen KI-Systeme ferner mit digitalen Gebrauchsanweisungen versehen werden, die präzise, vollständige, korrekte und eindeutige Informationen für die Nutzer von KI enthalten. Die Transparenzanforderungen richten sich also anders als im Datenschutzrecht nicht an die von der KI betroffenen Personen (z. B. Verbraucher:innen), können aber gegebenenfalls auch für die Datenschutzinformationen genutzt werden. Jene Informationen müssen barrierefrei zugänglich und in verständlicher Form verfasst sein. Die konkreten Anforderungen an diese Instruktionen werden in Art. 13 Abs. 3 KI-VO-E genannt.

4.6 Menschliche Aufsicht (Art. 14 KI-VO-E)

KI-Systeme müssen nach Art. 14 KI-VO-E so konzipiert werden, dass sie während der gesamten Dauer ihrer Verwendung wirksam von Menschen beaufsichtigt werden können. Dadurch sollen Risiken für die Gesundheit, die Sicherheit oder die Grundrechte minimiert werden. Anbieter von KI sollen dafür schon vor deren Inverkehrbringen beziehungsweise vor der Inbetriebnahme die menschliche Aufsicht bestimmen und entweder in das KI-System einbauen oder so konzipieren, dass sie von den Nutzern ausgeübt werden kann. Insbesondere muss es den Nutzern ermöglicht werden, die Fähigkeiten und Grenzen eines KI-Systems vollständig zu verstehen und seinen Betrieb so zu überwachen, dass Anzeichen von Anomalien, Fehlfunktionen und unerwarteter Leistung schnellstmöglich erkannt und behoben werden können. Außerdem soll den Personen, welche die KI überwachen, bewusst gemacht werden, dass Menschen dazu neigen, übermäßiges Vertrauen in die Arbeitsergebnisse von KI zu stecken, die sogenannte Automatisierungsbias. Dieses Bewusstsein ist insbesondere dann wichtig, wenn KI-Systeme Informationen oder Empfehlungen herausgeben, auf deren Grundlage weitergehende Entscheidungen getroffen werden. Es muss der Person, die die menschliche Aufsicht innehat, zudem möglich sein, die Ergebnisse der KI richtig zu interpretieren und zu erkennen, wann ein KI-System nicht verwendet oder sein Ergebnis außer Acht gelassen werden sollte. Schließlich muss in den Betrieb einer KI eingegriffen werden können und es muss mittels einer „Stopptaste“ unterbrochen oder vollständig beendet werden können.

4.7 Genauigkeit, Robustheit und Cybersicherheit (Art. 15 KI-VO-E)

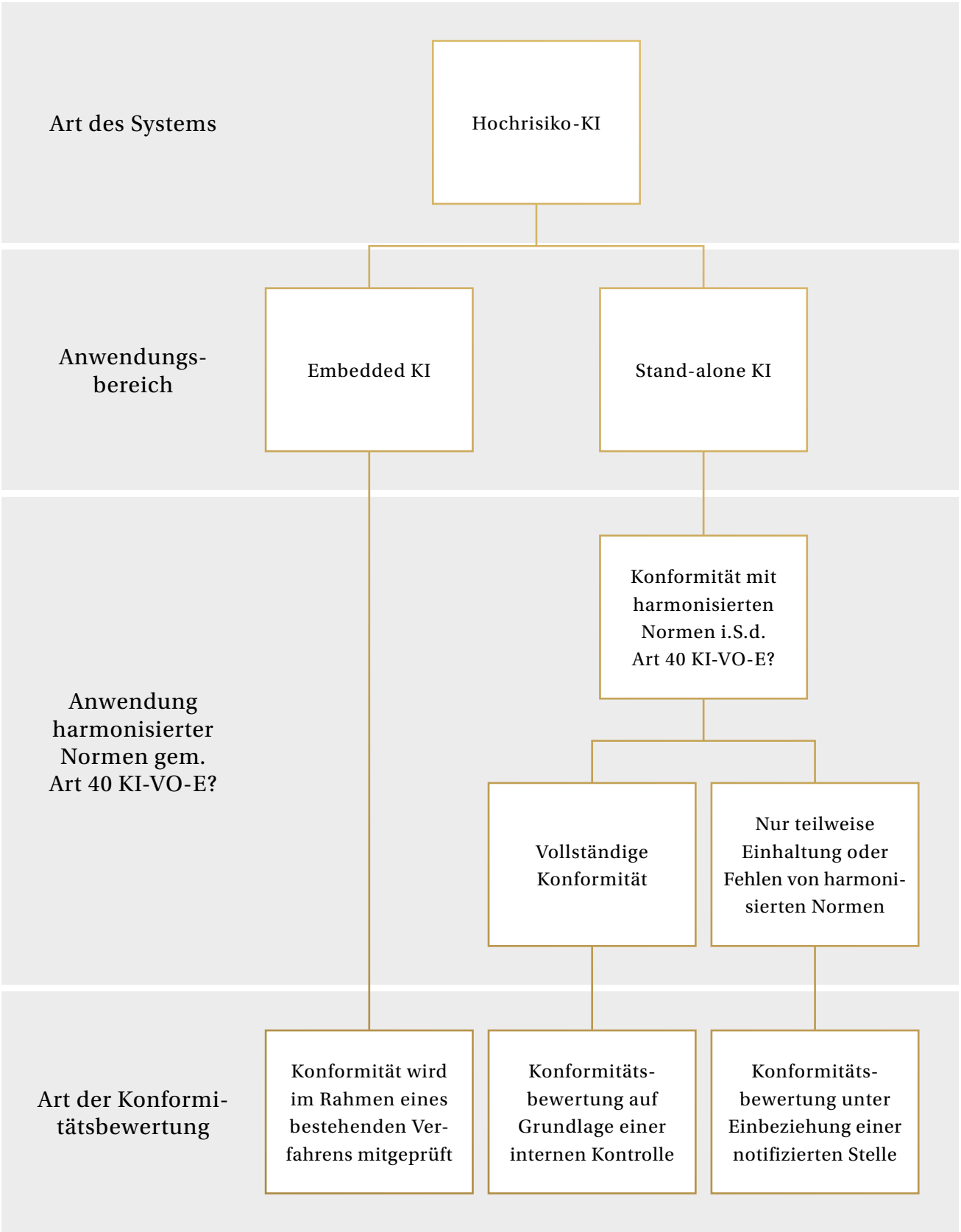
Bei der Konzeption und Entwicklung von KI-Systemen muss gem. Art. 15 KI-VO-E darauf geachtet werden, dass diese während ihres gesamten Lebenszyklus mit einem angemessenen Maß an Genauigkeit, Robustheit und Cybersicherheit funktionieren. Dadurch sollen KI-Systeme widerstandsfähig gegenüber Risiken aufgrund von systemimmanenten Grenzen sowie gegenüber schädlichen Eingriffen sein. Letztere können entweder KI-spezifische Ressourcen wie Trainingsdatensätze angreifen (z. B. für eine Datenvergiftung), Trainingsmodelle manipulieren oder Schwachstellen in den digitalen Ressourcen des KI-Systems oder der zugrunde liegenden IT-Infrastruktur ausnutzen. Um dagegen ein ausreichendes Maß an Cybersicherheit zu gewährleisten, müssen Anbieter von KI gem. Art. 15 IV KI-VO-E geeignete technische und organisatorische Maßnahmen ergreifen.

