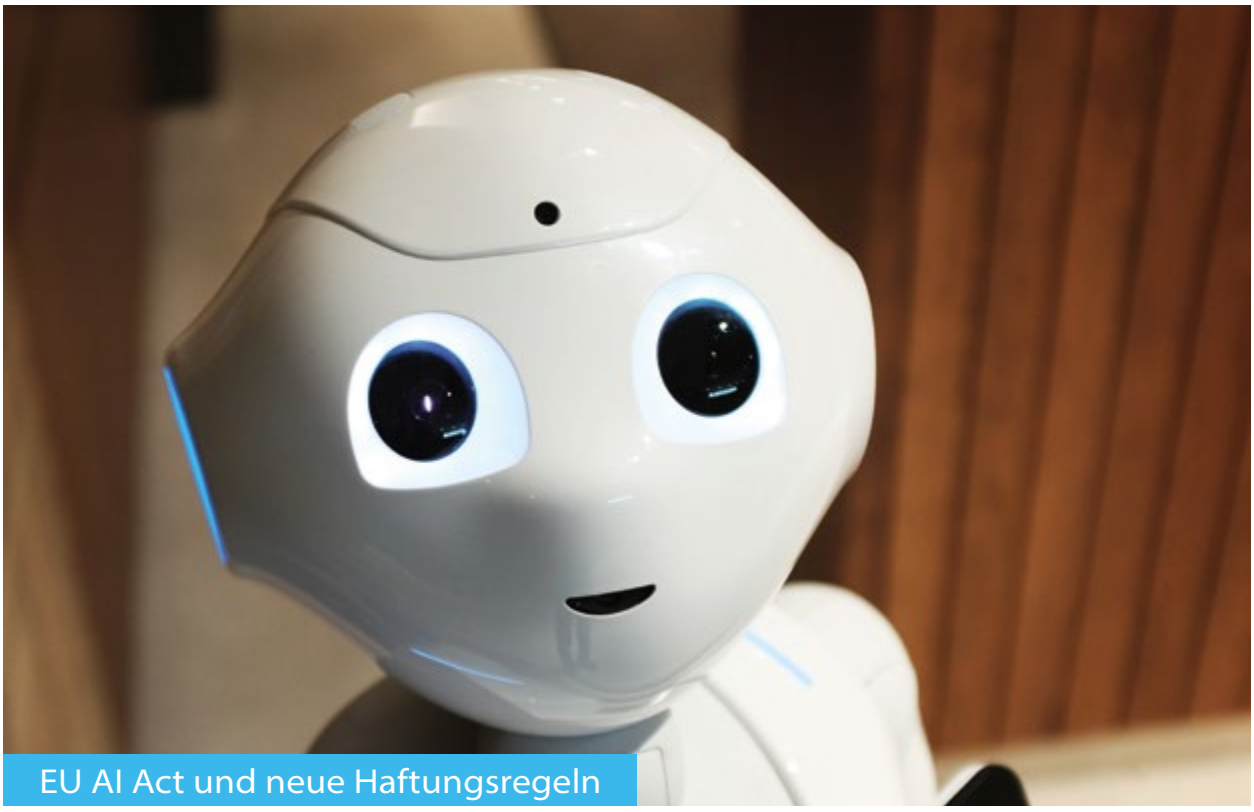

EU AI Act und neue Haftungsregeln

# KI und das wachsende Dickicht des Datenrechts

Brüssel plant ein Paket an Regulierungen, um Innovationen zu fördern: Angefangen bei Artificial Intelligence (AI) Act und einem neuen Haftungsregime für Künstliche Intelligenz bis zu Data Act und Data Governance Act. Entfalten die Neuregelungen die erhoffte Wirkung? Und was kommt auf Entwickler, Anbieter und Anwender zu?

