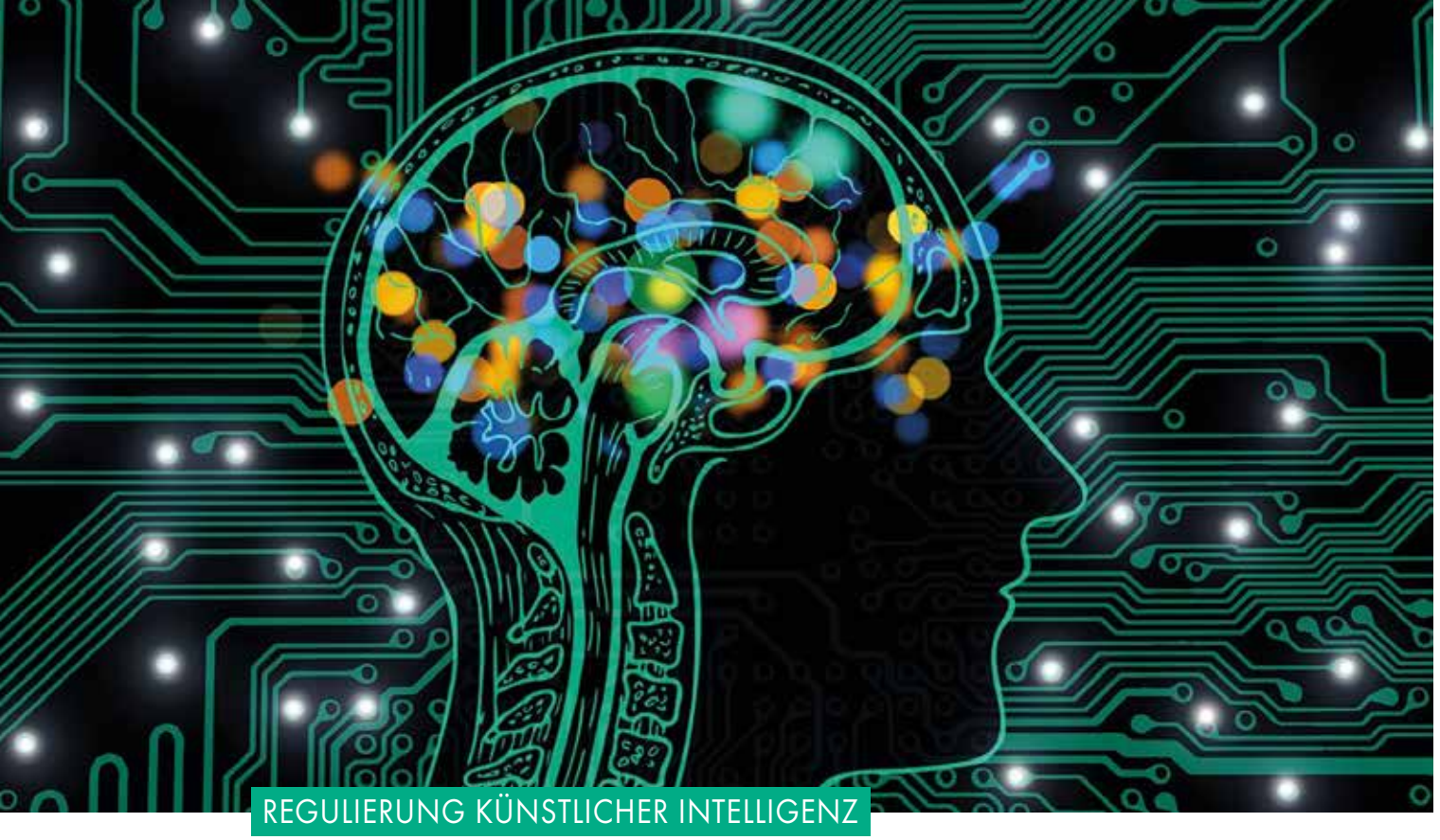

REGULIERUNG KÜNSTLICHER INTELLIGENZ

JE GRÖSSER DAS RISIKO, DESTO ENGER DAS KORSETT

Das Weißbuch für künstliche Intelligenz der EU-Kommission markiert Leitlinien für die Regulierung in Europa. Im Fokus steht lernende Software mit hohem Risiko, etwa für Medizin, Verkehr oder Energie. Brisanz für Unternehmen bergen Überlegungen zu einer verschärften Haftung und Beweislastumkehr.

„Von rein informationsgebender KI bis zu einem am Markt lernenden, agierenden System gibt es vielfältige Anwendungsfelder mit unterschiedlichen Risiken."