4.8 Qualitätsmanagementsystem (Art. 17 KI-VO-E)

Nach Art. 17 KI-VO-E werden Anbieter ein Qualitätsmanagementsystem einrichten müssen. Dieses soll systematisch und ordnungsgemäß in Form schriftlicher Regeln, Verfahren und Anweisungen dokumentiert werden. Es soll vor allem dazu dienen, die Einhaltung jeglicher anderen Anforderungen und Verpflichtungen aus der Verordnung zu gewährleisten. Die Aspekte, die mindestens umfasst sein müssen, werden in Art. 17 Abs. 1 lit. a–m KI-VO-E aufgeführt. Die Umsetzung dieser Verpflichtung soll in einem angemessenen Verhältnis zur Größe des jeweiligen Unternehmens stehen.

4.9 Konformitätsbewertungsverfahren (Art. 19 KI-VO-E)

Anbieter von KI-Systemen werden gem. Art. 19 KI-VO-E dazu verpflichtet, ihre Systeme einem Konformitätsbewertungsverfahren zu unterziehen, bevor sie auf den Markt gebracht oder verwendet werden. Im Rahmen der Konformitätsbewertung soll nachgewiesen werden, dass die jeweilige KI die Anforderungen aus Art. 8–15 KI-VO-E erfüllt. Infolge der Prüfung sollen die Anbieter für jedes KI-System eine EU-Konformitätserklärung ausstellen und dieses gem. Art. 49 KI-VO-E mit einer CE-Konformitätskennzeichnung versehen. Wenn eine KI Sicherheitsbestandteil eines Produktes ist (sog. embedded AI), das unter die in Anhang II Abschnitt A genannten EU-Harmonisierungsvorschriften fällt, und wenn diese Vorschriften ihrerseits ein Konformitätsbewertungsverfahren durch Dritte vorsehen, dann werden die Anforderungen aus der KI-VO im Rahmen dieses Verfahrens mitgeprüft. Dadurch soll der Verwaltungsaufwand gering gehalten und die Kohärenz zwischen der EU-Gesetzgebung in verschiedenen Sektoren gefördert werden. Handelt es sich dagegen um sogenannte „stand-alone" KI, mit der deshalb ein hohes Risiko assoziiert wird, weil sie einem der Bereiche aus Anhang III zuzuordnen ist, genügt in den meisten Fällen eine interne Prüfung. Lediglich für KI-Systeme, die zur biometrischen Identifizierung und Kategorisierung von Menschen genutzt werden, ist eine externe Konformitätsprüfung zwingend, sofern die KI-Anwendungen nicht andere harmonisierte EU-Vorschriften befolgen, die die Anforderungen der geplanten KI-VO mit abdecken.