► Nur neun Prozent der deutschen Unternehmen setzen laut einer aktuellen Umfrage des IT-Branchenverbands Bitkom Künstliche Intelligenz (KI) im Alltag ein. Zwar wird sie von rund 50 Prozent der Großunternehmen mit mehr als 2.000 Beschäftigten genutzt, aber kleine und mittlere Unternehmen (KMU) sind zögerlich. Vorbehalte gibt es bei Unternehmen jeder Größe: 79 Prozent sorgen sich wegen IT-Sicherheitsrisiken, 61 Prozent fürchten Verstöße gegen den Datenschutz. Mögliche Anwendungsfehler bei der KI-Nutzung schrecken 59 Prozent ab. Nicht nur Unternehmen, auch viele Menschen sind skeptisch, wenn KI über ihre Bewerbung oder einen Kredit entscheidet oder die Wahrscheinlichkeit eines Rückfalls von Straftätern beurteilt. Mit der Verordnung über Künstliche Intelligenz (EU AI Act) will die Europäische Kommission Abhilfe schaffen und Innovationen mehr Schubkraft verleihen. Der Entwurf sieht drei Stufen vor, um KI zu bewerten: Ist das Risiko einer Anwendung für die Gesundheit, Sicherheit und Grundrechte von Menschen gering, hoch oder unannehmbar? Grundsätzlich verboten bleiben in der EU zivile Anwendungen mit einem unannehmbaren Risiko wie Social-Scoring-Systeme, welche die Bevölkerung kontrollieren und mit Punkten für Wohlverhalten bewerten. Für KI mit hohem Risiko etwa im Gesundheitswesen, Verkehr oder Personalmanagement gelten künftig strenge Pflichten sowohl für Anbieter, die KI-Systeme entwickeln oder in Verkehr bringen, als auch Nutzer wie eine Bank, die maschinell lernende Software für das Recruiting einsetzt. Sofern ein KI-System nur ein geringes Risiko darstellt, wird es kaum

„Wenn externe Sachverständige die Risiko-Bewertungen vornehmen, kann das sehr teuer werden. Bei Selbstbewertungen stellt sich die Frage nach adäquaten Kontroll- und Prüfinfrastrukturen beziehungsweise dem Aufbau von Qualitätsmanagementsystemen."

**Nicole Formica-Schiller, KI Bundesverband, CEO und Gründerin der Pamanicor Health AG**

„Für Hochrisiko-KI-Systeme sind die Anforderungen sehr weitreichend. Bevor die KI auf den Markt kommt, bedarf es einer Konformitätsprüfung sowie CE-Zertifizierung."

**Dr. Stefan Dittmer, Partner bei der Wirtschaftskanzlei Dentons in Berlin und Experte für IT-Recht und Digitalisierung**

Regularien unterworfen. Den risikobasierten Ansatz halten viele Wirtschaftsvertreter im Grundsatz für richtig. Kritik gibt es aber an der Definition, was als KI gilt: „Bislang wurde gemäß dem Regulierungsvorschlag mehr oder weniger jegliche Software erfasst, die statistische Verfahren oder Such- und Optimierungsverfahren einsetzt, und damit fast jede bestehende und künftige Software", sagt Nicole Formica-Schiller vom KI Bundesverband, CEO und Gründerin der Pamanicor Health AG, einer globalen Beratungsfirma für KI- und Blockchain-Anwendungen. Stattdessen sei es sinnvoller, sich an der OECD-Definition für KI zu orientieren, so Formica-Schiller, die auch die OECD zu Artificial Intelligence berät. Der Europäische Rat hat die Bedenken vieler Mitgliedstaaten aufgegriffen und schlägt nun vor, die Definition von KI auf Systeme zu beschränken, die auf maschinellen Lerntechniken sowie logik- und wissensgestützten Ansätzen basieren.

**Strenge Pflichten für Hochrisiko-Anwendungen**

Je nach Risikoklasse gelten unterschiedlich strenge Zulassungsregeln und Kontrollen, erklärt Dr. Stefan Dittmer, Partner bei der Wirtschaftskanzlei Dentons in Berlin, der Unternehmen zu Fragen der Digitalisierung berät: „Sehr weitereichend sind die Anforderungen an Hochrisiko-KI-Systeme: Das fängt an bei einem Risiko-Managementsystem über die gesamte Lebensdauer der KI, geht weiter mit Transparenzanforderungen und Bereitstellung von Informationen für Nutzer und reicht bis zu Vorgaben für die technische Dokumentation und Aufzeichnung von Ereignissen. Hinzu kommen Anforderungen an die Genauigkeit, Robustheit und Cybersecurity der Systeme. Bevor die KI auf den Markt kommt, bedarf es einer Konformitätsprüfung sowie CE-Zertifizierung." Gerade Startups und KMU geraten bei den zur Diskussion stehenden Selbst- und Fremdbewertungen schnell an Grenzen, warnt Formica-Schiller: „Wenn zum Beispiel externe Sachverständige die Risiko-Bewertungen vornehmen, kann das sehr teuer werden. Bei Selbstbewertungen stellt sich die Frage nach adäquaten Kontroll- und Prüfinfrastrukturen beziehungsweise dem Aufbau von Qualitätsmanagementsystemen." Der KI Bundesverband fordert deshalb, Hochrisiko-Anwendungen realitätsnäher zu fassen und unverhältnismäßige Risikobewertungen zu vermeiden. Auch damit Startups und KMU weiterhin gegenüber Konkurrenten von außerhalb der EU wettbewerbsfähig bleiben.