– Dr. Thomas Laubert, Group General Counsel, Daimler AG

▸ Die EU-Kommission plant den großen Wurf. Mit den im Februar vorgestellten Strategien für Daten und künstliche Intelligenz (KI) will sie Europa in die Lage versetzen, zur attraktivsten, sichersten und dynamischsten datenagilen Wirtschaft der Welt zu werden. Bestandteil ist das Weißbuch der EU-Kommission, das eine Vision für die Zukunft von KI und ihren Rechtsrahmen skizziert.

Dabei bewegt sich die Kommission in einem komplexen Spannungsfeld: Einerseits warten beispielsweise Automobilhersteller dringend auf Investitionssicherheit durch international klare Rahmenbedingungen, damit autonome Autos grenzüberschreitend fahren können. Andererseits können zu detaillierte Regelungen innovative Startups sowie kleine und mittelständische Unternehmen (KMU) schnell überfordern. Und drittens gilt es, Sorgen der Bürger entgegenzuwirken und Vertrauen aufzubauen. Schließlich wird die Durchsetzung von Grundrechten im Hinblick auf Datenschutz, Privatsphäre und Gleichbehandlung erschwert, wenn Algorithmen bei

FÜR JEDEN SCHRITT DER RICHTIGE PARTNER.

Menold Bezler – Rechtsanwälte, Steuerberater, Wirtschaftsprüfer

MENOLD BEZLER

MITTELSTAND IM MITTELPUNKT®

FREEK STÄHR,
Head of Commercial Legal & Operations; Mitglied des SAP AI Ethics Steering Committee, SAP SE

TILL BARLEBEN,
Rechtsanwalt, Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) e.V.

THANOS RAMMOS,
Rechtsanwalt und Partner, Taylor Wessing

Kreditvergabe, Recruiting, Bewilligung von Sozialleistungen oder Rückfallwahrscheinlichkeit von Straftätern wie in einer Blackbox handeln und schwer oder gar nicht zu verstehen sind. Letzteres ist der Fall bei maschinell lernender KI-Software, die sich selbst weiterentwickelt, ohne dass jeder Schritt im Voraus festgelegt wird. Diese Anwendungen werden in geringem Maß oder schließlich gar nicht mehr unmittelbar von den Menschen gesteuert oder beaufsichtigt.

HOHES RISIKO IM GESUNDHEITSWESEN, IN VERKEHR UND ENERGIE

Um die Verhältnismäßigkeit des regulatorischen Eingreifens sicherzustellen, setzt die EU-Kommission auf einen risikobasierten Ansatz. „Es werden keine Verbotskataloge geschaffen und es steht keine Komplettrevision der rechtlichen Rahmenbedingungen an“, sagt Rechtsanwalt Till Barleben vom Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) in Frankfurt am Main. „Im ersten Schritt sollen stattdessen bestehende Vorschriften wie Produkthaftungs-, Datenschutz- und Medizinprodukterecht weiter angewendet werden“, erläutert Dr. Roland Wiring, Rechtsanwalt und Partner bei der Wirtschaftskanzlei CMS Deutschland am Standort Hamburg. „Schritt zwei sieht vor, diese für KI mit hohem Risiko etwa in den Sektoren Gesundheitswesen,

Compliance-Check für KI

1. Rechtlicher Rahmen
- Datenschutz
- Cybersicherheit
- KI-generiertes Intellectual Property
- Arbeitsrecht
- Produkt- und Produzentenhaftung
- Spezialvorschriften etwa für Medizinprodukte
- Im Weißbuch für KI mit hohem Risiko skizzierte Anforderungen an:
  - Trainingsdaten
  - Aufbewahrung von Daten und Aufzeichnungen
  - Vorzulegende Informationen
  - Robustheit und Genauigkeit
  - Menschliche Aufsicht
  - Besondere Anforderungen, etwa an Anwendungen für biometrische Fernidentifikation

2. Umfassende Risikoanalyse für alle Phasen im Produkt-Lebenszyklus: von Entwicklung und Produktion bis zum Einsatz beim Kunden

3. Prozesse zur Risikominimierung
- Sind Design-, Konstruktions- und Fabrikationsfehler so weit wie möglich ausgeschlossen?
- Regelmäßiges Monitoring: Welche praktischen Erfahrungswerte gibt es? Welche Sicherheitsrisiken können im weiteren Lebenszyklus entstehen, etwa wenn ein Produkt mit integrierter, maschinell lernender KI seine Funktionsweise verändert?
- Reicht die Dokumentation, um die Entscheidungen der Systeme nachzuvollziehen und Fehler nachträglich zu korrigieren und auszuschließen?

4. Klare Rahmenbedingungen für Nutzer und Geschäftspartner
- Wird der Nutzer ausreichend instruiert und über Risiken aufgeklärt?
- Ist angesichts der Komplexität und Vielzahl von Zuliefererprodukten die eigene Verantwortlichkeit vertraglich klar geregelt?

