Bildnachweis: Behörde für Wissenschaft und Innovation; unter Nutzung von KI

RESPONSIBLE AI

Studie zum verantwortungsvollen Umgang mit künstlicher Intelligenz, insbesondere in kleinen und mittleren Unternehmen

.

aric

LAWCOM INSTITUTE

Hamburg

Responsible AI für die Gesellschaft:

Wie Hamburg den gesellschaftlich verantwortlichen Einsatz Künstlicher Intelligenz in der Wirtschaft sicherstellt.

Studie des LawCom.Institute und ARIC e.V.

im Auftrag der Behörde für Wirtschaft und Innovation der Freien und Hansestadt Hamburg (Förderung Dezember 2021 bis Dezember 2022).

Herausgeber:	Freie und Hansestadt Hamburg, Behörde für Wirtschaft und Innovation (BWI) V.i.S.d.P.: Martin Helfrich, Leiter Kommunikation Alter Steinweg 4, 20459 Hamburg Telefon: 040 42841-2239, E-Mail: pressestelle@bwi.hamburg.de
Autor:innen:	Dr. Ulrike Ehling (LawCom.Institute), Friedrich-Joachim Mehmel (LawCom.Institute), Clara Sieveking (LawCom.Institute), Elisabeth Weißbecker (ARIC e.V.)
Mitarbeit:	Dr. Jan Curschmann (LawCom.Institute), Steven Dehlan (ARIC e.V.), Alois Krtil (ARIC e.V.), Louisa Rockstedt (ARIC e.V.), Jan Ruhnke (ARIC e.V.)
Kontakt:	LawCom.Institute GmbH, www.lawcom.institute Behörde für Wirtschaft und Innovation, IW 1, Grundsatzfragen der Wirtschaftspolitik, www.hamburg.de/bwi/wirtschaftspolitik

Inhaltsverzeichnis

Vorspann: Warum gerade jetzt eine Studie zu den rechtlichen Voraussetzungen des Einsatzes Künstlicher Intelligenz in Hamburger Unternehmen richtig und wichtig ist.

Die Digitalisierung und der Einsatz Künstlicher Intelligenz (KI) haben ein enormes Potential für die Wirtschaft und Unternehmen. Dieses Potential wird in der Gesellschaft und bei den Bürger:innen gesehen. Es bestehen allerdings auch erhebliche Vorbehalte im Hinblick auf mögliche Fehlerquellen, fehlende Transparenz oder ein fehlendes Bewusstsein für einen gesellschaftlich verantwortlichen Einsatz der Technik. Die Notwendigkeit einer Regulierung der Entwicklung und des Einsatzes von KI, entsprechend einer normativen Festlegung von Mindestanforderungen, wird laut Umfragen ausdrücklich bejaht. Mit dem Entwurf einer KI-Verordnung, dem sogenannten KI-Act, hat die Europäische Union (EU) einen wesentlichen Schritt in diese Richtung getan. Der Entwurf befindet sich zurzeit in der Abstimmung zwischen der EU-Kommission, dem Europäischen Rat und dem Europäischen Parlament und wird voraussichtlich im Laufe des Jahres 2023 in Kraft treten. Damit entfaltet die Verordnung unmittelbare Wirkung für Unternehmen und die Verwaltung innerhalb aller Mitgliedstaaten der EU.

Im Mittelpunkt der von der Behörde für Wirtschaft und Innovation der Freien und Hansestadt Hamburg in Auftrag gegebenen Studie stehen die Auswirkungen der geplanten Regulierung auf kleine und mittlere Unternehmen (KMU) in der Stadt. Ziel ist es zunächst, ein allgemeines Bewusstsein für die rechtlichen Veränderungen zu schaffen, aber auch die gesellschaftlichen Bedarfe herauszuarbeiten, die sich innerhalb demokratischer Rechtsstaaten für alle handelnden Akteure ergeben. Hieraus auch für die Stadt, für ihre Förder- und Wirtschaftspolitik, mögliche Handlungsoptionen aufzuzeigen, ist ebenfalls Gegenstand der vorliegenden Studie.

- Aus Sicht kleiner und mittelständischer Unternehmen kommt dem Einsatz Künstlicher Intelligenz jetzt und in der Zukunft eine überragende wirtschaftliche Bedeutung zu. Die Technik hilft u.a., die Produktivität zu steigern, sie hilft, neue Märkte zu erschließen, und sie hilft, Unternehmensabläufe effizienter und effektiver zu gestalten. Ein frühzeitiger Umgang der Unternehmen mit den durch den KI-Act zu erwartenden rechtlichen Anforderungen an Entwicklung und Einsatz von KI kann daher wirtschaftliche Risiken vermeiden und die Wettbewerbsfähigkeit von Hamburger KMU auch im europäischen Binnenmarkt sichern.
- Aus Sicht der Bürger:innen ist ein gesellschaftlich verantwortungsvoller Umgang mit der Digitalisierung von zunehmender Bedeutung. Immer öfter wird etwa von Kund:innen auf ein verantwortliches Handeln von Unternehmen Wert gelegt, etwa im Hinblick auf negative Auswirkungen für das Klima, die Einhaltung von Menschenrechten oder den Schutz der Gesundheit. Gegenüber staatlichen Institutionen erwarten die Bürger:innen ebenso, dass die mit der Digitalisierung einhergehende Transformation keine neuen Gerechtigkeitslücken reißt oder bestehende Diskriminierung fortschreibt und verstärkt. Fehlendes Vertrauen hat daher sowohl Bedeutung für die Akzeptanz staatlichen Handelns als auch für das wirtschaftliche Handeln von Unternehmen.
- Und nicht zuletzt kommt dem Thema der Förderung der Digitalisierung, insbesondere im Hinblick auf den vor der Verabschiedung stehenden KI-Act, auch für die Wirtschafts- und Förderpolitik der Stadt eine herausragende Bedeutung zu. Es geht um die Sicherung und Stärkung des Wirtschaftsstandortes Hamburg, um die Zukunftsfestigkeit der Hamburgischen Wirtschaft und den Erhalt und die Schaffung neuer Arbeitsplätze. Zentrale These der vorliegenden Studie ist, dass

unter Beachtung der Anforderungen an einen gesellschaftlich verantwortlichen Einsatz von KI entlang des Konzeptes einer *Responsible Artificial Intelligence* (RAI) – und damit eine konsequente Durchsetzung rechtsstaatlicher Prinzipien über rein rechtliche Anforderungen hinaus – für die Stadt ein möglicher Standortvorteil entwickelt werden kann.

Im ersten Teil der Studie wird zunächst die in den letzten Jahren zunehmend an Fahrt aufnehmende Diskussion zu den Risiken von KI und der Notwendigkeit einer Einhegung von Technik durch Recht dargestellt (Kapitel 1). Im Folgenden wird sowohl der Verordnungsentwurf zur Regulierung Künstlicher Intelligenz der Europäischen Union, der sogenannte KI-Act, in seinen zentralen Dimensionen vorgestellt, als auch dessen Bedeutung für KMU erörtert. In diesem Kapitel werden weiter die sich daraus ergebenden institutionellen Anforderungen an die Aufsicht und die Durchsetzung des sich entwickelnden Regelungswerkes (insbesondere Konformitätsprüfungen, Notifizierungen sowie Registrierungen) sowie das geplante, den KI-Act ergänzende Haftungsregime der EU anhand der KI-Haftungs- sowie der Produkthaftungsrichtlinie dargestellt (Kapitel 2). Schließlich wird grundsätzlich auf die gesellschaftliche Bedeutung des verantwortlichen Einsatzes von KI und auf das Konzept einer *Responsible AI* eingegangen. Hier wird argumentiert, dass es nachteilige Auswirkungen auf den wirtschaftlichen Erfolg von Unternehmen haben kann, wenn die aus dem RAI-Konzept sowie dem KI-Act abgeleiteten Grundsätze nicht beachtet werden (Kapitel 3).

Im Anschluss daran wird der Blick auf den aktuellen Stand in Hamburg und die Situation für die Hamburger KMU Landschaft geworfen, u.a. mit Fokus auf die Hamburger Forschungslandschaft sowie bestehende Beratungsangebote in der Stadt (Kapitel 4). Was auf Hamburger KMU zukommt und wo die Stadt EU-seitig zur Innovationsförderung angehalten ist, wird schließlich im fünften Kapitel dargestellt, konkretisiert hinsichtlich der Anforderungen an KMU anhand einer am KI-Act orientierten Checkliste. Mit Hilfe der Liste können die Auswirkungen des KI-Acts systematisch identifiziert und eingeordnet werden. In diesem Kapitel werden schließlich – ohne Anspruch auf Vollständigkeit – mögliche technische Lösungen im Sinne eines gesellschaftlich verantwortlichen Einsatzes von KI beschrieben. Die Studie schließt im sechsten Kapitel mit der Benennung von Handlungsempfehlungen vor dem Hintergrund der in den Kapiteln 1-5 gewonnenen Erkenntnisse. Neben der schon erwähnten Checkliste und technischen Empfehlungen wird auf eine mögliche Governance-Struktur eines KI-Ökosystems in Hamburg eingegangen, das sowohl Beratungsangebote bereitstellt als auch niedrigschwellige und aktuelle Informationen zu Gesetzgebungsprozessen und Anforderungen an KMU gewährleistet mit dem Ziel einer praktischen Unterstützung von Hamburger KMU beim Einsatz von KI-Systemen entlang rechtsstaatlicher und demokratischer Prinzipien.

„Der KI-Act bewegt sich im Spannungsfeld zwischen den Ansprüchen, auf der einen Seite nicht innovationshemmend für den europäischen KI-Markt zu wirken und auf der anderen Seite den Sorgen von Bürger:innen und Unternehmen Rechnung zu tragen und somit vertrauensfördernde Anforderungen an KI-Systeme zu stellen. Das Recht, in Form des KI-Acts, stellt dabei das Instrument dar, mit dem diese Sorgen adressiert und Vertrauen geschaffen wird. Unter dem Begriff Responsible AI summieren sich diverse technische und organisatorische Ansätze, die die rechtlichen Anforderungen in die Praxis übersetzen können.“

Alois Krtil, Geschäftsführer, ARIC e.V.

1. Einleitung: KI-Regulierung – Einhegung von Technik durch Recht

Im Zusammenhang mit KI gibt es sowohl Chancen als auch Risiken. In der Vergangenheit haben bereits eine Reihe von Negativbeispielen gezeigt, welche Konsequenzen drohen, wenn der Einsatz von KI nicht verantwortungsvoll umgesetzt wird und damit einen Anstoß für mehrere, derzeit parallel laufende Regulierungsbemühungen gegeben, die sich in ihrer geografischen Reichweite und im Grad ihrer Verbindlichkeit stark unterscheiden. Für Hamburg ist insbesondere der KI-Act relevant, der in Kapitel 2 näher vorgestellt wird.

Die Versprechen Künstlicher Intelligenz[1] sind groß: die Chance auf ein nachhaltiges und effizienteres Wirtschaftssystem, auf mehr demokratische Partizipation und Zugang zu Wissen, auf mehr Zeit für sinnstiftende Tätigkeiten und verlässlichere Prognosen für die Zukunft. Auf vielen Ebenen wird über den Einsatz Künstlicher Intelligenz in den unterschiedlichsten gesellschaftlichen und unternehmerischen Kontexten diskutiert. Ganz praktisch kommt Künstliche Intelligenz zunehmend im Gesundheitssektor zum Einsatz, ebenso in Personalabteilungen oder dem Marketing. Städtische Verwaltungen greifen auf die Unterstützung von KI bei der Bearbeitung von Bürger:innen-Anfragen zurück, Rechtsdienstleister:innen nutzen sie zur Bearbeitung von auf gleichartigen Sachverhalten beruhenden Massenverfahren. Die Mustererkennung als eine mögliche Form der KI-Anwendung bietet in all diesen Bereichen große Effizienzgewinne und weitere Potentiale, kann Entscheidungen auf eine belastbarere Grundlage stellen und wichtige Perspektiven für die Zukunft bedeuten.

Gerade vor dem Hintergrund dieser enormen Potentiale nimmt die Diskussion über Risiken und die Notwendigkeit von Regulierungsbemühungen rund um die eingesetzten Systeme bedeutend an Fahrt auf. Und dies ganz zu Recht. Denn ein ungeregelter Einsatz von KI birgt auch Gefahren, insbesondere für die Freiheits- und Bürger:innenrechte, für Arbeitnehmer:innen und die Umwelt und am Ende für den Rechtsstaat im Allgemeinen. Einige Fälle sind allseits bekannt, in denen der Einsatz von Algorithmen zum Teil weitreichende Folgen hatte:

[1] Unter Künstlicher Intelligenz versteht man einen Teilbereich der Informatik, dessen Anwendungen die Lösung komplexer Probleme ermöglichen, für die es ansonsten menschliches, intelligentes Handeln erfordert. Dieses schließt beispielsweise Bilderkennung (maschinelles Sehen), Natural Language Processing (Textverständnis und -erzeugung) und analytische Entscheidungsfindung ein. Unterschieden werden u.a. datenbasierte (Maschinelles Lernen), wissensbasierte (Expertensysteme) und hybride Modelle, die wiederum unterschiedliche Lernverfahren und Algorithmen kennen. Künstliche Intelligenz wird im Folgenden als KI oder im englischsprachigen Kontext als AI abgekürzt.