Art des Systems
Hochrisiko-KI
Anwendungs-bereich
Embedded KI
Stand-alone KI
Anwendung harmonisierter Normen gem. Art 40 KI-VO-E?
Konformität mit harmonisierten Normen i.S.d. Art 40 KI-VO-E?
Vollständige Konformität
Nur teilweise Einhaltung oder Fehlen von harmonisierten Normen
Art der Konformitätsbewertung
Konformität wird im Rahmen eines bestehenden Verfahrens mitgeprüft
Konformitäts-bewertung auf Grundlage einer internen Kontrolle
Konformitäts-bewertung unter Einbeziehung einer notifizierten Stelle

4.10 Weitere Verpflichtungen für Hochrisiko-KI

Der Pflichtenkatalog der Verordnung enthält weitere Vorgaben für Hochrisiko-KI. Dazu zählen eine Aufbewahrungspflicht für die automatisch erzeugten Protokolle (Art. 20 KI-VO-E), die Pflicht, Korrekturmaßnahmen vorzunehmen, wenn eine KI nicht mehr den Anforderungen der Verordnung entspricht (Art. 21 KI-VO-E), die Plicht, die nationalen Behörden zu informieren, wenn ein KI-System ein Risiko auf nationaler Ebene birgt (Art. 22 KI-VO-E), und die grundsätzliche Pflicht zur Zusammenarbeit mit den zuständigen nationalen Behörden (Art. 23 KI-VO-E).

4.11 Transparenzpflichten für bestimmte KI-Systeme (Art. 52 KI-VO-E)

Für KI-Systeme, von denen ein geringes Risiko ausgeht, sieht der KI-VO-E lediglich Transparenzpflichten vor. So sollen die Anbieter solcher Systeme, die für die Interaktion mit Menschen bestimmt sind, sicherstellen, dass diese Personen darauf hingewiesen werden, dass sie mit einer KI interagieren. Zudem soll offengelegt werden, dass Ergebnisse, die von einer KI stammen, künstlich erzeugt wurden. Diese Pflichten gelten auch für Hochrisiko-KI-Systeme, sofern sie mit Menschen interagieren.

4.12 Freiwillige Verhaltenskodizes für Systeme ohne hohes Risiko (Art. 69 KI-VO-E)

Für KI-Systeme mit einem geringen oder minimalen Risiko werden die EU-Kommission und die Mitgliedstaaten das Aufstellen von freiwilligen Verhaltenskodizes fördern und erleichtern. Diese sollen dazu beitragen, dass auch KI-Anwendungen dieser Risikogruppen den Anforderungen aus der KI-VO entsprechen. Auch im Hinblick auf diese Systeme wird es sich also lohnen, KI verordnungskonform zu entwickeln und zu nutzen, um von den Anreizen der EU-Kommission und den Mitgliedstaaten zu profitieren. Einige Unternehmen haben derartige „Codes of Conduct“ schon unabhängig vom KI-VO-E eingeführt. Der Softwarekonzern SAP war in Europa 2019 das erste Unternehmen, das mit seinen „Leitlinien für den ethischen Umgang mit künstlicher Intelligenz“ einen solchen Schritt unternommen hat (SAP’s Guiding Principles for Artificial Intelligence). Zur Orientierung beim Aufstellen von

Verhaltenskodizes für vertrauenswürdige KI hat die hochrangige Expertengruppe für künstliche Intelligenz der EU-Kommission ihrerseits Guidelines herausgegeben (Ethics guidelines for trustworthy AI). Diese haben zwar nicht ausdrücklich die Anforderungen aus der geplanten KI-VO zum Gegenstand, sind aber an vielen Stellen deckungsgleich mit diesen.

4.13 Folgen von Verstößen (Art. 71 KI-VO-E)

Kommt es zu Verstößen gegen die kommenden Vorgaben der KI-VO, sind empfindliche Sanktionen vorgesehen. Der Bußgeldrahmen übersteigt sogar die nach der DSGVO möglichen Beträge. So drohen Untersagungsverfügungen sowie Bußgelder von bis zu 30 Millionen Euro oder 6 Prozent des gesamten weltweiten Jahresumsatzes, je nachdem welcher Betrag höher ist.

Zusammengefasst

Die kommende KI-Verordnung enthält eine Fülle von Anforderungen und Verpflichtungen. Auch wenn sich die Verordnung noch im Entwurfsstadium befindet, sind die zentralen Herausforderungen bereits absehbar. Es ist daher damit zu rechnen, dass das Pflichtenprogramm für Unternehmen, wie es im jetzigen Entwurf beschrieben ist, weitgehend zum Inhalt der Verordnung werden wird. Unternehmen sollten daher schon jetzt damit beginnen, die geplanten Vorgaben umzusetzen. Denn die Verordnung stellt eine Reihe komplexer Anforderungen auf. Darüber hinaus lassen sich einige Anforderungen aus der KI-VO im Nachhinein nicht oder nur mit einem erheblichen Aufwand an Zeit und Kosten umsetzen, so etwa die Dokumentationspflicht aus Art. 11 KI-VO-E.

5 Lösungsansätze und Synergien zum Datenschutzrecht

Unternehmen sollten bereits frühzeitig damit beginnen, den Herausforderungen aus der kommenden KI-VO zu begegnen. Nur so kann eine erfolgreiche Vorbereitung auf das Inkrafttreten der Verordnung gelingen.