Verkehr, Energie sowie Teilen des öffentlichen Sektors zu flankieren durch weitere Regelungen, die den neuen Herausforderungen durch KI gerecht werden. Dabei soll immer auch gefragt werden: Wird die KI-Anwendung in dem jeweiligen Sektor so eingesetzt, dass mit erheblichen Risiken zu rechnen ist?“ Laut Weißbuch dürfte ein Fehler in einem Terminvereinbarungssystem eines Krankenhauses in der Regel keine so erheblichen Risiken mit sich bringen, dass ein gesetzgeberisches Eingreifen gerechtfertigt wäre. Bei einem Einsatz im Recruiting droht jedoch grundsätzlich in jedem Sektor das Risiko einer Diskriminierung. Dr. Thomas Laubert, Group General Counsel der Daimler AG, fordert deshalb: „Wir brauchen jeweils eine passgenaue Lösung: Von einer rein informationsgebenden KI bis hin zu einem am Markt lernenden, agierenden System gibt es vielfältige Anwendungsfelder mit unterschiedlichen Risiken.“

„Für KI-Anwendungen, die künftig als hohes Risiko einzustufen sind, nennt das Weißbuch bereits recht detaillierte Anforderungen an eine Konformitätsprüfung“, berichtet Thanos Rammos, Rechtsanwalt und Partner bei Taylor Wessing in Berlin. „Beispielsweise sollen die Trainingsdaten ausreichend repräsentativ sein und den Schutz der Privatsphäre und personenbezogener Daten sicherstellen. Damit Entscheidungen besser nachvollziehbar sind, soll zum Beispiel genau dokumentiert werden: Welche Daten werden für das Training verwendet? Und welche Methoden, Verfahren und Techniken liegen der Programmierung, Erprobung und Validierung zugrunde?“

„Im ersten Schritt sollen bestehende Vorschriften wie Produkthaftungs-, Datenschutz- und Medizinprodukterecht weiter angewendet werden. Schritt zwei sieht vor, diese für KI mit hohem Risiko etwa in den Sektoren Gesundheitswesen, Verkehr, Energie sowie Teilen des öffentlichen Sektors zu flankieren durch weitere Regelungen, die den neuen Herausforderungen durch KI gerecht werden.“

– Dr. Roland Wiring, Rechtsanwalt und Partner, Wirtschaftskanzlei CMS Deutschland

VERSCHÄRFTE HAFTUNG DURCH BEWEISLASTUMKEHR

Zudem finden sich recht konkrete Vorschläge im Weißbuch und Bericht der EU-Kommission über den Sicherheits- und Haftungsrahmen, welche die Haftungsrisiken für Unternehmen vergrößern können, warnt Till Barleben vom ZVEI: „Konkret geht es darum, ob und in welchen Fällen die Gefährdungshaftung über die existierenden Produkthaftungsregeln hinaus ausgebaut wird. Etwaige Anpassungen für KI sollten aber in einem gesonderten Rechtsinstrument und auf KI beschränkt diskutiert werden. Die etablierte technikneutrale Produkthaftungsrichtlinie sollte nicht angetastet werden.“

Kritisch sieht Barleben auch Überlegungen zu einer Beweislastumkehr: „Entsprechend dem risikobasierten Ansatz der EU-Kommission ist das allenfalls für KI-Anwendungen mit hohem Risiko zu diskutieren.“ Einig sind sich Syndizi und Anwälte darin, dass es klare Regeln zur Haftung der Unternehmen geben muss, damit sie ihr Risiko richtig bewerten können. Ansonsten würden hohe Investitionen in innovative Technologien schnell unkalkulierbar und dadurch ausgebremst.

Immer mehr Unternehmen und Verbände setzen KI selbst Grenzen

Sie stellen eigene Leitlinien für den Einsatz und Umgang mit cleveren Maschinen, Autos oder Software für das smart Home auf:

- Bosch KI-Kodex: https://www.bosch.com/de/stories/ethische-leitlinien-fuer-kuenstliche-intelligenz/
- Daimler-Prinzipien für KI: https://www.daimler.com/nachhaltigkeit/daten/ki-guidelines.html
- Grundsätze der SAP für den Umgang mit KI, die sich an den Ergebnissen der High Level Expert Group der EU-Kommission orientieren: https://news.sap.com/germany/2018/09/ethische-grundsaetze-kuenstliche-intelligenz/
- ZVEI-Positionspapier für „Menschenzentrierte KI in der Industrie“ https://www.zvei.org/presse-medien/publikationen/menschenzentrierte-kuenstliche-intelligenz-in-der-industrie-positionspapier/

„Zusammen mit den Technikern ist zu antizipieren: Wie kann sich die Funktionsweise einer Maschine mit selbstlernender KI im weiteren Verlauf ihres Lebenszyklus verändern? Unter Umständen kann es sinnvoll sein, dass die Produktentwickler das eigenständige Lernen der Software begrenzen und so eine menschliche Kontrolle in letzter Instanz sicherstellen."