**Neue Haftungsregeln passen Beweislast an**

Die strengen Sorgfaltspflichten für Hochrisiko-KI wiegen umso schwerer, als die EU-Kommission zugleich die Haftungsregeln an das Zeitalter von KI anpasst: Die seit 1986 geltende Produkthaftungsrichtlinie bekommt ein Update, um auch Schwachstellen von Tech-Produkten abzudecken – wie mangelhafte Cybersecurity oder Interkonnektivität für den Datenaustausch im Internet der Dinge. Zusätzlich hat die Kommission Ende September den Entwurf der KI-Haftungsrichtlinie (AI Liability Directive) für außervertragliche und verschuldensabhängige zivilrechtliche Schadensersatzansprüche vorgestellt. „Künftig steuert KI in vielen Lebensbereichen mit: Ein Zug fährt führerlos, LKWs und Autos sind autonom als Shuttle Service unterwegs. Um den Verbraucher auf dasselbe Schutzniveau zu heben wie bei herkömmlichen Produkten, bedarf es angepasster Beweislastregeln. Meist ist es ihm nicht möglich, einen Fehler anhand der ihm zugänglichen Informationen nachzuweisen, da er sich tief verborgen

im System befindet. Im Fall von Hochrisiko-KI erhält der Verbraucher deshalb laut Richtlinienentwurf ein Recht auf Zugang zu Beweismitteln im Besitz von Unternehmen", erklärt Dr. Michael Malterer, Partner bei Dentons in München und Experte für den Bereich Automotive und AI-Haftungsfragen. Um Geschäftsgeheimnisse zu schützen, sollen die Gerichte sicherstellen, dass nur notwendige Daten offengelegt werden. Kommen Unternehmen dem nicht nach, oder lässt sich infolge mangelnder Transparenz der Entscheidungsfindung moderner KI-Systeme nicht eindeutig feststellen, ob eine Pflichtverletzung des Herstellers oder Betreibers den entstandenen Schaden verursacht hat, kommt es zu einer widerlegbaren Kausalitätsvermutung. Das Verschulden des Herstellers oder Betreibers wird dann als ursächlich für den Schaden vermutet. Widerlegen lässt sich dies nur durch den Nachweis anderer plausibler Erklärungen.

**Wachsendes EU-Datenrechtspuzzle**

KI ist nicht denkbar ohne Big Data und auch im Internet der Dinge tauschen Geräte Daten mit Personenbezug aus. Vor allem in Bereichen mit vielen personenbezogenen Informationen wie dem Gesundheitssektor kann die KI-Regulierung Innovationen nur beflügeln, wenn das Zusammenspiel mit dem EU-Datenrecht funktioniert: Angefangen bei der DSGVO über den Data Governance Act bis zum geplanten EU Data Act. So sind Produkte gemäß Data Act künftig so zu konzipieren und herzustellen, dass während des Gebrauchs erzeugte Daten für Nutzer einfach und sicher zugänglich sind. Auf Verlangen muss der Hersteller auch Dritten Datenzugang einräumen, damit diese dem Nutzer Reparatur- oder Beratungsservices anbieten können. Der Data Governance Act schafft die gesetzlichen Grundlagen, um den Datenaustausch zwischen Unternehmen, Privatpersonen und dem öffentlichen Sektor zu vereinfachen. Prof. Dr. Dieter Kugelmann, Landesbeauftragter für Datenschutz und Informationssicherheit in Rheinland-Pfalz und Experte für Datenschutz im Gesundheitswesen, rät Syndizi, sich frühzeitig mit den Neuregelungen, ihren Wechselwirkungen und den Konsequenzen für das eigene Unternehmen zu befassen: „Schon jetzt bewegen sich Unternehmen in einem dichten Geflecht aus gesetzlichen Vorgaben: Für KI im Gesundheitswesen gelten neben DSGVO und Bundesdatenschutzgesetz teils auch Landeskrankenhaus- und Landesdatenschutzgesetze bis hin zu Sozialgesetzen. Die Erfahrung mit der DSGVO zeigt, dass die Rechtsunsicherheit erst einmal steigen wird, bis das Zusammenspiel der Rechtsakte geklärt und eine einheitliche Auslegung durch den Europäischen Gerichtshof erfolgt. Um in einem frühen Produktentwicklungsstadium die Weichen richtig zu stellen, sollten Unternehmen die Übergangszeit nutzen und sich mit den Aufsichtsbehörden austauschen." Je nach Geschäftsmodell können Kooperationen mit Universitäten und gemeinwohlorientierten Einrichtungen sinnvoll sein, um Abläufe zu vereinfachen, so Kugelmann: „Für Forschungsprojekte ist bundesweit eine Datenschutzbehörde zuständig. Und gemeinsam mit der Medizininformatik-Initiative haben wir eine Lösung gefunden, um Routinedaten der klinischen Versorgung künftig deutschlandweit für die medizinische Forschung zu nutzen." Hürden für Health- und Fitness-Apps könnte auch der Europäische Gesundheitsdatenraum beseitigen, der Informationen von über 500 Millionen Europäern zu einer der weltgrößten Gesundheitsdatenbanken zusammenführen soll. Das ermöglicht nicht nur bessere Prävention, Diagnosen und Therapien. Chancen für Forschung und Innovation ergeben sich auch, wenn beispielsweise Informationen aus Gesundheits- und Wellness-Anwendungen wie