In diesem Abschnitt wird dafür zunächst ein Überblick gegeben, was Unternehmen, die KI entwickeln oder nutzen, jetzt schon tun können. Im Anschluss wird erörtert, wie sich die Vorgaben aus dem KI-VO-E in bestehende, zum Teil bereits im Datenschutzrecht geforderte Prozesse integrieren lassen. Im Zusammenspiel mit dem Datenschutzrecht werden sich durch die KI-VO jedoch auch neue Herausforderungen ergeben. In diese wird im vorliegenden Kapitel ebenfalls ein Einblick gegeben.

5.1 Was Unternehmen jetzt schon tun sollten

Interdisziplinäres Team bilden: Zunächst gilt es, in allen Bereichen des eigenen Unternehmens die Sensibilität für KI und die davon ausgehenden Risiken zu stärken. Das Risikomanagement aus der KI-VO ist eine Neuheit, für die ein Bewusstsein geschaffen werden muss. Ferner sollten verantwortliche Personen bestimmt werden, die sich im Unternehmen mit der KI-VO-Compliance beschäftigen. Es empfiehlt sich, dafür ein Team aufzustellen, das sich aus Verantwortlichen aus verschiedenen Abteilungen zusammensetzt, schließlich wird sich die kommende KI-VO auf diverse Unternehmensbereiche auswirken. Insbesondere Stakeholder aus den Bereichen Recht und Datenmanagement sollten eingebunden werden.

KI-Assets identifizieren: Sodann ist zu bestimmen, ob der Entwurf zur KI-VO auf die eigene Software und sonstige Systeme Anwendung findet. So sollte identifiziert werden, wo und wie sich KI-Systeme im Unternehmen bereits in Benutzung befinden oder ob ihre Verwendung oder Entwicklung geplant ist. Dafür können Verzeichnisse erstellt werden, in denen alle KI-Systeme und ihre aktuelle oder geplante Verwendung aufgeführt sind.

Risikoklassifizierung vornehmen: Im Anschluss daran kann eine Risiko-Taxonomie entworfen werden, die mit den Risikoklassen des KI-VO-E übereinstimmt. Anhand dessen lassen sich die eingesetzten und entwickelten KI-Anwendungen den Risikogruppen zuordnen. Daraus lassen sich die korrespondierenden Anforderungen und Verpflichtungen aus der KI-VO schließen. Insbesondere wenn die Klassifizierung ergibt, dass im Unternehmen mit Hochrisiko-KI umgegangen wird, werden die umfangreichen Vorgaben der KI-VO einzuhalten sein.

Konformitätsbewertungsverfahren durchführen: Mit dem Beginn der Arbeit an oder mit einer KI-Anwendung sollte vor allem auch dem gegebenenfalls erforderlichen Konformitätsbewertungsverfahren Beachtung geschenkt werden. Je nachdem welche Art des Verfahrens eine KI durchlaufen muss, kann dieses als Anknüpfungspunkt zum effektiven Umgang und zur Minderung der mit KI verbundenen Risiken gesehen werden. Das Konformitätsbewertungsverfahren sollte vor allem auch deshalb nicht vernachlässigt werden, da es gegenüber den Aufsichtsbehörden als Nachweis dienen wird, dass die Anforderungen und Verpflichtungen der KI-VO eingehalten wurden.

5.2 Lösungsansätze bezüglich einzelner Anforderungen

Den vielfältigen Anforderungen aus der KI-VO wird sich unter Rückgriff auf bestehende Erfahrungssätze und Arbeitsweisen begegnen lassen. Dabei werden sich die konkreten Lösungsansätze zum Teil voraussichtlich in bestehende Compliance-Strukturen einbinden lassen. Für einen erfolgreichen Umgang mit der geplanten KI-Verordnung gilt es, diese Synergien zu erkennen und zu nutzen.

5.2.1 Bestehende Prozesse nutzen

In erster Linie wird es sich anbieten, die Compliance mit der geplanten KI-VO in bestehende datenschutzrechtliche Abläufe und Dokumente einzubinden. Für einige Anforderungen aus der KI-VO ist es zum Beispiel denkbar, sie im bereits bestehenden Verzeichnis von Verarbeitungstätigkeiten (VVT) umzusetzen.

So lässt sich das Risikomanagementsystem, das nach Art. 9 KI-VO-E erforderlich ist, daran anknüpfen. Im VVT wäre dann ein Unterpunkt „Technische Dokumentation nach Art. 11 KI-VO“ einzuführen. Anhang IV zum KI-VO-E bestimmt die Mindestanforderungen an die technische Dokumentation nach Art. 11. So soll unter anderem eine detaillierte Beschreibung des Risikomanagementsystems enthalten sein. Diese Anforderung ist daher der Anknüpfungspunkt, die technische Dokumentation und damit eingeschlossen das Risikomanagementsystem im VVT festzuhalten. Im Rahmen dessen ist beispielsweise aufzuführen, wer als verantwortliche Person für das Risikomanagement bestimmt wurde. Außerdem ist eine Risikoanalyse bezüglich aller Hochrisiko-KI-Systeme, die sich im Unternehmen in Benutzung oder Entwicklung befinden, vorzunehmen. Im Zuge dessen ist detailliert zu bestimmen und festzuhalten, welche konkreten Maßnahmen getroffen werden, um den ermittelten Risiken zu begegnen, um sie auf ein vertretbares Maß zu reduzieren.