– Dr. Philipp Haas, Leiter Recht für Digitales und neue Geschäfte, Robert Bosch GmbH

RISK ASSESSMENT ÜBERPRÜFEN

Was sind die Konsequenzen für Unternehmensjuristen? Sie müssen die Entwicklung der Diskussion im Blick behalten und gegebenenfalls ihr Risk Assessment anpassen. „Schon jetzt ist eine regelmäßige Konformitätsprüfung aller KI-Anwendungen sinnvoll, die das Unternehmen bereits einsetzt", rät Thannos Ramos. Es bedarf einer laufenden Selbstbeobachtung und Einzelfallbewertung im Hinblick auf den technologischen Fortschritt und auf Haftungsrisiken: „Zusammen mit den Technikern ist beispielsweise zu antizipieren: Welche Sicherheitsrisiken können entstehen, wenn intelligente Software nachträglich in Produkte eingebunden wird? Wie kann sich die Funktionsweise einer Maschine mit selbstlernender KI im weiteren Verlauf ihres Lebenszyklus verändern? Unter Umständen kann es sinnvoll sein, dass die Produktentwickler das eigenständige Lernen der Software begrenzen und so eine menschliche Kontrolle in letzter Instanz sicherstellen", erklärt Dr. Philipp Haas, Leiter Recht für Digitales und neue Geschäfte bei der Robert Bosch GmbH (siehe auch Kasten „Compliance-Check für KI" auf Seite 40).

„Wenn ein Unternehmen eine KI-Anwendung entwickelt oder nutzt, die voraussichtlich unter die Hochrisikoeinstufung fällt, sollte es bereits jetzt eigene Leitlinien aufstellen", rät Thannos Rammos. Bosch, SAP oder Daimler haben dies bereits getan: „Wir haben uns als erster Automobilhersteller im Herbst 2019 KI-Prinzipien gegeben: Verantwortungsvoller Einsatz, Erklärbarkeit, Schutz der Privatsphäre, Sicherheit und Zuverlässigkeit. Damit schaffen wir das Bewusstsein und die Rahmenbedingungen für einen verantwortungsvollen Umgang mit KI", berichtet Thomas Laubert von Daimler (siehe auch Kasten „Immer mehr Unternehmen und Verbände setzen KI selbst Grenzen" auf Seite 41).
Damit Europa wie von der Kommision geplant zur datenagilsten Wirtschaft der Welt aufsteigen kann, kommt es vor allem auf ausreichendes Trainingsmaterial für KI an. Freek Stähr, Head of Commercial Legal & Operations bei SAP in Walldorf und Mitglied des SAP AI Ethics Steering Committee, ist deshalb skeptisch: „Die meisten Business Cases für den Einsatz von KI beinhalten personenbezogene Daten. Dreh- und Angelpunkt sind also europäische Standards für Verhaltensregeln und Zertifizierungen etwa für die Anonymisierung. Bisher bremsen die unterschiedlichen Auslegungen der Datenschutzaufsichtsbehörden und die fragmentierte Ausgestaltung der Öffnungsklauseln in den Mitgliedsstaaten Innovationen aus." Zudem sei zu befürchten, dass der im Weißbuch skizzierte administrative Aufwand Start-Ups und KMU benachteiligie. ■ *Franziska Jandl*

- Anwendungsfelder und Formen von KI sind vielfältig und reichen von rein informationsgebenden bis hin zu autonom handelnden Systemen, deren Entscheidungen nicht vollständig nachvollziehbar sind. Die EU-Kommission verfolgt deshalb einen risikobasierten Ansatz für die Regulierung.
- Syndizi bewerten positiv, dass die EU-Kommission keine Verbotskataloge schaffen will und keine Komplettrevision der rechtlichen Rahmenbedingungen anstrebt.
- Kritisch sehen Unternehmen eine Haftungsverschärfung. Eine Beweislastumkehr zugunsten von KI-Geschädigten könnte Investitionen unkalkulierbar machen.
- Syndizi müssen die Entwicklung der Diskussion auf europäischer Ebene und in den Mitgliedsstaaten aufmerksam verfolgen und ihr Risk Assessment gegebenenfalls anpassen.
- Die im Weißbuch der Europäischen Union skizzierten regulatorischen Anforderungen könnten insbesondere KMU und Start-ups überfordern.