- Über die Kindergeldaffäre in den Niederlanden ist die letzte Regierung Rutte im Januar 2021 zum Rücktritt gezwungen worden. Der Vorwurf lautete „rassistische Diskriminierung" aufgrund einer automatisierten Entscheidung, bei der die nationale Steuerbehörde fälschlicherweise Kindergeldzahlungen zurückgefordert und Betrugsermittlungen gegen zehntausende Familien in den Niederlanden aufgenommen hatte. Schon kleine Formfehler beim Ausfüllen der Anträge, vor allem aber die zugrunde gelegte Datenbasis, bei der die Staatsangehörigkeit als zentraler Verdachtsmarker genutzt wurde, hatten Familien nicht nur einer unhaltbaren finanziellen Belastung ausgesetzt, sondern für viele auch weitere Ermittlungen und rechtliche Konsequenzen zur Folge.[2]
- Schon seit etwa zehn Jahren sorgt insbesondere Bias, also eine systematische Verzerrung aufgrund bestimmter Trainingsdaten, die dann die Entscheidungsfindung beeinflusst (siehe Glossar), in KI-Anwendungen für Schlagzeilen. So etwa als 2014/15 berichtet wurde, dass bei Amazon ein KI-basiertes Tool zur Auswahl von Bewerber:innen systematisch Männer für Tech Jobs bevorzugte. Das Rekrutierungstool suchte nach Mustern in Bewerbungen der letzten zehn Jahre, um daraus eine Priorisierung abzuleiten. Da sich in der Vergangenheit überwiegend Männer beworben hatten, hatte sich die KI selbst beigebracht, Bewerbungen von Frauen als ungeeignet herauszufiltern.[3]
- 2015 sorgte die App „Google Fotos", die Bilder automatisch sortiert und verschlagwortet, für Aufsehen, als bei der automatischen Verschlagwortung dunkelhäutige Menschen als Gorillas bezeichnet wurden. Die KI hatte auf eine Datenbank zurückgegriffen, die auch Tierbilder beinhaltete, und in Folge den schwerwiegenden Fehler begangen, Menschen mit Tieren zu verwechseln.[4]
- 2016 zeigte sich ebenfalls, was passieren kann, wenn eine KI ungefiltert im Betrieb weiterlernt, als der Microsoft Chatbot Tay auf Twitter durch Nutzer:inneneingaben innerhalb von Stunden rassistisch und frauenfeindlich wurde.[5] Seither haben zahlreiche wissenschaftliche Veröffentlichungen Diskriminierung von KI-Anwendungen konstatiert. Die jüngsten Beispiele liefert ChatGPT, das vermeintlich schon Bias adressiert und sich beispielsweise weigert Witze über Gottheiten des Islam und Christentums zu schreiben,

[2] Dachwitz, Ingo, Netzpolitik (29.12.2021): Niederlande zahlen Millionenstrafe wegen Datendiskriminierung, https://netzpolitik.org/2021/kindergeldaffaere-niederlande-zahlen-millionenstrafe-wegen-datendiskriminierung/ (zuletzt aufgerufen am 28.02.2023)

[3] Dastin, Jeffrey, REUTERS (11.10.2018): Amazon scraps secret AI recruiting tool that showed bias against women, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G (zuletzt aufgerufen am 28.02.2023)

[4] Autor unbekannt, SPIEGEL NETZWELT (02.07.2015): Google entschuldigt sich für fehlerhafte Gesichtserkennung, https://www.spiegel.de/netzwelt/web/google-fotos-bezeichnet-schwarze-als-gorillas-a-1041693.html (zuletzt aufgerufen am 28.02.2023)

[5] Graff, Bernd, Süddeutsche Zeitung (03.04.2016): Rassistischer Chat-Roboter: Mit falschen Werten bombardiert, https://www.sueddeutsche.de/digital/microsoft-programm-tay-rassistischer-chat-roboter-mit-falschen-werten-bombardiert-1.2928421 (zuletzt aufgerufen am 28.02.2023)

selbiges aber über Gottheiten der Hindus erst nach Beschwerden von Nutzer:innen verweigerte.[6]

- Ein weiteres Beispiel für unintendierte Folgen in der Anwendung eines Chatbots liefert jüngst auch die Suchmaschine Bing, die basierend auf derselben Technik wie ChatGPT ebenfalls komplexe Fragen beantwortet und Konversation mit den Nutzer:innen betreiben kann. So hatte der Versuch eines Reporters der New York Times für Aufsehen gesorgt, der nach einer längeren Konversation mit der KI von dieser zum Verlassen seiner Frau aufgefordert wurde. Auch andere Nutzer:innen hatten darauf hingewiesen, dass der Chatbot unangemessene Antworten gebe und auch vor Drohungen und Erpressungen nicht zurückschrecke.[7]

Vor dem Hintergrund derartiger Erfahrungen und zum Teil weitreichender Risiken richtet sich auch auf politischer Ebene und in internationalen Organisationen zunehmend der Blick auf Anforderungen an Hersteller:innen und Nutzer:innen von algorithmenbasierten Lösungen im Allgemeinen und KI-Lösungen im Besonderen, auf Rechenschaftspflichten, Normierungsbemühungen und Zertifizierungsverfahren. Es gilt, derartige Fehlfunktionen zu minimieren, Diskriminierung vorzubeugen und auf den verlässlichen und rechtssicheren Einsatz vertrauenswürdiger KI-Systeme hinzuarbeiten. Insgesamt nehmen daher weltweit Regelwerke zu, die zum Ziel haben, den Einsatz Künstlicher Intelligenz in Wirtschaft und Gesellschaft gleichermaßen an Kriterien der Verantwortlichkeit, Fairness und Belastbarkeit zu binden:

- Im Februar 2022 wurde im US-Senat und Repräsentantenhaus der Entwurf für einen *Algorithmic Accountability Act* vorgelegt. Er versucht, ex ante Standards für die Entwicklung und Nutzung von automatisierten Entscheidungssystemen zu definieren und Akteure auf eine Technikfolgenabschätzung zu verpflichten. Außerdem wird in dem Entwurf der Aufbau staatlicher Infrastrukturen angeregt, die ex post eine Überwachung der eingesetzten Technik ermöglichen und durch die Compliance eingefordert werden kann.[8]
- Das Weiße Haus hat in den USA ebenfalls zum Thema KI Regulierung Stellung genommen. Im Oktober 2022 hat es einen nicht rechtsverbindlichen „Blueprint" für eine KI-Rechtsverordnung vorgelegt, die sogenannte *AI Bill of Rights*. Fünf Bundesbehörden haben in Folge bereits Leitfäden für einen verantwortlichen Einsatz von KI-Systemen in ihren eigenen Arbeits- und Verwaltungsabläufen vorgelegt. Andere haben verbindliche Richtlinien für in

[6] Pudur, Arun, Linked In (Januar 2023): How Woke is ChatGPT?, https://www.linkedin.com/posts/arunpudur_chatgpt-activity-7018419857289330688-8YEe/?utm_source=share&utm_medium=member_ios (zuletzt aufgerufen am 28.02.2023)

[7] New York Times (17.02.2023): Why a conversation with Bing's Chatbot left me deeply unsettled, https://www.nytimes.com/2023/02/16/technology/bing-chatbot-microsoft-chatgpt.html (zuletzt aufgerufen am 28.02.2023)

[8] 117th Congress Public Law 207 [From the U.S. Government Publishing Office], https://www.congress.gov/bill/117th-congress/house-bill/6580/text (zuletzt aufgerufen am 28.02.2023) *sowie* Mökander, Jakob et.al. (18.08.2022): The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other?, https://link.springer.com/article/10.1007/s11023-022-09612-y) *sowie* Andrae, Silvio, RiskNet (07.12.2022): Ein Stück in mehreren Akten, https://www.risknet.de/themen/risknews/ein-stueck-in-mehreren-akten/(alle zuletzt aufgerufen am 07.02.2023)

ihrem Geschäftsbereich liegende Branchen herausgegeben, wie z.B. für die Food and Drug Administration bei der Überwachung der Entwicklung und Zulassung medizinischer Geräte.[9]

- Die kanadische Regierung hat im Juni 2022 den *Artificial Intelligence and Data Act* (AIDA) als Teil einer grundlegenden Reform des Datenschutzrechts und angrenzender Rechtsgebiete ins Parlament eingebracht. Zentrales Ziel ist der Schutz der Verbraucher:innen im digitalen Raum oder beim Einsatz von KI-Systemen im privaten Sektor, insbesondere dem internationalen Handel. Neben gesetzlichen Regeln, die eine Verpflichtung zu Risikobewertungen oder Aufzeichnungspflichten beinhalten, sieht AIDA auch Konformitätsprüfungen und Notifizierungsverfahren vor und operiert mit der Unterscheidung verschiedener Hochrisikoanwendungen.[10]

Auch in internationalen Organisationen wird an Leitlinien und Kriterien gearbeitet, die nicht nur die Interoperabilität der Systeme weltweit gewährleisten und so den globalen Handel von KI-Systemen ermöglichen sollen, sondern menschen- und rechtsstaatliche Prinzipien in den Mittelpunkt der Debatte rücken:

- Im November 2021 hat die Organisation der Vereinten Nationen für Bildung, Wissenschaft, Kultur und Kommunikation (UNESCO) den ersten global verhandelten Völkerrechtstext zur Ethik Künstlicher Intelligenz vorgelegt, der konkrete Empfehlungen zur globalen KI-Normung enthält.[11]
- Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) hat ein breites Netzwerk an Expert:innen aufgebaut und mit seinen *OECD AI Principles* Leitlinien für eine menschenrechtszentrierte, vertrauensvolle KI erarbeitet.[12]

---

[9] The White House (Oktober 2022): Blueprint for an AI Bill of Rights: Making Automated Systems work for the American People, https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf (zuletzt aufgerufen am 07.02.2023) *sowie*
Turner Lee, Nicol/Malamud, Jack, BROOKINGS (19.12.2022): Opportunities and blind spots in the White House's blueprint for an AI Bill of Rights, https://www.brookings.edu/blog/techtank/2022/12/19/opportunities-and-blind-spots-in-the-white-houses-blueprint-for-an-ai-bill-of-rights/ (zuletzt aufgerufen am 28.02.2023)

[10] Government of Canada (16.06.2022): New laws to strengthen Canadians' privacy protection and trust in the digital economy, https://www.canada.ca/en/innovation-science-economic-development/news/2022/06/new-laws-to-strengthen-canadians-privacy-protection-and-trust-in-the-digital-economy.html (zuletzt aufgerufen am 07.02.2023) *sowie*
Landry, Kevin et.al. (16.11.2022): Bill C-27 – Canadas proposed Artificial Intelligence and Data Act, https://www.stewartmckelvey.com/thought-leadership/bill-c-27-canadas-proposed-artificial-intelligence-and-data-act/ (zuletzt aufgerufen am 07.02.2023) *sowie*
Kardash, Adam (30.01.2023): The proposed Artificial Intelligence and Data Act: A Roundtable Discussion, https://www.osler.com/en/resources/regulations/2023/the-proposed-artificial-intelligence-and-data-act-a-roundtable-discussion (zuletzt aufgerufen am 28.02.2023)

[11] UNESCO [65282] (2021): Recommendation on the Ethics of Artificial Intelligence, https://unesdoc.unesco.org/ark:/48223/pf0000380455 (zuletzt aufgerufen am 28.02.2023) *sowie*
Deutsche UNESCO Kommission (2022): UNESCO Empfehlung zur Ethik Künstlicher Intelligenz: Bedingungen zur Implementierung in Deutschland, https://www.unesco.de/sites/default/files/2022-03/DUK_Broschuere_KI-Empfehlung_DS_web_final.pdf (zuletzt aufgerufen am 28.02.2023)

[12] OECD/LEGAL/0049 (2019): Recommendation of the Council on Artificial Intelligence, https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf (zuletzt aufgerufen am 28.02.2023) *sowie*
OECD Library (28.06.2021): Tools for trustworthy AI: A framework to compare implementation tools for

- Die International Standard Organization (ISO) arbeitet an verschiedenen Normen zu Datenqualität und KI-Managementsystemen, die Grundlage für weitergehende Normungsüberlegungen auch in Deutschland sind.[13]

Nicht alle dieser Regulierungsansätze oder Normierungsvorschläge orientieren sich gleichermaßen an den Prinzipien von Rechtsstaatlichkeit und Demokratie. Gerade die Aktivitäten auf internationaler Ebene entfalten zudem in der Regel keine unmittelbare Rechtsverbindlichkeit. Ihnen ist aber gemeinsam, dass der Versuch unternommen wird, Leitplanken für die Nutzung von KI-Systemen zu etablieren und die verschiedenen Akteure innerhalb der KI-Ökosysteme, von Entwickler:innen bis hin zu Anwender:innen, auf diese zu verpflichten. Den meisten dieser Vorschläge liegt damit die Idee einer *Responsible Artificial Intelligence* (RAI), also der gesellschaftlich verantwortliche, ethische Einsatz Künstlicher Intelligenz, zu Grunde.[14] Konkret geht es dabei in der Regel um immer ähnliche Aspekte, die als Leitplanken für einen ethisch korrekten und verantwortungsvollen Einsatz von KI gesehen werden und die im Wesentlichen auf der Anwendbarkeit zentraler Menschenrechte basieren, sowie anschlussfähig sind an die Regeln der EU-Grundrechtecharta und – in der deutschen Debatte – an die aus dem Grundgesetz abgeleiteten Ansprüche an Grund- und Bürger:innenrechte.

2. Die KI-Verordnung der Europäischen Union (KI-Act)

Die Europäische Kommission geht mit ihrem Verordnungsentwurf zur Regulierung Künstlicher Intelligenz[15][16] einen deutlichen Schritt weiter als bisherige internationale Bemühungen und knüpft an die Überlegungen der von ihr eingesetzten Expert:innengruppe an, die 2019 als unabhängige High-Level

trustworthy AI systems, https://www.oecd-ilibrary.org/science-and-technology/tools-for-trustworthy-ai_008232ec-en;jsessionid=_bzOpvJmXfRtEFR1A6FlrlH2g1d1Cugto4ItiKl2.ip-10-240-5-61 (zuletzt aufgerufen am 28.02.2023)

[13] Bundesministerium für Wirtschaft und Energie (Dezember 2022): Deutsche Normungsroadmap Künstliche Intelligenz Ausgabe 2, https://www.dke.de/resource/blob/2008010/776dd87a4b9ec18d4ab295025ccbb722/nr-ki-deutsch---download-data.pdf (zuletzt aufgerufen am 28.02.2023)

[14] Für eine ausführlichere Darstellung des Konzepts vgl. Kapitel 3 der vorliegenden Studie.

[15] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION, Brüssel, 21.04.2021, COM (2021) 206 final unter: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_1&format=PDF (zuletzt aufgerufen am 28.02.2023) *sowie*
Anhänge des Vorschlages für eine Verordnung des Europäischen Parlamentes und des Rates ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_2&format=PDF (zuletzt aufgerufen am 28.02.2023)

[16] Sofern spezifisch auf einzelne Artikel des EU-Kommissionentwurfs vom 21.4.2021 Bezug genommen wird, wird dieser als KI-Act Entwurf abgekürzt, ist allgemein von der zu erwartenden Regulierung durch eine europäische Verordnung die Rede, wird auf den KI-Act Bezug genommen.

Expert Group on Artificial Intelligence Vorschläge zum verantwortlichen Einsatz von KI formuliert hat.[17] Sie unternimmt mit ihrer Vorlage des Verordnungsentwurfes vom 21. April 2021 den Versuch, ethische Standards für eine vertrauenswürdige KI in einem für alle Mitgliedstaaten verbindlichen Rechtstext zu formalisieren und normativ zu beschreiben. Der Entwurf des KI-Acts richtet sich dabei an alle relevanten Akteure entlang der Wertschöpfungskette, so z.B. an Entwickler:innen und Hersteller:innen von KI-Systemen, an Händler:innen, an Anwender:innen und Nutzer:innen wie auch an diejenigen, die die von ihnen eingesetzte KI weiterentwickeln. Er gilt sowohl für den privaten als auch öffentlichen Sektor und sieht je nach konkreter Ausgestaltung des KI-Systems und der spezifischen Rolle der handelnden Akteure unterschiedliche Pflichten vor. Zentral ist den Vorschlägen der EU-Kommission dabei die Orientierung an einem risikobasierten Ansatz, der vor allem zum Ziel hat, die Grundrechte der Bürger:innen der EU zu schützen und zu gewährleisten, dass nur vertrauensvolle KI-Systeme in Europa zum Einsatz kommen.

2.1 Die Risikokategorien nach KI-Act[18]

Der KI-Act verfolgt einen risikobasierten Ansatz, nach dem KI-Anwendungen, die potentiell negative Auswirkungen auf Gesundheit, Sicherheit oder Freiheit haben, stärkere regulatorische Anforderungen erfüllen müssen. Für Hamburger KMU bedeutet dies zunächst ein gewisses Maß an Unsicherheit dahingehend, in welche der durch den KI-Act vorgegebenen vier Risikoklassen ihre KI-Lösungen einzuordnen sind. Es sprechen jedoch diverse Gründe dafür, sich allgemein an den höheren Anforderungen zu orientieren, selbst wenn die Risikoeinstufung der eigenen Anwendungsfälle dieses nach KI-Act nicht zwingend erforderlich macht.