Wie bereits erläutert, kann als Unterpunkt auch die technische Dokumentation nach Art. 11 KI-VO im VVT ergänzt werden. Wichtig ist, dass die technische Dokumentation auch schon vor Inverkehrbringen oder Inbetriebnahme der KI erfolgt. Im VVT sind dann die, in Anhang IV dezidiert genannten Anforderungen an die technische Dokumentation umzusetzen.

Auch im Datenschutzrecht dient das VVT vor allem dazu, risikobehaftete Datenverarbeitungsvorgänge zu identifizieren. Diese werden dann im Rahmen einer sogenannten Datenschutz-Folgeabschätzung (DSFA) gem. Art. 35 DSGVO einer genaueren Analyse unterzogen. Die Methodiken der DSFA werden sich in weiten Teilen auch auf die Risikoanalyse nach Art. 9 KI-VO-E übertragen lassen. Unterschied ist jedoch, dass die DSGVO klar definiert, dass die DSFA dem Schutz der Rechte und Freiheiten natürlicher Personen dienen soll. In dieser Klarheit wird im KI-VO-E nicht bestimmt, welche Art von Risiken durch das Risikomanagementsystem gemindert werden soll. Aus der Begründung zum Entwurf geht jedoch hervor, dass auch durch die KI-VO Risiken insbesondere von Einzelpersonen und deren Rechte abgewendet werden sollen. Die Zentrierung auf das Individuum zeigt auch Art. 9 Abs. 8 KI-VO-E, der bestimmt, dass beim Einrichten des Risikomanagementsystems insbesondere zu berücksichtigen ist, ob ein Hochrisiko-KI-System für Kinder zugänglich sein wird, deren besonderer Schutz garantiert werden soll.

Synergien können sich auch hinsichtlich der Anforderungen ergeben, die der KI-VO-E in Art. 10 an den Einsatz von Daten zu Trainingszwecken stellt. Diese Daten können in den gegebenenfalls schon bestehenden Datenkatalog aufgenommen werden. In einem Begleitdokument ist dann die Einhaltung der KI-VO-Vorgaben zu dokumentieren. In einem Unterpunkt „Nutzung“ lässt sich festhalten, wie die Anforderungen an Daten-Governance und Datenverwaltungsverfahren umgesetzt werden. In einem weiteren Unterpunkt „Daten“ kann die Einhaltung der Bestimmungen bezüglich der verwendeten Daten schriftlich festgehalten werden.

5.2.2 Zur Produktivsetzung von KI

Zusätzlich zu bereits bestehenden Dokumentationen empfiehlt sich ein weiteres Dokument, in dem skizziert und festgehalten wird, wie die anderen Anforderungen aus dem KI-VO-E eingehalten werden. Dieses sollte schon während der Entwicklung einer KI-Anwendung, aber spätestens vor ihrer Vermarktung oder Verwendung, der „Produktivsetzung", erfolgen. Das Dokument bietet einen Überblick, wie die KI-VO-Anforderungen umgesetzt wurden, und erleichtert eine spätere Nachverfolgung. Hier ist aufzuführen, ob die verpflichtende technische Dokumentation stets durchgeführt wurde, ob die Hochrisiko-KI so konzipiert wurde, dass die automatische Protokollierung nach Art. 12 KI-VO-E erfolgt, und wie gewährleistet wird, dass diese für den gesamten Lebenszyklus einer KI in Einklang mit den Vorgaben aus der KI-VO ist.

Auch sollte das Dokument zur Produktivsetzung der Hochrisiko-KI beinhalten, inwiefern bei der Konzeption und Entwicklung der KI die Transparenz- und Instruktionspflichten gegenüber Nutzern aus Art. 13 KI-VO-E beachtet wurden.

Ferner ist schon hier zu darzustellen, wie die Anforderungen bezüglich der menschlichen Aufsicht aus Art. 14 KI-VO-E realisiert wurden. So zum Beispiel, wer die verantwortliche Person für die menschliche Aufsicht ist und welche Vorkehrungen implementiert wurden, um diese Aufgabe umzusetzen.

5.3 KI und datenschutzrechtliche Anforderungen

Aus der inhaltlichen Nähe der KI-Verordnung zum Datenschutzrecht werden sich nicht lediglich Synergien ergeben. Durch die parallele Geltung der KI-VO mit der DSGVO kommt es zu Doppelverpflichtungen. So erfordern einige Direktiven und Verpflichtungen aus dem KI-VO-E die Verarbeitung von Daten. Dazu gehören etwa die Überprüfung von Trainingsdaten auf die in Art. 10 Abs. 3 KI-VO-E genannten Qualitätskriterien oder Fälle, in denen Daten im Rahmen der Aufzeichnungspflichten aus Art. 12 KI-VO-E gespeichert werden. Es sind dann stets die Grundsätze des Datenschutzes aus der DSGVO zu beachten und freilich bedarf es für die Verarbeitung von Daten durch KI einer Rechtsgrundlage. Die EU-Kommission hat in Erwägungsgrund 41 ausdrücklich klargestellt, dass die KI-VO selbst keine solche Rechtsgrundlage darstellt. Es muss daher immer eine andere Rechtsgrundlage gefunden werden, in Betracht kommen beispielsweise eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO oder ein berechtigtes Interesse nach 6 Abs. 1 lit. f DSGVO.