„Unternehmen mit KI-Innovationen sollten die Übergangszeit nutzen und sich in einem frühen Produktentwicklungsstadium mit den Aufsichtsbehörden zu Auslegungsfragen austauschen."

**Prof. Dr. Dieter Kugelmann, Landesbeauftragter für Datenschutz und Informationssicherheit in Rheinland-Pfalz**

Wearables einbezogen werden. „Hierzu gibt es aber bereits jetzt große Diskussionen und dies wird viele neue Fragestellungen etwa zum Schutz der Privatsphäre mit sich bringen", berichtet Formica-Schiller.

**Digitales Mindset ist entscheidend**

Ob AI Act, Data Act und Gesundheitsdatenraum Künstliche Intelligenz beflügeln können, hängt laut Formica-Schiller vor allem von einem digitalen Mindset ab: Von der Gesetzgebung und Umsetzung bis zur Kontrolle durch die Behörden. Inhouse Counsel können ebenfalls einen Beitrag leisten, so Stefan Dittmer: „Wer Chancen aufzeigt und schildert, wie sich Risiken begrenzen lassen, stärkt auch das Vertrauen in KI." Zudem lassen sich im Gesetzgebungsverfahren noch Verbesserungen erzielen. Seit die Kommission den Entwurf im April 2021 präsentiert hat, wurden über 3.000 Änderungsanträge eingereicht. Voraussichtlich wird der AI Act nicht vor 2024 in Kraft treten. Entwickler, Anbieter und Anwender von KI-Systemen sollten aber jetzt die Weichen stellen, um Risiken aktiv zu managen und Geschäftschancen infolge der neuen EU-Datenregulierung zu nutzen. ■ *Franziska Jandl*

## Risk-Assessment KI-Regulierung

Sechs Maßnahmen, um die Haftung zu minimieren und Risiken aktiv zu managen:

**1. Aufbau eines Risikomanagementsystems für alle Phasen im Lebenszyklus von Hochrisiko-KI**

- Prozesse, um Design-, Konstruktions- und Fabrikationsfehlern vorzubeugen
- Regelmäßiges Monitoring möglicher Risiken im weiteren Lebenszyklus, etwa wenn ein Produkt mit integrierter, maschinell lernender KI die Funktionsweise verändert
- Werden KI-Vorfälle schnell erkannt und kann auf etwaige Schäden rasch reagiert werden?
- Permanente Verbesserung der Dokumentation: Die strengen Anforderungen der KI-Haftungsrichtlinie hinsichtlich Beweislast und Kausalität lassen sich überwinden, wenn Unternehmen nachweisen: Was wurde wann und wie hergestellt, eingeführt, geändert oder aktualisiert?
- Regelmäßige Tests von Systemen und Risikoplänen

**2. Haftungsumfang klären**

- Wie groß ist der Spielraum der Mitgliedsstaaten bei der Umsetzung der EU-KI-Haftungsrichtlinie?
- Bei Unternehmen mit internationalem Bezug: Welche Haftungsregime sehen die verschiedenen Länder vor?

**3. Vertrags-Checkup**

- Haftung und Schadenshöhe limitieren
- Lücken der Richtlinie analysieren und für Vertragsgestaltung nutzen
- Verantwortlichkeit für Komponenten von Drittunternehmen regeln: Freistellungs- beziehungsweise Regressansprüche bestimmen und gegebenenfalls begrenzen

**4. Schutz von Geschäftsgeheimnissen:**

- Auf welche Dokumente haben potenzielle Kläger künftig Zugriff? Mit welchen Maßnahmen lässt sich ein zu tiefer Einblick Fremder verhindern?

**5. Kommunikation:**

- Trainings für Beschäftigte, die KI mit hohem Risiko konzipieren, entwickeln, implementieren oder betreiben
- Interne Handbücher und Guidelines, die auf neue Regelungen und Pflichten hinweisen
- Wird der Nutzer ausreichend instruiert und über Risiken aufgeklärt?

**6. Versicherungsschutz prüfen**

*Quelle: Dentons*