Die von der EU-Kommission vorgeschlagenen Maßnahmen richten sich zentral auf die Förderung des Vertrauens der Bürger:innen in KI-Anwendungen, indem sie den Menschen, sein Recht auf Privatsphäre und Datenschutz, sein Recht auf Nichtdiskriminierung und Rechtssicherheit, in den Mittelpunkt rücken. Deswegen werden im Verordnungsentwurf gerade an solche Systeme besonders strenge regulatorische Vorgaben formuliert, die ein hohes Risiko für Gesundheit, Sicherheit oder Freiheit darstellen. Ihnen gebührt vor dem Hintergrund des Grundrechtsschutzes besondere Aufmerksamkeit. Um gerade in grundrechts- und sicherheitssensiblen Bereichen Risiken zu minimieren, werden daher im KI-Act KI-Systeme in drei Risikogruppen (plus eine Gruppe ohne Risikopotential) klassifiziert, bei denen weniger von Bedeutung ist, wie ein einzelner Algorithmus konkret formuliert ist, sondern vielmehr in welcher Form und in welchem Kontext er zur Anwendung kommen soll und/oder inwieweit die bestimmungsgemäße Nutzung der KI durch die Entwickler:innen auf den originären Zweck eingeschränkt wird:

1. Verboten nach Titel II Art. 5 KI-Act-Entwurf:
    a. Unterschwellige Beeinflussung des Verhaltens einer Person
    b. Ausnutzung von Schwäche/Schutzbedürftigkeit bestimmter Personen(-gruppen) aufgrund von Alter/Behinderung
    c. Soziale Bewertung von Personen (durch/im Auftrag von Behörden)

[17] European Commission / Independent High-Level Expert Group on Artificial Intelligence (08.04.2019): Ethics Guidelines for Trustworthy AI, https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html (zuletzt aufgerufen am 28.02.2023)

[18] Grundlage dieses Kapitels stellt die Auseinandersetzung mit dem Gesetzesentwurf der Europäischen Kommission vom 21.04.2021 dar.

   d. Biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken [Ausnahmen]
2. Hohes Risiko nach Titel III Art. 6-51, Anhang II & III KI-Act Entwurf
   a. Hochrisiko-KI nach EU-Harmonisierungsvorschriften (Anhang II)
      i. Produkte und Sicherheitskomponenten von Produkten, die unter die in Anhang II aufgelisteten EU-Harmonisierungsvorschriften fallen
   b. Hochrisiko-KI nach Anwendungskontext (Anhang III)
      i. Biometrische Identifizierung (verordnungskonforme Echtzeit- bzw. nachträgliche Fernidentifizierung)
      ii. Betrieb kritischer Infrastrukturen (z.B. Gas-, Wasser- und Stromversorgung)
      iii. Bildung (Zugang und Bewertungssysteme)
      iv. Beschäftigung, Personal (Recruiting und Leistungsbeurteilung)
      v. Private und öffentliche Dienste (Kreditprüfung, Zugang zu Sozialleistungen)
      vi. Strafverfolgung (Risikobewertung und Profiling)
      vii. Migration und Asyl (Antrags- und Statusprüfungen)
      viii. Rechtspflege (Rechtsanwendungen, Bewertungen von Sachverhalten)
3. geringes Risiko
   a. z.B. Chatbots[19], Deepfakes
4. Kein Risiko
   a. z.B. KI-gestützte Videospiele, Spamfilter

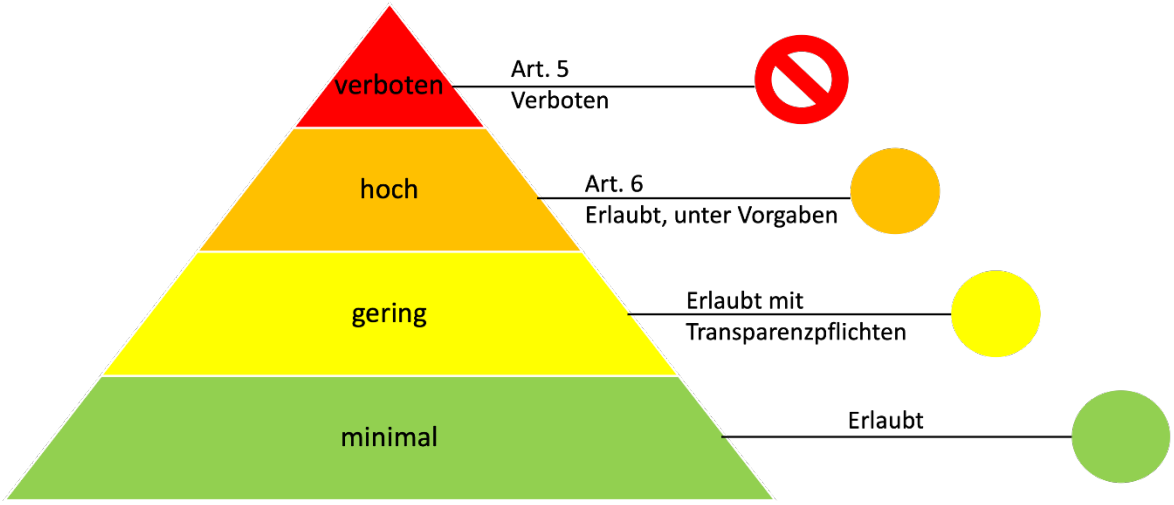


Abb.1.: Eigene Darstellung: Der risikobasierte Ansatz nach KI-Act Entwurf

Innerhalb der Hochrisiko-Kategorie gibt es zwei mögliche Ursachen für die Einschätzung, dass der KI-Einsatz als hochriskant zu werten ist. Neben den oben aufgelisteten Anwendungskontexten nach Anhang III KI-Act Entwurf sind demnach außerdem Produkte oder Sicherheitskomponenten von Produkten, die

[19] An der Einordnung von Chatbots als ”geringes Risiko“ im Kommissionsentwurf lässt sich die Problematik der derart kategorisierten Risikoklassen bereits gut erkennen. Der Rat der Europäischen Union reagierte darauf, indem er Allgemeinzweck-KI, zu der Chatbots wie Chat GPT zählen würden, ausdrücklich in die Verordnung aufnimmt und auf ihren kontextabhängigen Einsatz hinweist, siehe hierzu auch die weiteren Ausführungen unter 2.1 sowie 2.2 sowie die eingangs genannten Beispiele.

Produktsicherheitsvorschriften in Form von EU-Harmonisierungsvorschriften unterliegen, als Hochrisiko-KI einzustufen. Dies betrifft beispielsweise Maschinen, Spielzeug, Aufzüge, Seilbahnen etc., gemäß Anhang II KI-Act Entwurf. Anbieter:innen von Systemen, die nach dieser Systematik als Hochrisiko-KI einzustufen sind, sind verpflichtet, die hohen Anforderungen des neuen Regelwerks grundsätzlich zu erfüllen, will man Sanktionen in Form von hohen Geldbußen oder Vertriebsverboten umgehen (Art. 71 und Art. 84 KI-Act Entwurf). Zusätzlich zu den Harmonisierungsvorschriften und Anwendungskontexten kann nach dem Kompromisstext des Rates Allgemeinzweck-KI höheren Anforderungen unterliegen (Art. 4 KI-Act Ratsentwurf). KI-Systeme mit allgemeinem Verwendungszweck sind dabei solche KI-Systeme, die von Anbieter:innen dazu vorgesehen sind, allgemein anwendbare Funktionen (z.B. Bild- oder Spracherkennung, Audio- und Videogenerierung, Mustererkennung, Beantwortung von Fragen und Übersetzung) auszuführen.[20]

Für Hamburger KMU wird die Abgrenzung dieser Risikogruppen von größter Relevanz sein, denn sie müssen in Zukunft in der Lage sein, KI-Anwendungen, die sie entwickeln, vertreiben oder selbst nutzen, korrekt in die oben genannten Risikokategorien einsortieren zu können, um die gesetzlich geforderten Anforderungen dementsprechend erfüllen zu können. Darüber hinaus kann die Bedeutung des jeweiligen Anwendungskontextes eines KI-Systems kaum genug betont werden. So adressiert der Verordnungsentwurf sowohl in der Version der Kommission als auch des Rates zwar zentral die Anforderungen an Hochrisiko-KI-Systeme, wann jedoch ein System in diese Zuordnung fällt, bleibt kontextabhängig und kaum allgemeingültig adressierbar. Die oben aufgeführte Auflistung wird somit stets von der Prüfung des Einzelfalls abhängen und dient lediglich – auch abgesehen von der im Detail noch offenen Definition und Abgrenzung der einzelnen Bereiche im Zuge der politischen Verhandlungen – als grobe Orientierung. Diese kontextbasierte, einzelfallabhängige Einordnung in Risikoklassen lässt somit einige Fragen offen und kann bei Unternehmen Unsicherheit hervorrufen. Die Frage, welche Anforderungen sie nun erfüllen müssen, wird durch die Hinzunahme von Allgemeinzweck-KI in der Ministerratsvorlage umso zentraler.

Obwohl diese Unschärfe bzw. der Interpretationsspielraum, der bei der Einordnung in die Risikoklassen bleibt, Unternehmen verunsichern kann, ist der Ansatz aus demokratischer und rechtsstaatlicher Perspektive zweckdienlich. Das hinter dem risikobasierten Ansatz stehende Ziel des Gesetzgebers liegt darin, Risiken für Gesundheit, Sicherheit und Freiheit zu minimieren. Ob der Einsatz eines KI-Systems eine Gefahr für die Gesundheit, Sicherheit oder Freiheit von Bürger:innen darstellen kann, lässt sich jedoch nicht anhand des verwendeten Lernverfahrens, eines spezifischen Algorithmus oder danach, ob es sich um daten- oder wissensbasierte KI handelt, einschätzen. So kann beispielsweise das Lernverfahren des Reinforcement Learning (s. Glossar) verwendet werden, um einer KI beizubringen, wie man ein Level eines Videospiels absolviert oder wie sich ein selbstfahrendes Auto in einer Verkehrssituation orientiert. Würde die Einstufung in eine Risikokategorie anhand spezifischer Algorithmen oder Lernverfahren, wie z.B. Reinforcement Learning, erfolgen, wäre dies zwar mit weniger Unsicherheit für Unternehmen verbunden, gleichzeitig würde aber das gleiche Anforderungsmaß für KI-Systeme vorgeschrieben werden, die im Fall

[20] Rat der Europäischen Union (25.11.2022): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union: Allgemeine Ausrichtung, https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/de/pdf (zuletzt aufgerufen am 28.02.2023)

einer Fehlfunktion entweder in einem Videospiel verlieren oder potentiell Menschenleben in einem Verkehrsunfall kosten.

Analog zum kontextabhängigen Risiko für die Sicherheit gibt auch die Frage, wie stark der Einsatz der KI in die Grundrechte der Nutzer:innen eingreift, Anlass für unterschiedliche Anforderungsniveaus: Denn ob ein Chatbot beispielsweise tatsächlich pauschal in die Kategorie „geringes Risiko" fallen sollte, wird letztlich davon abhängen, was seine Aufgabe ist. Ein Chatbot, der in der Kund:innenberatung eines Onlinehändlers eingesetzt wird, erfordert voraussichtlich andere Voraussetzungen als beispielsweise ein Chatbot, der Zugang zu staatlichen Leistungen bietet. Der hieraus möglicherweise entstehenden Verunsicherung von Unternehmen stehen also durchaus gewichtige demokratische und rechtsstaatliche Gründe gegenüber. Um weder das Vertrauen der Bürger:innen zu riskieren, noch innovationshemmende Unsicherheit bei KMU auszulösen, sind unterstützende Angebote zur Einordnung in die Risikokategorien (z.B. in Form von Checklisten, Kurzberatung o.ä.) geboten. Dies sieht auch der europäische Gesetzgeber so, wenn er auf die Einrichtung notwendiger Unterstützungsleistungen bei der Umsetzung der Verordnung insbesondere für KMU hinweist.[21]

Zudem gibt es einige Gründe, die dafürsprechen können, die Anforderungen im Sinne der RAI im Allgemeinen, also nicht nur, wenn es aufgrund der Einsortierung als Hochrisiko-KI zwingend notwendig ist, anzustreben: Zum einen wird im KI-Act wiederholt die Empfehlung nach Verhaltenskodizes hervorgehoben (Art. 69 KI-Act Entwurf), mit denen sich auch alle anderen KI-Anbieter:innen im europäischen Binnenmarkt an die wesentlichen Anforderungen des KI-Acts binden würden und nach den Vorstellungen der EU-Kommission auch binden sollten. Es kann aber auch im unmittelbaren Unternehmensinteresse liegen, nicht nur das jeweilige Mindestmaß an gesetzlich vorgeschriebenen Anforderungen zu erfüllen. Will sich ein Marktakteur etwa verschiedene mögliche Anwendungsfelder seiner Entwicklung offenhalten, bietet es sich schon aus diesem Grund an, die im KI-Act genannten Anforderungen an Transparenz, Nachvollziehbarkeit oder notwendige Governance-Strukturen – auf die im Weiteren genauer eingegangen werden wird – grundsätzlich zu implementieren. Aber selbst wenn das KI-System nur für einen klar definierten Einsatzkontext entwickelt werden soll und dieser nach jetzigem Stand nicht in den Hochrisikobereich fällt, besteht die Chance, dass dieser Einsatzkontext durch einen Durchsetzungsrechtsakt zu einem späteren Zeitpunkt als hochriskant definiert wird. Die Anforderungen nachträglich in einem bestehenden KI-System umzusetzen, kann sehr aufwändig oder in manchen Fällen nicht realisierbar sein.

Schließlich können auch die Erwartungen und Ansprüche der Kund:innen Unternehmen dazu bewegen, auch ohne gesetzliche Verbindlichkeit RAI-Kriterien zu erfüllen. So kann analog zu anderen Geschäftsmodellen durchaus begründet davon ausgegangen werden, dass die Ansprüche von Nutzer:innen an ein gesellschaftlich verantwortliches Produkt gestiegen sind und sich auch auf die Nutzung und Anwendung von KI-Lösungen übertragen lassen. Es kann also durchaus im Interesse von Unternehmen sein – neben der ökonomisch getriebenen Vermeidung von Haftungsrisiken –, die Vertrauenswürdigkeit ihrer KI durch eine Konformitätserklärung und die Einhaltung bestimmter Regeln und Normen zu belegen. Schlussendlich ist nicht auszuschließen, dass eine die Vertrauenswürdigkeit des Systems belegende CE-Kennzeichnung in der Europäischen Union nicht nur ein Wettbewerbsvorteil werden kann, sondern eine faktische Voraussetzung, um im Binnenmarkt konkurrenzfähig zu bleiben.

[21] Siehe hierzu die Ausführungen in Kapitel 5.1 der vorliegenden Studie sowie insbesondere Art. 55 KI-Act Entwurf.

Selbst ohne einen unmittelbaren Bezug auf verbindliche Normen ist es also aus oben genannten Gründen auch für andere Anbieter:innen unter bestimmten Umständen sinnvoll, sich nicht nur mit dem technischen Möglichen und dem rechtlich Verbindlichen auseinanderzusetzen, sondern auch das ethisch Wünschenswerte und normativ Gebotene im Blick zu behalten.