Um die datenschutzrechtlichen Risiken und damit die Anforderungen im Zusammenhang mit KI zu reduzieren, empfiehlt es sich, die verwendeten Daten soweit möglich zu pseudonymisieren oder zu anonymisieren. Zudem bietet sich in vielen Fällen die Verwendung von synthetischen Daten an. Dies sind keine echten Daten, sondern sie werden künstlich generiert. Der Informationswert synthetischer Daten ist auf Basis echter Datensätze simuliert. Somit sind sie nicht gänzlich frei erfunden, sondern haben den Anschein und Wert von authentischen, hochqualitativen Daten, sind aber grundsätzlich keine personenbezogenen Daten i. S. v. Art. 4 Nr. 1 DSGVO. Denkbar ist schließlich die Verwendung von speziellen Testdatensätzen (vgl. dazu etwa Amazon Mechanical Turk).

Eine weitere datenschutzrechtliche Herausforderung, die sich nicht aus der KI-VO selbst, sondern aus dem Umgang mit KI an sich ergibt, sind die besonderen Informationspflichten aus Art. 13 Abs. 2 lit. f DSGVO für die Direkterhebung sowie Art. 14 Abs. 2 lit. g DSGVO für die Dritterhebung. Betroffene müssen danach darüber informiert werden, ob eine automatisierte Entscheidungsfindung nach Art. 22 DSGVO einschließlich Profiling vorliegt. Ist dies bei der eingesetzten KI der Fall, sind die Betroffenen über die involvierte Logik sowie Tragweite und die angestrebten Auswirkungen der Datenverarbeitung zu informieren. Dabei müssen Informationen zur Funktionsweise der KI, zu den Grundannahmen des dahinterstehenden Algorithmus und zum Gegenstand der Entscheidung bereitgestellt werden. Auf welche Weise dies geschehen kann und wie sich die eingesetzte KI den Betroffenen hinreichend erklären lässt, wird in der Praxis eine große Herausforderung darstellen. Komplexe rechtliche und technische Erläuterungstexte allein schaffen nicht immer Transparenz. Vielmehr muss eine vernünftige Balance zwischen Genauigkeit und Verständlichkeit der Erklärung gefunden werden. Erforderlich ist ein kontextspezifisches, auf den Empfänger zugeschnittenes Informationskonzept. In gewisser Weise korrespondieren die Transparenzpflichten aus der DSGVO jedoch mit denen aus dem KI-VO-E. Im Rahmen der Pflicht aus Art. 13 KI-VO-E ist die Funktionsweise einer KI gegenüber dem Nutzer zu schildern. Diese Informationen werden sich auch für Betroffene nach der DSGVO aufbereiten lassen.

Zusammengefasst

Ein Teil der Vorgaben der KI-VO lässt sich gut umsetzen, indem auf bereits etablierte Compliance-Prozesse rekurriert wird. Und auch dort, wo neue Prozesse ins Leben gerufen werden müssen, sind die Herausforderungen aus dem KI-VO-E mit ausreichend Vorbereitung und Expertise gut zu meistern. Arbeiten KI-Systeme dabei mit Daten, sind stets zugleich die Anforderungen aus der DSGVO zu berücksichtigen.

6 Fazit

Die KI-VO wird aller Voraussicht nach sehr bald verabschiedet werden und sie wird vielfältige Herausforderungen mit sich bringen. Von diesen werden zahlreiche KI-Systeme betroffen sein, denn entgegen dem Wortlaut „Hochrisiko“-KI wird der Begriff in der KI-VO voraussichtlich weit definiert sein. Unternehmen sollten sich daher frühzeitig mit den zu erwartenden Anforderungen aus der KI-VO auseinandersetzen und sich auf ein Inkrafttreten der Verordnung vorbereiten. Dabei gilt es zunächst, sich mit dem Entwurf zur KI-VO vertraut zu machen und zu erkennen, ob eigene Systeme vom Anwendungsbereich umfasst sein werden. Anschließend sollte erörtert werden, welche konkreten Maßnahmen zur Umsetzung der Anforderungen bereits getroffen werden können. Die Erfahrungen rund um das Inkrafttreten der DSGVO zeigen, dass eine zu späte Vorbereitung auf bevorstehende Regelungen zu einem erheblichen Aufwand an Zeit und Kosten führen kann. Dies wird auch in Bezug auf die KI-VO gelten. Bereiten sich Unternehmen jedoch bereits frühzeitig sorgfältig auf die KI-VO vor, wird die rechtskonforme Entwicklung und Nutzung von KI-Systemen gut gelingen können. Wird dabei aus Erfahrungen mit der Umsetzung der datenschutzrechtlichen Anforderungen geschöpft und werden Synergie-Effekte genutzt, kann der Umsetzungsaufwand nicht unerheblich reduziert werden.

Die Umsetzung der KI-Verordnung erfordert ein interdisziplinäres Team, insbesondere mit juristischer Fachexpertise im Bereich des Technologierechts. Spezifische branchen- und bereichsspezifische Anforderungen sowie Problemstellungen erfordern einen großen Erfahrungsschatz sowie umfangreiches Praxiswissen – das macht das Heranziehen von spezialisierten Anwält:innen empfehlenswert.