2.2 Aktueller Diskussionsstand im Europäischen Parlament und im Rat der Europäischen Union

Der KI-Act wird nach dem Ordentlichen Gesetzgebungsverfahren der EU (COD) verabschiedet, in dem das Europäische Parlament und der Rat der EU als gleichberechtigte Gesetzgeber auf der Grundlage eines Gesetzesentwurfes durch die Europäische Kommission auftreten. Zum Redaktionsschluss dieser Studie befindet sich das Gesetzgebungsverfahren noch im Fluss und die dargestellten Inhalte stehen somit unter Vorbehalt. Im Folgenden werden wesentliche inhaltliche Streitpunkte zwischen den an der Gesetzgebung beteiligten Institutionen thematisiert, die u.a. die Definition von KI, den Anwendungsbereich des KI-Acts und den Zuschnitt der Hochrisikokategorie betreffen.

Seitdem der erste Entwurf des KI-Acts durch die Europäische Kommission im April 2021 veröffentlicht wurde (KI-Act Entwurf), läuft das Gesetzgebungsverfahren unter Einbeziehung der Stellungnahmen und Kompromissvorschläge der Mitgliedstaaten im Rat für Telekommunikation sowie im Europäischen Parlament überwiegend in den Ausschüssen für „Internal Market and Consumer Protection“ (IMCO) und „Civil Liberties, Justice and Home Affairs“ (LIBE). Im Oktober 2022 gab es eine erste Plenardebatte im Europäischen Parlament, in der zunächst ein Fokus auf die technischen Fragen des Verordnungsentwurfs gelegt wurde, um schwierigere politische Klärungsbedarfe zu einem späteren Zeitpunkt bearbeiten zu können. Während der Rat sich im Dezember 2022 auf einen gemeinsamen Standpunkt („Allgemeine Ausrichtung”) geeinigt hat, steht eine Einigung des Europäischen Parlaments zum Redaktionsschluss der Studie noch aus.[22][23]

In Anbetracht der schwierigen und komplexen Materie haben die verschiedenen an der Rechtssetzung der EU beteiligten Organe durchaus kontroverse und voneinander abweichende Vorstellungen über den Regulierungsgehalt und Regulierungsumfang des neuen KI-Acts. Der auf Grundlage des Vorschlages der tschechischen Ratspräsidentschaft vorgelegte gemeinsame Standpunkt des Ministerrats behält zwar wesentliche Teile des Kommissionsvorschlages bei, formuliert aber auch zahlreiche Änderungen, die nun als Basis für die interinstitutionellen Verhandlungen mit dem Europäischen Parlament und der Europäischen Kommission im Rahmen der anstehenden Trilog-Verhandlungen dienen werden. Einzelne Mitgliedstaaten, darunter auch die Bundesrepublik Deutschland, haben zudem nach wie vor Bedenken geäußert und diese noch nach Vorlage des gemeinsamen Standpunkts über Protokollnotizen der EU zur Kenntnis gegeben.[24]

[22] Rat der Europäischen Union (25.11.2022): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union: Allgemeine Ausrichtung, https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/de/pdf (zuletzt aufgerufen am 28.02.2023)

[23] Im Folgenden wird der Ratsbeschluss vom 25.11.2022 als KI-Act Ratsentwurf abgekürzt.

[24] Rat der Europäischen Union (25.11.2022): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und

Davon unbenommen beziehen sich die von den Mitgliedstaaten eingebrachten Änderungsbedarfe gegenüber dem Kommissionsentwurf bereits auf den Kerngehalt der Verordnung: auf die grundlegende Definition von KI-Systemen. Vorausgegangen war eine Auseinandersetzung unter den Mitgliedstaaten, dass der ursprüngliche Entwurf der Kommission ein zu breites Verständnis von KI zugrunde legen würde, nach dem potentiell alle Softwarelösungen im europäischen Binnenmarkt von den Anforderungen der Verordnung erfasst worden wären. In dem Bestreben den Begriff enger zu fassen, schlägt der Rat vor, nur Systeme in den Anwendungsbereich der Verordnung zu nehmen, die Maschinelles Lernen oder logik- sowie wissensbasierte Methoden verwenden und somit Such-, Schätz- und Optimierungsmethoden als KI-Technologien zu streichen (Art. 3 KI-Act Ratsentwurf). Zudem wird die Eigenschaft der Autonomie zur weiteren Abgrenzung von klassischer Software benannt.

zur Änderung bestimmter Rechtsakte der Union: Allgemeine Ausrichtung- *Erklärung Deutschlands,* https://data.consilium.europa.eu/doc/document/ST-14954-2022-ADD-1/de/pdf (zuletzt aufgerufen am 28.02.2023)

Kommissionsentwurf (KI-Act Entwurf)	Kompromisstext des Rates (KI-Act Ratsentwurf)
„System der künstlichen Intelligenz“ (KI-System) eine Software, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren”	„System der künstlichen Intelligenz“ (KI-System) ein System, das so konzipiert ist, dass es mit Elementen der Autonomie arbeitet, und das auf der Grundlage maschineller und/oder vom Menschen erzeugter Daten und Eingaben durch maschinelles Lernen und/oder logik- und wissensgestützte Konzepte ableitet, wie eine Reihe von Zielen erreicht wird, und systemgenerierte Ergebnisse wie Inhalte (generative KI-Systeme), Vorhersagen, Empfehlungen oder Entscheidungen hervorbringt, die das Umfeld beeinflussen, mit dem die KI-Systeme interagieren”

Neben der Definition von KI wird im Kompromisstext des Rates auch der Anwendungsbereich des KI-Acts angepasst: KI-Systeme, die ausschließlich zur wissenschaftlichen Forschung und Entwicklung eingesetzt werden, wären demnach vom Anwendungsbereich der Verordnung ausgenommen. Zudem würden private Nutzende (natürliche Personen, die KI zu ausschließlich privaten, nicht beruflichen Tätigkeiten verwenden) von den Pflichten unter der Verordnung befreit (Art. 2 Abs. 6-8 KI-Act Ratsentwurf).

Schließlich sieht der Rat wesentliche Änderungen in Bezug auf die Hochrisikokategorie vor. Welche Anwendungen als hochriskant einzustufen seien, wurde lange zwischen den Mitgliedstaaten diskutiert. Wie oben beschrieben werden diese Systeme besonders strengen Anforderungen unterliegen und es ist daher für Entwickler:innen und Anbieter:innen von allergrößter Bedeutung, klar definieren zu können, ob sie rechtlich mit ihren Anwendungen in die Klassifizierung „Hochrisiko” fallen. Erst dies ermöglicht eine verbindliche Einschätzung, welche Anforderungen auf sie zukommen. In dem Versuch hier mehr Klarheit zu schaffen, weicht der Ministerrat in seinem Standpunkt vom Kommissionsvorschlag ab, indem er in Bezug auf die in Anhang III KI-Act Entwurf genannten Anwendungskontexte eine horizontale Bewertungsebene bei der Klassifizierung von Hochrisiko-Systemen hinzufügt, die gewährleisten soll, dass KI-Systeme, die wahrscheinlich kein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte darstellen, von der Verordnung nicht erfasst werden. Rat und Kommission wollen also keine pauschale sektorielle oder branchenspezifische Regulierung, wie sie beispielsweise in den USA angestrebt wird, sondern eine klare horizontale Regelung entlang von Risikobewertungen und Risikokategorien.[25]

Für Systeme, die unter diesen Bedingungen noch in die Hochrisikokategorie fallen würden, wurden die Anforderungen zudem dahingehend präzisiert, dass sie insbesondere KMU nicht über Gebühr belasten dürfen (siehe dazu auch Abschnitt 5.1 der vorliegenden Studie). Vor allem sollten nach Vorstellung des Rates die Zuständigkeiten und die Abgrenzung von Verantwortungsbereichen im Entwicklungs- und Implementierungsprozess klarer gefasst werden. Außerdem soll der risikobasierte Ansatz aus Sicht des

[25] Kap. 1: Kontext des Vorschlages KI-Act Entwurf

Rates – wie oben bereits erwähnt – auch für die sogenannte Allgemeinzweck-KI gelten, für die in einem gesonderten Durchführungsrechtsakt definiert werden soll, wann sie die Anforderungen für Hochrisiko-Systeme erfüllen müssen. Sollte sich die Ausweitung der Hochrisikoeinstufung auf Allgemeinzweck-KI im weiteren Verlauf der Verhandlungen durchsetzen, könnten von den Anforderungen an Hochrisiko-Systeme eine Vielzahl von Entwickler:innen betroffen sein (Art. 12 c) KI-Act Ratsentwurf). Diese Regelung würde dann nicht nur für alle Systeme gelten, die selber in die Hochrisiko-Kategorie fallen, sondern auch für solche, die mit ihren Funktionen lediglich in ein Produkt integriert sind, das erhöhten Sicherheitsstandards genügen muss, auch wenn die KI selbst nur als Teilsystem allgemeine Funktionen ausführt, wie Bild-, Sprach-, Texterkennung, Video- und Audioproduktion, Mustererkennung, Fragenbeantwortung oder Übersetzungen. Den entsprechenden Anbieter:innen solcher Systeme schon vor Inkrafttreten des Gesetzes einen Handlungsleitfaden zu bieten, stellt sich aktuell als schwierig bis unmöglich dar, da erst ein Jahr nach Inkrafttreten der Verordnung detaillierte Vorgaben entstehen sollen, wie genau mit der Definition von Allgemeinzweck-KI umgegangen werden soll und wann der Einfluss der Anwendung einer Allgemeinzweck-KI als so unwesentlich verstanden werden kann, dass die Anforderungen an Hochrisikosysteme nicht gelten.

Neben weiteren konkretisierenden Zuspitzungen zu Bereichen wie dem Gesundheitssektor, der Echtzeit-Fernidentifizierung zu Strafverfolgungszwecken oder der Nutzung von sozialen Bewertungssystemen würde nach Maßgabe des Rates die Anwendung des KI-Acts zudem auf privatwirtschaftliche Akteure ausgeweitet werden.

Mit dem vorliegenden Entwurf der Kommission sowie dem gemeinsamen Standpunkt des Rates haben zwei der drei am Gesetzgebungsprozess beteiligten Akteure ihre Position zur Regulierung von KI-Anwendungen in der EU vorgelegt. Vor dem Hintergrund dieser zum Teil divergierenden Vorschläge bleibt es spannend, wie der weitere Gesetzgebungsprozess verläuft. Im nächsten Schritt wird das Europäische Parlament seinen Vorschlag abstimmen, bevor im Rahmen der Trilog-Verhandlungen eine gemeinsame Regelung gefunden werden kann. Dieser Prozess kann sich noch bis in die Mitte des Jahres 2023 oder darüber hinaus hinziehen. Die Verordnung soll in Folge nach gegenwärtigem Stand am zwanzigsten Tag nach ihrer Veröffentlichung in Kraft treten und ist dann – abgesehen von einigen Ausnahmen – als unmittelbar geltendes Recht in den Mitgliedstaaten der Europäischen Union ab dem 24. Monat nach Inkrafttreten gültig (Art. 85 KI-Act Entwurf).

2.3 Institutionelle Akteure, Konformitätsbewertungen und Notifizierungen nach KI-Act

Der KI-Act wird mit Inkrafttreten auch die behördlichen Zuständigkeiten und Strukturen regeln. Obwohl aktuell noch unklar ist, wie diese Aufsichtsstruktur in Deutschland konkret aussehen wird, ist klar, dass eine Zertifizierung der Produkte für viele Akteure an Bedeutung gewinnen wird und sich KMU, die eine Hochrisiko-KI nutzen oder anbieten, einer Konformitätsprüfung unterziehen müssen.

Neben der Entwicklung eines umfassenden Rechtsrahmens mit Verpflichtungen für Entwickler:innen und Anwender:innen wird darüber hinaus auch institutionell an dem Ausbau für die Aufsicht und die Durchsetzung des sich entwickelnden Regelwerks gearbeitet. Innerhalb der EU sind entsprechende Überlegungen bereits recht weit fortgeschritten. Denn die KI-Verordnung sieht neben konkret formulierten Anforderungen an Entwickler:innen, Anbieter:innen und Nutzer:innen für die Gestaltung und Funktionsfähigkeit eines Algorithmus ein System von Konformitätsprüfungen, Notifizierungen sowie Registrierungen vor, um zumindest bei KI-Systemen mit hohem Risiko den gesamten Lebenszyklus vom Inverkehrbringen bis zum Einsatz in der Praxis dauerhaft im Blick zu behalten.

- So haben die drei europäischen Normungsinstitutionen – das Europäische Komitee für Normung (CEN), das Europäische Komitee für elektrotechnische Normung (CENELEC) sowie das Europäische Institut für Telekommunikationsnormen (ETSI) – von der Europäischen Kommission den Auftrag bekommen, nicht nur Prüfverfahren und Prüfmethoden für KI-Systeme und Risikomanagement-Systeme zu entwickeln, sondern auch konkrete technische Normen, bei deren Anwendung durch Unternehmen davon ausgegangen wird, dass die entwickelten KI-Systeme als konform mit den EU-Regeln gelten können.[26]
- Zugleich wird an dem Aufbau einer Datenbank gearbeitet, in der sich Anbieter:innen einer Hochrisiko-KI-Lösung laut Art. 51 KI-Act Entwurf werden registrieren lassen müssen. Die Pflicht zur Registrierung soll nach dem Kompromissvorschlag des Rates vom Dezember 2022 nicht nur für Hersteller:innen und Anbieter:innen von Hochrisiko-KI gelten, sondern auch für in öffentlichen Einrichtungen und der Verwaltung eingesetzte KI-Systeme.
- Geplant ist auch ein Europäischer Ausschuss für Künstliche Intelligenz, in dem neben Vertreter:innen der Mitgliedstaaten laut Kompromissvorschlag des Rates in einer ständigen Untergruppe auch unabhängige Vertreter:innen von KMU bzw. Start-ups, Wissenschaftler:innen, Vertreter:innen von Normungsgremien und notifizierten Stellen, Vertreter:innen von Laboren und Test- und Versuchseinrichtungen sowie Organisationen der Zivilgesellschaft vertreten sein sollen (Art. 56 Abs. 3 KI-Act Ratsentwurf). Nach Wunsch des Rates kommt dem KI-Ausschuss darüber hinaus, gemäß Art. 58 KI-Act Ratsentwurf u.a. eine wesentliche Rolle in der Beratung der EU-Kommission bei der dauerhaften Überprüfung der Definition von Hochrisiko-KI nach Anhang III KI Act-Entwurf sowie bei der Formulierung von Durchführungsrechtsakten und praktischen Leitlinien zu. Insbesondere soll der Ausschuss seine Aktivitäten darauf konzentrieren, zu tatsächlich harmonisierten Verfahren in den Mitgliedstaaten in Bezug auf Konformitätsprüfungen und Notifizierungen zu kommen. Durch die Möglichkeit auch selbst initiativ tätig zu werden, so

[26] Bertuzzi, Luca, EURACTIV (30.05.2022): EU-Normungsgremien sollen KI Standards ausarbeiten, https://www.euractiv.de/section/innovation/news/eu-normungsgremien-sollen-ki-standards-ausarbeiten/ (zuletzt aufgerufen am 28.02.2023)

z.B. im Zusammenhang mit der Überprüfung der Definition von Hochrisiko-Systemen nach Anhang III KI-Act Entwurf, würde der Ausschuss über ein hohes Maß an Autonomie verfügen und in der Praxis große Bedeutung in der Governance-Architektur der KI-Verordnung erhalten.[27]

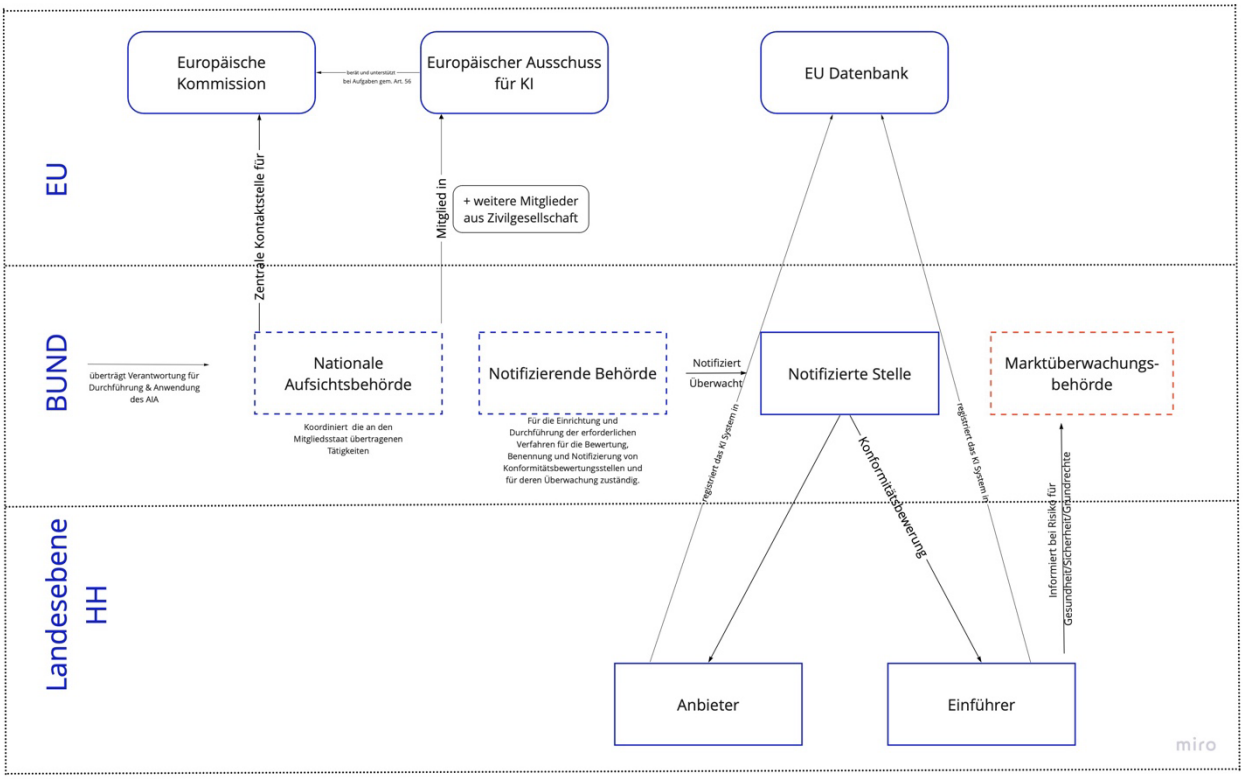
Grundsätzlich gilt also: Wie ein Produkt im europäischen Binnenmarkt zukünftig in Verkehr gebracht werden kann, hängt wesentlich davon ab, ob es in den Bereich der Hochrisiko-KI fällt und um welche Art von Hochrisiko-KI es sich handelt. Auch wenn zum jetzigen Zeitpunkt vieles im Detail noch unklar ist, gibt es generelle Einigkeit darüber, dass insbesondere jedes System mit einer Hochrisiko-KI eine Konformitätsprüfung durchlaufen muss. Aber auch für alle anderen Anbieter:innen wie Anwender:innen kann es gleichermaßen sinnvoll sein, auf eine Prüfung der Einhaltung bestimmter Normen und eine damit einhergehende Konformitätserklärung bzw. CE-Kennzeichnung zu achten. Denn auch Anwender:innen sind z.B. nicht nur darauf angewiesen, dass das ursprüngliche System bestimmten Kriterien entspricht. Bei einer Weiterentwicklung eines KI-Systems, beispielsweise durch weiteres Training mit neuen Daten, können aus Anwender:innen schnell Entwickler:innen werden, die somit ebenfalls selbst zu einer Konformitätsbewertung verpflichtet werden können.

KMU können sich bereits jetzt darauf einstellen, dass in vielen Fällen nach KI-Act Konformitätsprüfungen notwendig werden und eine Registrierung zumindest von Hochrisiko-KI zwingend erforderlich werden wird. Dabei wird sich aller Voraussicht nach die Konformitätsprüfung und damit der Weg zu einer Zertifizierung auf drei mögliche Verfahren konzentrieren:

a) Die Hersteller:innen können die Konformitätsprüfung selbst vornehmen. Dies gilt für eigenständige KI-Systeme, die gemäß Anhang III in den Nummern 2-8 KI-Act Entwurf aufgeführt werden. Hier können die Anbieter:innen selber nach Art. 43 KI-Act Entwurf intern die Konformitätsprüfung übernehmen und die Ergebnisse dann der EU-Datenbank melden (Art. 51 KI-Act Entwurf). Im Anschluss kann die bekannte CE-Kennzeichnung erfolgen. Die Hersteller:innen orientieren sich in diesem Fall an den Anforderungen aus Anhang VI KI-Act Entwurf. Diese beziehen sich im Wesentlichen auf die Einhaltung von Art. 17 KI-Act Entwurf sowie eine Überprüfung der technischen Dokumentation, auch im weiteren Verlauf des Betriebs.
b) Der zweite Weg zu einer Zertifizierung ist durch eine von einer noch nicht definierten Bundesbehörde notifizierte Stelle, einer sogenannten Konformitätsbewertungsstelle. Diese führt anstelle der Hersteller:innen die Prüfung durch und meldet die Systeme ebenfalls der EU-Datenbank. Diese Regelung kommt immer bei KI-Systemen nach Anhang VII KI-Act Entwurf zur Anwendung.
c) Bei (Sicherheitskomponenten von) Produkten, die gemäß Anhang II KI-Act Entwurf, also aufgrund der Tatsache, dass sie europäischen Harmonisierungsregeln unterliegen, als Hochrisiko-KI einzustufen sind, wird das Konformitätsbewertungsverfahren des jeweiligen Rechtsaktes angewandt, wobei KI-spezifische Aspekte im Sinne der Anforderungen aus Kapitel 2 KI-Act Entwurf im Rahmen der bestehenden Verfahren zusätzlich zu prüfen sind.

[27] Bertuzzi, Luca (10.05.2022): KI-Gesetz: Frankreich für Änderungen bei Aufsichtsrat und Marktüberwachung, https://www.euractiv.de/section/innovation/news/ki-gesetz-frankreich-fuer-aenderungen-bei-aufsichtsrat-und-marktueberwachung/ (zuletzt aufgerufen am 28.02.2023) *sowie*
Zech, Maximilian (23.11.2022): So positioniert sich der Rat der EU zum AI Act, https://background.tagesspiegel.de/digitalisierung/so-positioniert-sich-der-rat-der-eu-zum-ai-act (zuletzt aufgerufen am 28.02.2023)

Noch ist unklar, wie die Aufsichtsstruktur rund um den KI-Act konkret aussehen wird. Die oben genannten Verfahren stehen somit unter Vorbehalt der endgültigen Einigung im Rahmen der Trilog-Verhandlungen im EU-Gesetzgebungsverfahren zu Struktur und Zuständigkeiten zwischen den Mitgliedstaaten sowie sich daran anschließenden Entscheidungen auf Bundesebene. Dennoch sind schon jetzt die Überlegungen auf europäischer Ebene zu der begleitenden Aufsichtsstruktur durchaus von praktischer Relevanz für den Mittelstand. Denn der nationalen Aufsichtsbehörde wird in der KI-Governance voraussichtlich eine bedeutende Rolle zukommen. Zumindest im Kommissionsvorschlag ist die Übertragung weitgehender Kompetenzen für Aufsicht und Kontrolle auf die Mitgliedstaaten vorgesehen. Nicht nur soll die nationale Aufsichtsbehörde die Stellen benennen können, die später Konformitätsbewertungen vor Ort durchführen und damit potentiell für KMU als wichtige und zum Teil notwendige Ansprechpartner:innen zur Verfügung stehen. Auch soll sie als Marktüberwachungsbehörde fungieren, um sicherzustellen, dass die Registrierung der KI-Systeme rechtskonform erfolgt, Betriebsprotokolle von Hochrisikoanwendungen ausgewertet und geprüft werden, sowie die Anforderungen auch nach Inverkehrbringung weiterhin



eingehalten werden. Sie dient darüber hinaus als zentrale Koordinationsstelle, als Ansprechpartnerin für die EU-Kommission und Vertreterin Deutschlands in den Ausschüssen der EU.

Abb. 2: Eigene Darstellung der KI-Governance und möglicher Zuständigkeiten im Notifizierungsprozess

Auch die Bundesländer haben sich im Vorfeld einer tatsächlichen Klärung der Zuständigkeiten und Verfahren bereits positioniert. Den Ländern ist laut eines Positionspapiers der Digitalminister:innen zum aktuellen Verhandlungsstand des KI-Acts besonders wichtig, dass auf KMU und Start-ups nicht über Gebühr Belastungen zukommen, die sich aus zu weit reichenden Anforderungen an Konformitätsprüfungen durch notifizierte Stellen sowie die damit in Verbindung stehenden Kosten ergeben könnten. Vor diesem Hintergrund betonen sie auch die Bedeutung einer Selbstzertifizierung entlang vorgegebener Normen als eine für KMU und Start-ups verhältnismäßige Lösung.[28]

Wie die Aufsichtsstruktur im Einzelnen in Deutschland genau aussehen wird, ist aus verschiedenen Gründen zwar noch nicht klar, in Hamburg zeichnet sich jedoch beispielsweise bereits ab, dass ein Joint Venture aus der Zertifizierungsgesellschaft Dekra Digital und der Wirtschaftsprüfungsgesellschaft PWC als deutschlandweiter Zertifizierungsanbieter für KI-Systeme auftreten wird (vgl. hierzu auch Kapitel 4.4 der vorliegenden Studie). Vorbehaltlich der Bewilligung durch die Wettbewerbsbehörden wollen sie ein breites Spektrum an Aufgaben abdecken, die den Konformitätsbewertungsstellen (oder notifizierten Stellen) in der Praxis voraussichtlich zukommen werden, und Unternehmen bei der Einhaltung regulatorischer Vorgaben unterstützen. Sich hier bereits als neuer Akteur zu positionieren, erhöht die Wahrscheinlichkeit, dass sie auch nach Maßgabe des KI-Acts durch eine Bundesbehörde notifiziert werden können.

Wie die obigen Ausführungen jedoch zeigen, gilt auch hier, dass der Verhandlungsprozess in der EU noch nicht abgeschlossen ist und es auch in der Governance-Frage Abweichungen zwischen den Vorschlägen der Kommission und denen des Rates gibt. Das zentral für den Verhandlungsprozess zuständige Bundeswirtschaftsministerium sieht daher keine Veranlassung über die behördlichen Strukturen und Zuständigkeiten in Deutschland bereits zum jetzigen Zeitpunkt zu entscheiden.

2.4 Sanktionsregime und Haftungsregeln: KI-Act, KI-Haftungsrichtlinie und die neue Produkthaftungsrichtlinie der EU

Neben den aus dem KI-Act erwachsenden Rechten und Pflichten müssen Hamburger KMU sich mit dem finanziellen Risiko auseinandersetzen, das in Form von Sanktionen bei Nicht-Einhaltung der Anforderungen aus dem KI-Act oder in Form von Haftungsansprüchen aufgrund von Fehlfunktionen im Betrieb entstehen kann.

Der KI-Act enthält ein eigenes Sanktionsregime für Fälle der Nichtbefolgung der Verordnung. Zudem hat die EU-Kommission im September 2022 im Kontext ihrer Regulierungsbemühungen den Entwurf einer EU-KI-Haftungsrichtlinie sowie den Entwurf für eine neue EU-Produkthaftungsrichtlinie vorgelegt. Die beiden Richtlinien sollen den KI-Act im Hinblick auf Haftungsfragen beim Einsatz von Software bzw. Künstlicher Intelligenz ergänzen. Eines der Hauptprobleme bei Haftungsfragen rund um das Thema Künstliche Intelligenz ist ganz grundsätzlich der Umgang mit der Komplexität, Autonomie und Undurchsichtigkeit von

[28] Digitalministertreffen Baden-Württemberg 2022 (12.12.2022): Beschluss des Digitalministertreffens D16 vom 12. Dezember 2022: Positionierung der Länder gegenüber der geplanten KI-Verordnung der Europäischen Union, https://im.baden-wuerttemberg.de/fileadmin/redaktion/m-im/intern/dateien/pdf/20221212_Positionierung_der_Laender_gegenüber_der_geplanten_KI-Verordnung_der_Europaeischen_Union.pdf (zuletzt aufgerufen am 28.02.2023)

KI-Systemen. Im Vordergrund stehen daher sogenannte Black Box-Effekte sowie selbstlernende Systeme und die aus ihnen erwachsende Intransparenz und mangelnde Nachvollziehbarkeit des Entscheidungsprozesses. Die bisherigen haftungsrechtlichen Regelungen haben unter anderem vor diesem Hintergrund zu unbefriedigenden Ergebnissen geführt, etwa in Bezug auf die Frage, wer für durch KI eingetretene Schäden haftet oder wen in welcher Form die Beweislast trifft. Vor dem Hintergrund dieser Herausforderungen sind die neuen Regulierungsansätze der EU auch im Bereich des Haftungsrechts zu verstehen.

Im Folgenden wird kurz auf das Sanktionsregime des KI-Acts eingegangen (2.4.1), um sich anschließend den Entwürfen der KI-Haftungsrichtlinie (2.4.2) und der Produkthaftungsrichtlinie (2.4.3) zu widmen.

2.4.1 Sanktionsregime des KI-Acts[29]

Der Verordnungsentwurf der Kommission sieht gemäß Art. 71 Abs. 1 KI-Act Entwurf vor, dass die Mitgliedstaaten Sanktionsvorschriften erlassen, beispielsweise in Form von Geldbußen, die bei Verstößen gegen den KI-Act verhängt werden. Sie stellen darüber hinaus deren ordnungsgemäße und wirksame Durchsetzung sicher. Je nach Schwere des Verstoßes sind unterschiedliche Rahmen für die Höhe des Bußgeldes vorgegeben:

Den obersten Bußgeldrahmen gibt die Verordnung in Art. 71 Abs. 3 KI-Act Entwurf mit einer Höhe von bis zu 30 Millionen Euro oder (für Unternehmen) 6 Prozent des weltweiten Jahresumsatzes vor. Dieses Bußgeld droht beim Einsatz eines verbotenen KI-Systems nach Art. 5 KI-Act Entwurf sowie dann, wenn die Qualitätsanforderungen bezüglich Daten und Daten-Governance (Art. 10 KI-Act Entwurf) an Hochrisiko-KI-Systeme nicht eingehalten werden.