7 Weitere rechtliche Herausforderungen – Exkurs ins Patent- und Urheberrecht

Die aufkeimende Bedeutung von KI bringt auch zahlreiche weitere rechtliche Herausforderungen mit sich. So werden im Zusammenhang mit KI-Systemen insbesondere urheberrechtliche Fragestellungen immer virulenter. Dabei geht es etwa um die Patentierbarkeit von KI-Anwendungen oder den urheberrechtlichen Schutz der Erzeugnisse einer KI. Der KI-VO-E hat derlei urheberrechtliche Problematiken nicht zum Gegenstand. Dennoch lohnt sich ein Exkurs in das Urheberrecht im Zeitalter der künstlichen Intelligenz.

KI-Anwendungen zu patentieren, liegt im Trend. Im Zeitraum von 2009 bis 2019 stieg die Zahl der Patentanmeldungen für KI in Deutschland um 80 Prozent (KI und IP – ein Überblick, Bundesverband Deutscher Patentanwälte). Und dies, obwohl KI in Deutschland und der EU nur sehr eingeschränkt patentierbar ist. Denn die Algorithmen stellen Software dar, das heißt sogenannte computerimplementierte Verfahren. Diese sind als solche jedoch nicht patentierfähig. Damit eine KI patentiert werden kann, muss sie vielmehr einen Beitrag zur Lösung eines konkreten technischen Problems mit technischen Mitteln darstellen. Ein besonders wichtiges Anwendungsbeispiel sind KI-Lösungen zum autonomen Fahren (Künstliche Intelligenz und Schutzrechte, Deutsches Patent- und Markenamt).

Daneben können KI-Anwendungen urheberrechtlichen Schutz genießen. Schließlich stellen sie Computerprogramme dar; diese gehören als Sprachwerke gem. §§ 2 Abs. 1 Nr. 1, 69a UrhG zu den urheberrechtlich geschützten Werken. Es muss allerdings genau differenziert werden: Nicht unter den Schutz fallen abstrakte Algorithmen, die nicht für ein spezielles Computerprogramm entwickelt wurden, sondern Basis eines jeden Computerprogramms sind. Denn geschützt wird die konkrete Quellcode-Gestaltung als „kreative“ Leistung einer Programmiererin oder eines Programmierers als konkreter Ausdruck eines Werkes (Künstliche Intelligenz und Machine Learning – Eine urheberrechtliche Betrachtung, Ausarbeitung vom Wissenschaftlichen Dienst des Bundestages, S. 17).

Darüber hinaus stellt sich die Frage, inwieweit die Erzeugnisse eines KI-Systems ihrerseits urheberrechtlich geschützt sein können. Ein eindrucksvolles Beispiel ist das Kunstprojekt „The Next Rembrandt“. Eine KI-Anwendung wurde dazu mit 346 Gemälden Rembrandts trainiert, die „Handschrift“, den charakteristischen Stil des niederländischen Künstlers zu analysieren und dann auf Basis der Bilddaten ein gänzlich neues „Rembrandt“-Gemälde zu erschaffen. Das Ergebnis, das Porträt eines Mannes mit Hut und Kragen, sieht den Vorbildern des Barockmalers täuschend ähnlich (Ein echter Rembrandt – aus dem Rechner, sueddeutsche.de). Fraglich ist, ob ein solches Werk überhaupt urheberrechtlich schutzfähig ist und wenn ja, wer als Urheber gilt. Grundvoraussetzung des urheberrechtlichen Schutzes ist die persönliche geistige Schöpfung. Erzeugnisse einer KI unterliegen daher nur dann einem urheberrechtlichen Schutz, wenn sie auf einen menschlich-geistigen Schöpfungsakt zurückgeführt werden können (Künstliche Intelligenz und Machine Learning – Eine urheberrechtliche Betrachtung, Ausarbeitung vom Wissenschaftlichen Dienst des Bundestages, S. 18). Ob dies der Fall ist, hängt davon ab, ob die KI eher als technisches Hilfsmittel eines Menschen einzuordnen ist oder ob die wesentliche Gestaltung und Entscheidung der KI obliegt, sie also als „Schöpfer“ anzusehen ist. Im ersten Szenario kann auch das mittels KI erzeugte Werk urheberrechtlich geschützt sein; als Urheber gilt dann die Person, die die KI entwickelt hat. Im zweiten Fall ist das Erzeugnis nicht als Werk i. S. d. § 2 UrhG zu sehen, da es an einer persönlichen geistigen Schöpfung eines Menschen fehlt. In der Konsequenz ist das von der KI erzeugte Ergebnis nicht schutzfähig und die programmierende Person gilt nicht als Urheber des Werkes (*Scheufen,* Die Bedeutung des Urheberrechts im Zeitalter Künstlicher Intelligenz, Institut der deutschen Wirtschaft, IW-Kurzbericht). Ein nicht urheberrechtlich geschütztes KI-Erzeugnis liegt also dann vor, wenn kein Mensch eine Gestaltungsmöglichkeit an dem entstandenen Werk hatte, sondern die KI die Gestaltungsentscheidungen automatisiert übernommen hat, so etwa bei Texten, die vollständig von einem Übersetzungscomputer hergestellt wurden (*Ahlberg,* BeckOk Urheberrecht, § 2 Rn. 55).