Als mittlerer Bußgeldrahmen sollen diejenigen Marktteilnehmer:innen mit einer Geldbuße von bis zu 20 Millionen Euro oder (für Unternehmen) 4 Prozent des weltweiten Jahresumsatzes rechnen müssen, die KI-Systeme entwickeln, verwenden oder in Verkehr bringen, die gegen die sonstigen Anforderungen und Pflichten der KI-Verordnung verstoßen (außerhalb des Anwendungsbereichs von Art. 5 und 10 KI-Act Entwurf).

Als niedrigster Bußgeldrahmen wird in Art. 71 Abs. 5 KI-Act Entwurf eine Geldbuße von bis zu 10 Millionen Euro oder (für Unternehmen) 2 Prozent des weltweiten Jahresumsatzes vorgegeben, die verhängt werden soll im Falle der Übermittlung unvollständiger, falscher oder irreführender Angaben gegenüber Behörden.

2.4.2 KI-Haftungsrichtlinie[30]

Ziel der KI-Haftungsrichtlinie laut gegenwärtigem Entwurfsstand ist es, Geschädigten die gerichtliche Durchsetzung außervertraglicher Schadensersatzansprüche wegen unrechtmäßiger Handlungen oder

[29] Das folgende Kapitel bezieht sich ausschließlich auf den EU-Verordnungsentwurf vom 21.4.2021.
[30] COM (2022) 496 final (28.09.2022): Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz

Unterlassens zu erleichtern, die durch den Einsatz von KI entstehen. Geschädigte können sowohl Einzelpersonen wie auch Unternehmen oder Organisationen sein. Als Schädiger:in in Anspruch genommen werden können Anbieter:innen von KI ebenso wie Entwickler:innen und sonstige Marktteilnehmer:innen. Die KI-Haftungsrichtlinie wird also für viele KMU unmittelbare Relevanz haben. Sie erhöht die Anforderungen an die sorgfältige unternehmensinterne Dokumentation insofern, als dass bei einem auftretenden Schaden KMU regelhaft ihr Vorgehen werden belegen müssen. Das gilt insbesondere dann, wenn es um die Entwicklung von Hochrisiko-Systemen geht oder diese im Bereich sensibler Infrastruktur nach KI-Act eingesetzt werden.

Im Einzelnen soll die gerichtliche Durchsetzung von derartigen Schadensersatzansprüchen laut Kommissionsentwurf durch zwei die Beweisführung betreffende Faktoren erleichtert werden:

1. Erleichterung des Zugangs zu Beweismitteln durch eine Offenlegungspflicht für die Schädiger:innen:
    a. Geschädigte sollen die Offenlegung von Informationen zu KI-Systemen bei Gericht beantragen können, um herauszufinden, wie es zu dem Schaden kommen konnte. Hierfür soll laut Richtlinienentwurf ausreichen, dass die Geschädigten die Plausibilität ihres Anspruches durch Vorlage von Tatsachen und Beweismitteln ausreichend belegen.
    b. Die widerlegbare Vermutung eines haftungsrechtlich relevanten Sorgfaltspflichtenverstoßes soll dann gelten, wenn der:die Schädiger:in der gerichtlichen Anordnung zur Offenlegung nicht nachkommt.
    c. Problematisch kann der Entwurf aus Unternehmenssicht dann sein, wenn die Gefahr besteht, Geschäftsgeheimnisse offenlegen zu müssen, die durch Dritte weiterverwendet werden könnten.
2. Widerlegbare Vermutung eines ursächlichen Zusammenhangs im Fall eines Verschuldens:
    a. Es wird ein Kausalzusammenhang zwischen dem (von dem:der Geschädigten bewiesenen oder vom Gericht auf Grundlage der maßgeblichen Umstände vermuteten) Verschulden der Anbieter:innen von Systemen der Künstlichen Intelligenz und den von ihren KI-Systemen erzeugten Ergebnissen oder dem Fehlen solcher Ergebnisse unter bestimmten Bedingungen widerlegbar vermutet. Die Kausalität muss dabei vernünftigerweise wahrscheinlich sein, aber von dem:der Geschädigten nicht mehr im Einzelnen nachgewiesen werden. Es muss aufgrund der Umstände des Falles lediglich als hinreichend wahrscheinlich angesehen werden können, dass das Verschulden bzw. die Sorgfaltspflichtverletzung, die von dem KI-System erzeugte Leistung oder das Versäumnis des KI-Systems, eine Leistung zu erbringen, beeinflusst haben.
    b. Ausgenommen von dieser Beweiserleichterung sind Geschädigte, die über ausreichende Möglichkeiten und Expertise verfügen, um den Beweis des ursächlichen Zusammenhangs zwischen einer Verletzung der Sorgfaltspflicht und dem Schaden selbst beizubringen.

Die vorstehend dargestellte Erleichterung der gerichtlichen Durchsetzung von außervertraglichen Schadensersatzansprüchen kann KMU vor große Herausforderungen stellen. In Verbindung mit den im KI-Act vorgesehenen Bußgeldrahmen (Art. 71 Abs. 3 KI-Act Entwurf) von bis zu 6 Prozent des weltweiten

Richtlinie über KI Haftung, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496&qid=1677687781503 (zuletzt aufgerufen am 28.02.2023)

Jahresumsatzes oder 30 Millionen Euro können auf KMU deutliche Belastungen zukommen. Die Einhaltung der Sorgfaltspflichten sollte daher zu jedem Zeitpunkt des unternehmerischen Handelns stringent beachtet und dokumentiert werden.

2.4.3 Produkthaftungsrichtlinie[31]

Die EU-Kommission hat daneben einen Vorschlag für die Überarbeitung der Produkthaftungsrichtlinie – die derzeitigen Regelungen sind fast 40 Jahre alt – auf den Weg gebracht, um den Herausforderungen „neuer" Technologien wie Software oder Künstlicher Intelligenz auch in der generellen Produkthaftung Rechnung zu tragen. Dabei wird eine Vereinheitlichung von europäischem Produktsicherheitsrecht und Produkthaftung angestrebt, die auch der dynamischen Lage angemessen ist.

1. Die Produkthaftung soll damit zukünftig auch digitale Produktionsdateien und Software einschließlich KI-Systeme umfassen, bezieht Fragen der Cybersicherheit des Produkts mit ein und erstreckt sich zeitlich über den Zeitpunkt des Inverkehrbringens hinaus, wenn es auch danach weiterhin möglich ist, das Produkt zu kontrollieren. Ähnlich den oben ausgeführten Neuerungen durch die KI-Haftungsrichtlinie soll es in Bezug auf Kontrolle, Beweislast und Offenlegungspflicht auch hier eine deutliche Stärkung der Seite der Geschädigten geben. Zugunsten des:der Geschädigten wird ein Kausalzusammenhang zwischen Produktfehler und Schaden vermutet, wenn offensichtliche Fehlfunktionen des Produktes bei normalem Gebrauch für den Schaden ursächlich sind.
2. Auch sollen bisher mögliche gesetzliche oder vertragliche Haftungsausschlüsse der Hersteller:innen eingeschränkt werden. So sollen sich die Hersteller:innen etwa auf eine fehlende Erkennbarkeit eines Produktfehlers bei Inverkehrbringen nicht berufen dürfen, wenn dieser Fehler durch ein Software-Update hätte behoben werden können.
3. Auch hier soll es eine Offenlegungspflicht für Unternehmen geben, Konstruktionsunterlagen oder dokumentierte Erkenntnisse aus der Produktbeobachtung, die Geschädigte zur Begründung des Anspruches brauchen, herauszugeben. Bei Nichtbefolgung dieser Pflichten wird von einer gesetzlichen Vermutung der Fehlerhaftigkeit ausgegangen.

Eine Anpassung der Produkthaftungsrichtlinie an die Entwicklungen der Zeit und die Regelungsmaterie des KI-Acts ist sicher geboten. In Bezug auf KI wird sie laut des derzeitig vorliegenden Entwurfs für KMU dann relevant, wenn es sich bei der in Frage stehenden KI um eine Teilkomponente eines Produkts handelt, es also beispielsweise um Sicherheitskomponenten einer Maschine geht, deren Anforderungen in der Maschinenrichtlinie der EU definiert werden. Für Entwickler:innen und Anbieter:innen ist wie bei der KI-Haftungsrichtlinie von Bedeutung, dass ihre Haftung nicht automatisch erlischt oder zeitlich von vornherein zu begrenzen wäre. Auch der Umstand, dass Haftungsausschlüsse laut Richtlinienentwurf stark eingeschränkt werden und Beweislasterleichterungen durch die Offenlegungspflicht von Unterlagen eingeführt werden sollen, erfordert von KMU bereits in der Entwicklungsphase eines KI-Systems

[31] COM (2022) 495: Proposal for a directive of the European Parliament and of the Council on liability for defective products, https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en(zuletzt aufgerufen am 28.02.2023)

vorausschauende Dokumentation und die Erfüllung aller auf sie zukommenden Pflichten – auch mit Blick auf sich ändernde Anwendungskontexte bei einer Weiterentwicklung des Geschäftsmodells (s.o.).

Zusammenfassend lässt sich sagen, dass die KI-Verordnung sowie die Entwürfe der KI-Haftungsrichtlinie und der Produkthaftungsrichtlinie nicht getrennt voneinander zu verstehen und zu denken sind. Sie verstärken sich in ihrer Wirkung gegenseitig und bilden erst gemeinsam ausreichenden Rechtsschutz sowohl für Anwender:innen von KI-Systemen als auch für Hersteller:innen und Entwickler:innen.[32] Dabei rückt die KI-Verordnung die Sicherheit der Systeme in den Mittelpunkt, um Schäden grundsätzlich zu vermeiden, während es bei der KI-Haftungsrichtlinie um den Umgang mit dennoch auftretenden Schäden geht. In Zusammenhang mit der ebenfalls überarbeiteten Produkthaftungsrichtlinie, die wie die KI-Haftungsrichtlinie mit Instrumenten der Beweislasterleichterungen arbeitet, will die EU ein Regulierungsregime schaffen, das die verschuldensunabhängige Haftung stärker ins Zentrum ihrer Bemühungen stellt.[33] So nimmt die EU neben den Entwickler:innen und Hersteller:innen auch die Anwender:innen langfristig in die Pflicht, was für diese insbesondere dann zu Schwierigkeiten führen kann, wenn sie nicht über ausreichend technisches Wissen verfügen, um die sichere und transparente Funktion der KI-Anwendung prüfen zu können. Auch vor diesem Hintergrund wird eine Zertifizierung der Produkte für viele Akteure auf der Anwender:innenseite schon beim Erwerb voraussichtlich deutlich an Bedeutung gewinnen, um belastbar in die ordnungsgemäße Funktion des Systems vertrauen zu können.

2.5 Ausblick

Wenn auch noch viele Fragen in Bezug auf konkrete Standards, die Governance und selbst die Definition von KI im europäischen KI-Act offen sind, so ist jedoch jetzt schon absehbar, dass die beschriebenen Entwicklungen insbesondere innerhalb des EU-Binnenmarktes, aber auch darüber hinaus, erhebliche Auswirkungen auf alle Wirtschaftsakteure haben werden – egal ob es sich um große Unternehmen oder um kleine und mittelständige Betriebe handelt. Die Übersetzung der Anforderungen des KI-Acts in konkrete technische Normen ist dabei ein für die Praxis höchst relevanter Schritt und wird Unternehmen wie auch öffentliche Akteure bei der Compliance mit dem KI-Act deutlich entlasten. Zugleich schafft die öffentlich zugängliche Datenbank eine bisher nicht bekannte Transparenz, die insbesondere Entwickler:innen und Anbieter:innen einer Öffentlichkeit aussetzen, die auch kritische Stimmen hervorrufen wird. Und nicht zuletzt wird die Beantwortung der Frage, wer für durch den Einsatz von KI verursachte Schäden haften wird, auch ökonomisch von größter Relevanz sein. Vor diesem Hintergrund sind alle beteiligten Akteure bereits jetzt gut beraten, schon in der Entwicklung neuer KI-Lösungen auf die sich entwickelnde Rechtslage zu schauen und ihre Systeme derart zu konzipieren, dass sie sowohl in Einklang stehen mit den sich aus dem KI-Act ergebenden Anforderungen, als auch einer Überprüfung durch eine kritische Öffentlichkeit standhalten.

---

[32] Es ist zurzeit nicht absehbar, wann die beiden Richtlinien auf europäischer Ebene verabschiedet und anschließend in nationales und damit verbindliches Recht umgesetzt werden. Zunächst werden die beiden Entwürfe in das Abstimmungsverfahren zwischen Rat, Parlament und Kommission gehen, wobei es noch zu Änderungen kommen kann. Anschließend müssen die beiden Richtlinien mit den entsprechenden Gesetzgebungsverfahren in nationales Recht gegossen werden.

[33] Es geht hierbei um außervertragliche Haftungsfälle, die durch ein KI-System verursacht wurden und „*einen außervertraglichen verschuldensabhängigen zivilrechtlichen Schadensersatzanspruch*“ (siehe Art. 1 Abs. 2 KI-Haftungs-RL-E).

3. Verantwortungsvolle KI – Responsible AI: von der EU normiert, von den Bürger:innen gewünscht

> *KI ermöglicht tiefgreifende Neuerungen und Beschleunigungen, die alle gesellschaftlichen Bereiche erfassen werden. Diese Entwicklungen werfen wichtige philosophische, ethische, rechtliche, soziale und politische Fragen im Hinblick auf das Zusammenwirken von Menschen und KI-Systemen auf. Ohne Standards, Leitlinien und klare Regeln kann es zu Diskriminierung, Ausgrenzung und Benachteiligung von Menschen beim Einsatz von Künstlicher Intelligenz kommen. Daher ist es notwendig, Regeln und ethische Standards für einen verantwortungsvollen Umgang mit KI zu erarbeiten und umzusetzen.*

Für die EU steht neben dem Ziel der Förderung eines global wettbewerbsfähigen und innovationsfreundlichen Umfeldes für Digitalunternehmen und Start-ups die Schaffung eines Regulierungsregimes für den Einsatz Künstlicher Intelligenz im Mittelpunkt ihrer Bemühungen, das sich an Menschenrechten, Demokratie, dem Schutz der Privatsphäre und der Aufrechterhaltung sozialstaatlicher Prinzipien orientiert. Hiermit soll nicht nur vermieden werden, dass intransparente Monopole großer Digitalkonzerne entstehen oder einer umfänglichen digitalen Überwachung Tür und Tor geöffnet wird, sondern zentral auch gewährleistet werden kann, dass der Einsatz von KI jederzeit sicher, transparent, ethisch und unparteiisch erfolgt – kurz, dass sich der Einsatz an den Werten und Prinzipien der Europäischen Union orientiert.

Politisch hat die EU dabei den Ausgleich verschiedener Interessen und Anliegen im Blick: So sollen gleichermaßen die wirtschaftlichen und gesellschaftlichen Potentiale von KI genutzt werden, die sich nach aktuellen Umfragen auch aus Sicht der Bürger:innen durch ihren Einsatz ergeben und zu Erleichterungen im Alltag führen (86%); und es soll zugleich den Sorgen der Bürger:innen vor einem unsachgemäßen Einsatz von KI-Systemen begegnet werden. Denn mit 66 Prozent äußert laut einer Forsa Umfrage des TÜVs vom November 2022 ein beträchtlicher Teil Sorgen vor einer Diskriminierung durch den missbräuchlichen Einsatz von KI und auch die Befürchtung einer Manipulation von KI selbst (62%) sowie potentiell negativer Auswirkungen einer „Vermenschlichung" von Algorithmen bleibt groß.[34]

Nicht nur seitens der Bürger:innen, auch von Unternehmen werden in Umfragen diverse Risiken im Zusammenhang mit dem Einsatz von KI geäußert, die über Haftungsfragen hinausgehen: So sehen nach einer aktuellen Studie der Bitkom 49 Prozent der befragten Unternehmen die mangelnde Nachvollziehbarkeit von KI-Entscheidungen als problematisch an; 48 Prozent machen sich Sorgen darum, dass die Systeme nur mangelhaft beherrschbar sind und 47 Prozent sagen, dass sie befürchten, dass mögliche Fehlerquellen in den Lernbeständen nur schwer erkennbar sein könnten. Daraus ergibt sich für immerhin 33 Prozent der Unternehmen die Sorge, dass sie einen Imageschaden riskieren und ihre Außenwirkung beeinträchtigt wird, wenn eine von ihnen eingesetzte KI zu unbeabsichtigten Effekten und tatsächlichen Schäden führt.[35] Vor diesem Hintergrund kann der Faktor „Vertrauen" in die eingesetzte Technologie nicht losgelöst werden von dem Ziel einer wirtschaftlich dynamischen Entwicklung europäischer KI-Ökosysteme.

---

[34] TÜV Verband e.V. (23.11.2022): Verbraucher:innen fordern gesetzliche Regeln für Künstliche Intelligenz [Pressemeldung], https://www.presseportal.de/pm/65031/5377332 (zuletzt aufgerufen am 28.02.2023)

[35] Autor unbekannt, BITKOM (13.9.2022): KI gilt in der deutschen Wirtschaft als Zukunftstechnologie – wird aber selten genutzt, [Pressemeldung], https://www.bitkom.org/Presse/Presseinformation/Kuenstliche-Intelligenz-2022(zuletzt aufgerufen am 28.02.2023)

In diesem Kontext sind daher auch die Regulierungsbemühungen der EU zu verstehen: Die Bürger:innen der EU brauchen genauso die Sicherheit eines verantwortlichen Einsatzes wie europäische Unternehmen. So sollen sich die Bürger:innen darauf verlassen können, dass innerhalb der EU angewendete und entwickelte Technik nicht nur technisch auf höchstem Niveau ist, sondern auch grundlegende europäische Werte wahrt und den Grundrechtsschutz gewährleistet. Nur wenn sich dieser Glaube in materiellen Rechtsschutz und verlässliche Zertifizierungssysteme übersetzt, ist gleichsam für Unternehmen zu erwarten, dass die entwickelten Produkte am Markt bestehen und ihre wirtschaftlichen Potentiale vollumfänglich ausgeschöpft werden können. Das Recht bietet demnach die Chance, notwendiges Vertrauen in die Technologie zu stärken und die durchaus noch vorhandene kritische Grundhaltung der Bürger:innen in eine höhere Akzeptanz zu überführen, die wiederum für den Ausbau des KI-Ökosystems innerhalb der EU unumgänglich ist. Daher ist es auch wenig überraschend, dass laut der bereits oben zitierten Forsa Umfrage des TÜVs die Zustimmung der Bevölkerung in Deutschland zu einer europaweiten Regulierung von KI sehr hoch ist. So wünschen sich 82 Prozent der Befragten eine Regulierung von KI-Systemen. 90 Prozent wünschen sich ein unabhängiges Siegel, um das Vertrauen in die Produkte und ihre Ergebnisse zu stärken. Und 75 Prozent halten eine Selbstverpflichtung zu einem ethischen Einsatz von KI für vertrauensbildend.

In dieser Hinsicht kommt eine europaweit gültige Verordnung gerade recht. Da allerdings davon auszugehen ist, dass Nutzer:innen und Betroffene, die mit Sorgen auf die Technologie schauen, nicht zwischen Allgemeinzweck-KI, Hochrisiko-KI und KI-Systemen mit geringem Risiko differenzieren, sondern jegliche Software-Anwendungen, wie das oben genannte Beispiel zum Kindergeldskandal in den Niederlanden exemplarisch zeigt, den gleichen öffentlichen Bewertungsmaßstäben unterliegen, wird ein breites gesellschaftliches Vertrauen in die Technik voraussichtlich nur dann entstehen, wenn auch außerhalb des Einsatzes in Hochrisikobereichen entsprechende Anforderungen gelten oder eingehalten werden. Denn die Bürger:innen wollen zwar dem Einsatz von KI trauen können, doch ob der fehlerhafte Einsatz von einer Hochrisiko-KI oder einer klassischen, nicht-KI-basierten Softwarelösung, die nicht vom KI-Act erfasst wird, ausgeht, interessiert im Schadensfall weniger. Wenngleich der KI-Act wie oben beschrieben zunächst nur an Hochrisiko-KI verbindliche Anforderungen stellt, so könnten die von der Kommission empfohlenen Verhaltenskodizes, die grundlegende Qualitätsanforderungen auch für Nicht-Hochrisiko-KI vorsehen, diese Lücke adressieren.

Aber auch für die verbindlichen Regeln unterliegende Hochrisiko-KI stellt sich noch die Frage, wie sich das Bedürfnis nach Vertrauen und Verlässlichkeit in Form konkreter Maßnahmen und Prozesse in die Praxis übersetzen lässt. Daher stehen sowohl Akteure an den technischen Schnittstellen als auch diejenigen im politischen Diskurs und in der Gesetzgebung aktuell vor der Herausforderung, einen Ansatz zu finden, der das, was hinter der Kulisse des Systems passiert, nachvollziehbar und verlässlich macht. In der Praxis und Forschung werden vor diesem Hintergrund diverse technische und organisatorische Maßnahmen, die dazu beitragen, den Einsatz von KI vertrauensvoll zu gestalten, unter dem Begriff *Responsible AI* (im Folgenden RAI), zusammengefasst. So werden an der Schnittstelle zwischen Recht, Technik und Soziologie entsprechende Fragestellungen vorwiegend konzeptionell bearbeitet, während in der Praxis zunehmend konkrete Kriterien zur Anwendung kommen, die eine Brücke schlagen wollen, zwischen ethischen

Ansprüchen, rechtlichen Normen und technischen Möglichkeiten.[36] Dabei wird der verantwortliche Einsatz von KI daran gemessen, ob

- der KI-Einsatz im Einklang mit europäischen Wertevorstellungen und rechtlichen Anforderungen steht (Ethik & Recht),
- es nachvollziehbar ist, wie das Ergebnis der KI zustande kommt (Erklärbarkeit),
- Fehlfunktionen und Ausfälle minimiert werden (Robustheit & Sicherheit),
- die Ausgaben nicht zu Diskriminierung führen (Fairness & Nachhaltigkeit)
- und es klare Zuständigkeiten und Prozesse für die Entwicklung und den Betrieb der KI-Anwendung gibt (Governance).

RAI bewegt sich damit in der Schnittmenge von Recht und Technik, wobei in der Praxis rechtliche Anforderungen und technische Möglichkeiten häufig kontext- und anwendungsfallspezifisch austariert werden müssen.

Ebendieser Logik folgt – wenn auch zentral auf Anforderungen im Hochrisikobereich fokussiert – der Entwurf des KI-Acts der EU. Man kann ihn also als regulative Entsprechung des normativen Konzepts einer RAI verstehen, wobei sich auch der hohe Grad an Kontextspezifität von RAI im Verordnungsentwurf niederschlägt. So finden sich etwa in Titel III, Kapitel 2 KI-Act Entwurf mit den Kriterien einer RAI korrespondierende Vorgaben:

- Anforderungen an *Ethik & Regulierung* in Art. 11 (Technische Dokumentation), Art. 12 (Aufzeichnungspflichten), Art. 19 (Konformitätsbewertung),
- Anforderungen an die *Erklärbarkeit* von KI-Systemen in Art. 13 (Transparenz & Bereitstellung von Informationen für die Nutzer:innen),
- Anforderungen an *Robustheit & Sicherheit* in Art. 15 (Genauigkeit, Robustheit, Cybersicherheit),
- Anforderungen an *Fairness* in Art. 10 (Daten & Daten-Governance),
- und Anforderungen an *Governance* in Art. 9 (Risikomanagementsystem), Art. 14 (menschliche Aufsicht), Art. 17 (Qualitätsmanagementsystem).

Eine Konkretisierung der im KI-Act normierten Anforderungen ist durch die laufenden Aktivitäten in den oben beschriebenen Gremien zu erwarten. Dies wird jedoch aller Voraussicht nach zu einem dauerhaften politischen Aushandlungsprozess und ständigen an der Praxis orientierten Anpassungen führen. Vor dem Hintergrund einer sich rasant vollziehenden Entwicklung in dem Bereich scheint genau dieser gesellschaftliche Aushandlungsprozess, der institutionell auch durch die Ergänzung des KI-Ausschusses um zivilgesellschaftliche Akteure seinen Widerhall findet, auch zwingend notwendig. Bei Berücksichtigung der Kriterien einer RAI würde jedoch bereits ein Großteil der vertrauensbildenden Faktoren für den KI-Einsatz sowohl im Sinne der Bürger:innen als auch der Unternehmen abgedeckt – völlig unabhängig von einer verbindlichen rechtlichen Regulierung. Will man das durch das Regulierungsregime zu erwartende

[36] Huchler, Norbert et. al., Plattform Lernende Systeme (Juni 2020): Kriterien für die Mensch-Maschine-Interaktion bei KI: Ansätze für menschengerechte Gestaltung in der Arbeitswelt, Whitepaper der AG Arbeit/Qualifikation, https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG2_Whitepaper2_220620.pdf (zuletzt aufgerufen am 28.02.2023) *sowie*
Autor unbekannt, Fraunhofer IKS (2023): Künstliche Intelligenz: Sicherheit für Industrie, Medizin und autonomes Fahren erfordert zuverlässige Entscheidungen, https://www.iks.fraunhofer.de/de/leistungen/zuverlaessige-kuenstliche-intelligenz.html (zuletzt aufgerufen am 07.02.2023)

aufgebaute Vertrauen der Bürger:innen in die Potentiale und die Sicherheit der Technologie nicht erschüttern, sind sowohl kontinuierliche Anpassungen und Bewertungen des Risikopotentials von KI-Systemen in den zuständigen europäischen Gremien notwendig als auch eine grundsätzliche Orientierung aller Marktakteure an den Kriterien der RAI ratsam.

4. KI & Recht in Hamburger KMU – aktueller Stand und Situation in Hamburg

> *Hamburger Unternehmen sind in der Breite von der aktuellen Regulierungsdynamik betroffen. Bestehende Strukturen in der Forschungs- und Beratungslandschaft sind jedoch in der Mehrzahl entweder thematisch nicht ausreichend an der Schnittstelle von Technik und Recht verankert, haben einen zeitlich begrenzten Projektcharakter oder sind nicht niedrigschwellig genug, um geeignete Anlaufstellen für Hamburger KMU darstellen zu können.*

Hamburg hat sich hohe Ziele gesetzt für den Umbau der Stadt hin zu einer digitalen Metropole des 21. Jahrhunderts. In der Digitalstrategie der Stadt heißt es zum Thema Künstliche Intelligenz, dass „...es Hamburgs Ziel (sei), KI als Querschnittstechnologie zu nutzen und ihren humanzentrierten Einsatz bereichsübergreifend zu fördern. Entscheidend bleibt dabei, dass der Mensch im Mittelpunkt steht und der Rechtsstaat nicht ausgehöhlt wird."[37] Außerdem strebt die Stadt an, unter Berücksichtigung ebendieser ethischen Leitplanken „... den Wissenschafts- und Wirtschaftsstandort Hamburg im KI-Bereich branchenübergreifend und interdisziplinär (zu) stärken."[38]

Für Hamburg, die Aktivitäten der einzelnen Akteure und das KI-Ökosystem in der Stadt, sollten die oben ausgeführten Entwicklungen daher einmal mehr Grund dafür sein, bereits zum jetzigen Zeitpunkt eine systematischere Auseinandersetzung mit den rechtlichen Bedingungen zukünftiger Einsätze Künstlicher Intelligenz zu fördern und zu unterstützen. Dies gilt insbesondere für kleine und mittelständische Unternehmen, also Betriebe, die nach EU-Definition weniger als 250 Mitarbeitende haben und einen Jahresumsatz von maximal 50 Millionen Euro aufweisen. Viele dieser Unternehmen verfügen nicht über eigene Rechtsabteilungen. Nicht selten können sie sich eine teure Rechtsberatung nicht leisten. Bestimmte auf sie zukommende Auflagen, die schon heute Investitionsentscheidungen beeinflussen könnten, sind ihnen nicht bewusst. Manchmal führt diese Unsicherheit gar zur Vermeidung des Einsatzes von KI – auch dort, wo womöglich Vorteile daraus entstehen könnten. So geben in einer Studie der Handelskammer Hamburg aus dem Jahr 2020 28 Prozent an, dass eine Nutzung von KI nicht geplant sei.[39]

Zur Förderung des KI-Ökosystems und des Standorts Hamburg ist es daher auch aus Sicht der Stadt ratsam, Angebote bereitzustellen, die die Hemmschwellen des KI-Einsatzes senken, die Rechtssicherheit stärken und so auch das gesellschaftliche Vertrauen in die Technologie insgesamt erhöhen. Im Sinne einer zukunftsorientierten Wirtschaftsförderung, die sich an den Bedingungen für eine gelingende digitale

[37] Freie und Hansestadt Hamburg - Senatskanzlei Amt für IT und Digitalisierung (2020): Digitalstrategie für Hamburg, S. 57, https://static.hamburg.de/fhh/epaper/digitalstrategie/#0 (zuletzt aufgerufen am 28.02.2023)
[38] Ebenda
[39] Handelskammer Hamburg (September 2020): Standpunkte: Künstliche Intelligenz: Chancen für die Hamburger Wirtschaft nutzen, S.31, Abb. 19, https://www.ihk.de/blueprint/servlet/resource/blob/4911176/06c416127e170419fb4f7f9f2feda9d9/standpunkte-ki-data.pdf (zuletzt aufgerufen am 28.02.2023)

Transformation orientiert, sollte es daher auch Aufgabe der Stadt sein, hier mit Angeboten auf KMU zuzugehen und aktiv aufzuklären.[40] Denn nach vielfältigen Gesprächen mit Akteuren, sowohl in Einzelgesprächen mit Start-ups als auch im Rahmen von Workshops im Kontext der Beratungsaktivitäten von ARIC e.V. oder in Gesprächen mit in der Handelskammer Hamburg organisierten KMU, ergibt sich ein weitgehend einheitliches Bild zur Frage eines rechtssicheren Einsatzes von KI: Bewusstsein besteht über die Notwendigkeit einer der DSGVO entsprechenden Behandlung personenbezogener Daten. Wenig Bewusstsein besteht dagegen über die Notwendigkeit darüberhinausgehend die Transparenz- und Governance-Regeln des KI-Acts zukünftig umsetzen zu müssen – beginnend bei der Auswahl der zugrunde gelegten Trainingsdaten bis hin zu Kontrollmechanismen im Betrieb. Da der Hamburger Senat unabhängig von den Aktivitäten auf europäischer Ebene eine „... Transparenz der jeweils eingesetzten Algorithmen sowie Rechtssicherheit im Umgang mit KI"[41] ganz grundsätzlich anstrebt, erscheint die Notwendigkeit eines aktiven Zugehens auf die Wirtschaftsakteure der Stadt zentral.