Die für das Training von KI-Systemen relevanten Datenmengen werden unter anderem durch sogenanntes Text- und Data-Mining gewonnen. In diesem Zusammenhang bestand lange Unsicherheit darüber, ob und inwiefern diese Art der Datenbeschaffung Urheberrechte verletzten könnte.

Einen einheitlichen Rechtsrahmen für Text und Data Mining innerhalb der Europäischen Union bildet nun Art. 4 der Richtlinie über das Urheberrecht im digitalen Binnenmarkt (Richtlinie (EU) 2019/790), „DSM-RL“). Mit dieser Regelung soll Rechtssicherheit bzgl. der urheberrechtlichen Relevanz und Zulässigkeit des Minings geschaffen werden, damit das wirtschaftliche Potential von Text- und Data-Mining voll ausgeschöpft werden kann. In Deutschland wurde Art. 4 der DSM-RL mit der Einführung des § 44b UrhG umgesetzt.

§ 44b Abs. 1 UrhG wird Text und Data Mining zunächst wie folgt definiert:

> *Text und Data Mining ist die automatisierte Analyse von einzelnen oder mehreren digitalen oder digitalisierten Werken, um daraus Informationen insbesondere über Muster, Trends und Korrelationen zu gewinnen.*

Die Analyse von Inhalten und Informationen an sich ist zunächst nicht urheberrechtsrelevant. Doch in den meisten Fällen werden die Informationen für die Analysezwecke in einer bestimmten Form aufbereitet und in diesem Zusammenhang vervielfältigt, was wiederum grundsätzlich eine urheberrechtsrelevante Handlung darstellt, vgl. § 16 UrhG. § 44b Abs. 2 S. 1 UrhG erlaubt nun die Vervielfältigung von rechtmäßig zugänglichen Werken für das Text- und Data-Mining; unabhängig davon, zu welchen Zwecken das Mining erfolgt. Vervielfältigungen für Text und Data Mining für Zwecke der wissenschaftlichen Forschung waren bereits vor der Einführung des § 44b UrhG gem. § 60d UrhG zulässig.

Umfasst werden auch solche Werke, die zunächst in analoger Form vorlagen und zum Zwecke des Minings digitalisiert wurden.

Werke sind dann rechtmäßig zugänglich, wenn sie etwa auf öffentlichen Websites zugänglich sind oder der Nutzer über eine Lizenz verfügt. Werke dürfen hingegen nicht für das Text- und Data-Mining vervielfältigt werden, wenn der Rechtsinhaber sich diese Nutzung vorbehalten hat. Für online zugängliche Werke muss der Nutzungsvorbehalt in maschinenlesbarer Form erfolgen. Bei analogen Werken muss der Nutzungsvorbehalt ausdrücklich erklärt werden.

Gem. § 44b Abs. 2 S. 2 sind die Vervielfältigungen zu löschen, wenn sie für das Text und Data Mining nicht mehr erforderlich sind. Wann genau die Erforderlichkeit entfällt, wird in § 44b Abs. 2 UrhG nicht näher definiert und bedarf im Zweifel einer unionsrechtskonformen Auslegung dahingehend, dass sich die Erforderlichkeit nach den mit dem Mining verfolgten Zwecken bemisst.

Auch wenn einzelne Auslegungsfragen verbleiben, schafft die Regelung einen angemessenen Rahmen für eine rechtssichere Anwendung von Text- und Data-Mining.

Rechtsanwälte für Digitales Business, Technologie & Medien

Unser Team aus hochspezialisierten Anwältinnen und Anwälten bietet Ihnen maßgeschneiderte juristische Strategien und eine effiziente Umsetzung Ihrer Innovationen. Sie lösen komplexe Fragestellungen im Bereich Technologie und Medien sowie Datenschutz und IT mit juristischem Know-how, technischem Verständnis, Exzellenz und Augenmaß.

Ihre Ansprechpartner

Kathrin Schürmann
Rechtsanwältin und Partnerin

Simone Rosenthal
Rechtsanwältin und Partnerin

Philipp Müller-Peltzer
Rechtsanwalt und Partner

Ilan Leonard Selz
Rechtsanwalt, LL.M. (Minnesota),
Senior Associate

Kontaktieren Sie uns!

SCHÜRMANN ROSENTHAL DREYER Rechtsanwälte
Am Hamburger Bahnhof 4, 10557 Berlin | +49 (0)30 21 30 028-0
office@srd-rechtsanwaelte.de | srd-rechtsanwaelte.de

SCHÜRMANN, ROSENTHAL, DREYER
Partnerschaft von Rechtsanwälten mbB

BERLIN
Am Hamburger Bahnhof 4
10557 Berlin

DÜSSELDORF
Uerdinger Straße 62
40474 Düsseldorf

MÜNCHEN
Elsenheimerstraße 59
80687 München

Weitere Informationen entnehmen Sie bitte unserem
Impressum unter srd-rechtsanwaelte.de/impressum