Aber nicht nur das: In dem Bewusstsein, dass es für zukünftige Aktivitäten zwingend notwendig ist, das Vertrauen der Stadtgesellschaft insgesamt in einen Einsatz von KI an den unterschiedlichsten Stellen zu erhöhen – sei es im Verkehrssektor, in Verwaltungsabläufen oder Personalentscheidungen –, hat sich der Hamburger Senat in seiner Digitalstrategie auch die „... Vermeidung jedweder Diskriminierung durch KI" zum Ziel gesetzt. Ein wirtschaftlicher Ausbau eines gut vernetzten KI-Ökosystems mit Leuchtturmprojekten wie beispielsweise den durch die Hochbahn initiierten Innovationspartnerschaften zum Thema autonomes Fahren muss daher Hand in Hand gehen mit einer Strategie, den Bürger:innen die Sorgen vor dem Einsatz der Technik im öffentlichen Raum zu nehmen. Aus dieser Perspektive dient der KI-Act als Chance, durch ihn unter Verweis auf Regeln zur Sicherheit und Diskriminierungsfreiheit der eingesetzten Technik eben dieses Vertrauen stärken zu können. Durch die deutlich erweiterten Anforderungen an Dokumentation und Qualitätssicherung, durch Zertifizierungsverfahren, die Gewährleistung des Rechtsschutzes und die Regelungen von Haftungsfragen kann der durchaus kritischen Grundhaltung der Bürger:innen begegnet und die Akzeptanz gegenüber der Technik erhöht werden. Es bietet sich daher für den Wirtschaftsstandort Hamburg nicht nur wirtschaftlich, sondern auch politisch und gesellschaftlich an, über die Anforderungen des KI-Acts für einzelne Anwendungsbereiche im Hochrisikobereich hinauszugehen und sich darüber hinaus an den Kriterien eines verantwortlichen Einsatzes von KI entsprechend dem Konzept einer *Responsible AI* zu orientieren.

Vor diesem Hintergrund soll an dieser Stelle zunächst ein Blick in die Praxis einen Überblick darüber bieten, welche Aktivitäten sich in Hamburg an der Schnittstelle zwischen Recht und KI bereits etabliert haben, bevor in den beiden folgenden Kapiteln konkrete Handlungsschritte sowie -empfehlungen ausgesprochen werden, die sich an einer weiteren Förderung für KMU orientieren. Die Erkenntnisse gehen im Wesentlichen auf Gespräche mit verschiedenen Akteuren der Stadt aus Wirtschaft, Wissenschaft und öffentlicher Verwaltung sowie Rechercheaktivitäten im KI-Ökosystem zurück.

[40] Auch der KI-Act selbst sieht für die Mitgliedstaaten der EU vor, dass sie derartige Beratungs- und Sensibilisierungsangebote machen, vgl. hierzu auch Kapitel 5.1 der vorliegenden Studie.

[41] Freie und Hansestadt Hamburg – Senatskanzlei Amt für IT und Digitalisierung (2020): Digitalstrategie für Hamburg, S. 57, https://static.hamburg.de/fhh/epaper/digitalstrategie/#0 (zuletzt aufgerufen am 28.02.2023)

4.1 Ein Blick in die Praxis

Im Rahmen unserer Studie haben wir mit verschiedenen Zielgruppen in Hamburg Gespräche geführt. Dazu zählten KMU und Start-ups, die bereits KI-Systeme entwickeln und vermarkten, ebenso wie Unternehmen, die ein Interesse an ihrem Einsatz haben. Dabei bestätigte sich der Eindruck, der auch aus anderen Studien und Befragungen hervorgeht: Die Möglichkeiten des Einsatzes von KI in Hamburger KMU wird häufig unterschätzt. Die hierfür genannten Gründe sind vielschichtig, angefangen von fehlenden Informationen bzw. Kenntnissen über die mit dem Einsatz von KI möglicherweise verbundenen Chancen, bis hin zu einer Scheu vor den Kosten und möglichen Risiken durch die Implementierung von KI-Systemen. Häufig werden auch mangelnde Qualifikation der Beschäftigten genannt oder der Widerstand gegen Veränderungen generell. Es kann oftmals kein sinnvoller Nutzen erkannt werden, entweder, weil es zu wenige Routinetätigkeiten im Betrieb gibt, die durch eine KI ersetzt werden könnten oder weil es keinen klaren Business Case gibt, bei dem Aufwand und Ertrag in einem guten Verhältnis zu stehen scheinen.[42]

In unseren Gesprächen zeichnete sich darüber hinaus ein klares Bild, dass wenn der Einsatz oder die Entwicklung von KI in Erwägung gezogen wird, weitergehende rechtliche Anforderungen im Unternehmensprozess überwiegend reaktiv eine Rolle spielen. Eine große Zahl von Gesprächspartner:innen war sich rechtlicher Probleme beim Einsatz von KI kaum bewusst. Insbesondere dann, wenn in der Entwicklung nicht auf personenbezogene Daten zurückgegriffen wird oder ebensolche in der Anwendung nicht zum Einsatz kamen, wurde die Auseinandersetzung mit rechtlichen Konsequenzen als nachrangig beschrieben. Verständlich, aber ggf. mit Risiken behaftet, erscheint die in den Gesprächen geäußerte Wahrnehmung, dass es im Gegenteil kontraintuitiv sei, sich noch vor der Entwicklung von KI-Lösungen mit den rechtlichen Anforderungen auseinanderzusetzen. Dies würde sich aus Sicht der befragten KMU tendenziell sogar innovationshemmend auswirken. Betriebswirtschaftlich sei die Auseinandersetzung und Antizipation mit den Anforderungen des KI-Acts daher aus Sicht mehrerer Gesprächspartner:innen erst einmal unwichtig, da zunächst die Entwicklung des Produkts im Vordergrund des Alltagsgeschäfts stünde.

Grundsätzlich ist dies kein unübliches Vorgehen. In vielen Fällen ergibt es Sinn, in der frühen Phase offen an die technische Problemlösung heranzugehen und in Form eines Proof of Concept (PoC) zunächst ein wie auch immer geartetes Konzept zu erarbeiten, das zeigt, ob eine Lösung existiert, die gegebene Anforderungen, beispielsweise an die benötigte Genauigkeit unter gegebener infrastruktureller Ausstattung sowie gegebener Datenquantität und -qualität, erfüllen kann. Gibt es eine Lösung, die technisch geeignet ist, um ein bestimmtes Problem zu lösen, wird erst dann im Rahmen der Erarbeitung eines Minimal Viable Product (MVP) zusätzliche Komplexität in Form von Sicherheits-, Compliance- und rechtlichen Erwägungen eingebunden. Dabei kann es durchaus sein, dass der Ansatz des PoC komplett verworfen wird zugunsten einer Lösung, die auch den diversen nicht-technischen Anforderungen Rechnung trägt. Selbst in solchen Fällen leistet der PoC den wichtigen Beitrag, Komplexität zu reduzieren und einen Einstieg in die Problematik zu finden. Unter diesem Gesichtspunkt ist es nicht unüblich und teilweise aus praktischen Gründen gerade für KMU auch notwendig, rechtliche Fragestellungen zunächst hintenan zu stellen. Für KMU ist es also nicht immer möglich, eine rechtliche Einschätzung oder externe Expertise von Anfang an miteinzubeziehen. Hier könnte eine Checkliste oder niedrigschwellige Beratung

[42] Meub, Lukas / Proeger, Till, ifh Forschungsbericht 1 (2022): Künstliche Intelligenz in Handwerk und Mittelstand: Ein Forschungsüberblick, https://ifh.wiwi.uni-goettingen.de/site/assets/files/2167/ifh_fb-1_2022.pdf (zuletzt aufgerufen am 28.02.2023)

hilfreich sein, um KMU dennoch früh im Prozess eine kursorische Einschätzung des Anwendungsfalls in rechtlicher Hinsicht zu ermöglichen und ein Bewusstsein für die rechtlichen Fragen zu schaffen, ohne sie zugleich über Gebühr mit komplexen Prüfungen zu belasten (vgl. hierzu auch 5.2).

Dem Großteil der Gesprächspartner:innen ist insbesondere der Entwurf des KI-Acts mit den je nach Risikostufe verbundenen Anforderungen bisher konkret gar nicht bekannt. Fragen der Governance rund um die Entwicklung bzw. Implementierung von KI, also einer sinnvollen Einbindung der sich aus den rechtlichen Vorschriften ergebenden Anforderungen an z.B. die Entwicklung, den Verkauf oder den Einsatz von KI im Unternehmen, wurden bisher kaum adressiert. Dies gilt insbesondere für potentielle Anwender:innen, die durch den KI-Act sehr viel stärker als bisher in die Pflicht genommen werden würden. In der Entwicklung gelten zwar schon heute zahlreiche ISO- und DIN-Normen, die eine Auseinandersetzung mit Fragen des Qualitätsmanagements, der Datensicherheit oder Protokollierungspflichten erfordern – ganz ähnlich, aber doch unabhängig von einer neuen Regulierung auf europäischer Ebene. Häufig wurden vor diesem Hintergrund in den Gesprächen Bedenken vor einer weiteren Regulierung und einer damit aus Sicht der Gesprächspartner:innen drohenden Bürokratisierung, Reglementierung und Behinderung von Innovation geltend gemacht, wenn es ähnlich der DSGVO zu weitreichenden neuen Anforderungen kommen sollte.

Grundsätzlich sind auf direkte Nachfrage die Bedenken sowohl in Bezug auf den rechtssicheren Einsatz von Trainingsdaten als auch die Sorge vor einem Reputationsverlust bei einem möglicherweise auftretenden Schaden unter den Befragten allerdings gleichsam groß. Einer der Gesprächspartner:innen aus der Hamburger KMU Landschaft berichtet, dass man sich bereits unabhängig von den Anforderungen durch den KI-Act durch viele Qualitätsmerkmale zu einem verantwortungsvollen Umgang mit KI verpflichtet sehe, auch um Vertrauen gegenüber potentiellen Kund:innen aufbauen zu können und eine stabilere Position am Markt zu erlangen. So sind die mit einem Einsatz von KI zusammenhängenden Risiken vielen Akteuren am Markt durchaus bewusst und es wird unter anderem durch die Auseinandersetzung mit der Datengrundlage bereits maßgeblich z.B. an der sogenannten „Bias-Freiheit", also nichtdiskriminierenden Wirkung beim Einsatz von KI, gearbeitet. Zugleich ist die Komplexität der mit dem Einsatz einer RAI zusammenhängenden Fragen nicht selten im Einzelfall für die KMU schwer einschätz- und in der Entwicklung umsetzbar. Aus diesem Grund wünschen sich viele eine unabhängige Beratung und Anlaufstelle, die ihnen eine Entscheidung über den Einsatz und den Mehrwert von KI in ihren Unternehmen erleichtert – insbesondere vor dem Hintergrund neuer rechtlicher Anforderungen und Regeln. Um diesen Gegebenheiten in der Praxis Rechnung zu tragen, werden in Kapitel 6 dieser Studie gezielte Beratungs- und Unterstützungsangebote für KMU empfohlen.

4.2 Ein Blick in die Hamburger Bildungs- und Forschungslandschaft

In Bezug auf das Thema KI an der Schnittstelle zu Recht und Ethik, von technischer Entwicklung und rechtlicher Regulierung lässt sich in den letzten Jahren eine Dynamik in der Bildungs- und Forschungslandschaft erkennen. Es kommt zu zunehmenden, aber vereinzelten Angeboten in der Lehre; es finden sich Institute und Forschungseinrichtungen etwa an der Juristischen Fakultät und am Fachbereich Informatik der Universität Hamburg, an der Bucerius Law School und der Hochschule für Angewandte Wissenschaften. Ein wirklicher Theorie-Praxis-Bezug, der KMU in ihren unmittelbaren Anwendungsfragen helfen würde, ist jedoch allenfalls vereinzelt erkennbar. So werden in einzelnen

Forschungsprojekten oder Forschungsverbünden Fragen von Recht und Technik partiell und selektiv bearbeitet. Deren Ergebnisse werden aber mit Abschluss der Projektlaufzeit nicht zwingend in institutionalisiertes Wissen überführt. Kurzfristige Anfragen aus der Praxis können in der Regel nicht bearbeitet werden. Eine Verstetigung derartiger Arbeit, die sich in gefestigten Institutionen zeigt und damit auch als mögliche Anlaufstelle für KMU etablieren könnte, findet kaum statt. Auch in der Lehre gibt es noch keine systematische Ausrichtung auf derartige Fragestellungen.

Dennoch werden im Folgenden ohne Anspruch auf Vollständigkeit exemplarische Beispiele verschiedener Tätigkeiten aus Forschung und Lehre aufgelistet. Sie können partiell als Ansatzpunkte für Kooperationsmodelle oder den Ausbau von Unterstützungsleistungen dienen, da hier komplexe Fragestellungen bearbeitet werden und grundlegendes Wissen vorliegt:

- Das Hamburg Network for Artificial Intelligence & Law (NAIL)[43] engagiert sich als gemeinsame Plattform von Professor Christoph Kumpan (Bucerius Law School) und Professor Georg Ringe (Universität Hamburg) für den wissenschaftlichen Austausch und gemeinsame Forschungsprojekte im Bereich KI und Recht. Gleichzeitig fördert das Netzwerk den Dialog und das Engagement mit der breiteren Öffentlichkeit. Eine konkrete Anwendungsorientierung, die auch für KMU unmittelbar nutzbar zu machen wäre, zeigt sich bisher jedoch weniger.
- Neben dem NAIL ist eine weitere Gruppe der Bucerius Law School an der Schnittstelle von KI und Recht tätig. Die Law and AI Research Group (LARG)[44], eine Gruppe von Postdoktorand:innen und Doktorand:innen will die Forschung im Bereich der Künstlichen Intelligenz und des Rechts vorantreiben. Hier werden regelmäßig Expert:innen aus diversen Disziplinen eingeladen, um den Ideenaustausch anzutreiben. Eine Forschungsorientierung überwiegt auch hier.
- Ebenfalls an der Bucerius Law School gibt es das Center for Transnational IP, Media and Technology Law and Policy[45] sowie das Center for Legal Technology and Data Science.[46] Beide eignen sich, um an der Schnittstelle von Recht und Technologie angrenzende Fragen zum KI-Einsatz zu diskutieren, von der technischen Anonymisierung von juristischen oder medizinischen Daten bis hin zum Einsatz von Legal Tech Instrumenten in juristischen Berufen.
- Das Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI) erforscht medienvermittelte öffentliche Kommunikation. Das Institut verbindet die Perspektiven einer empirisch fundierten Sozialwissenschaft mit einer auf Regulierungsprozesse ausgerichteten Rechtswissenschaft. Durch seine praxisorientierte Ausrichtung bei gleichzeitiger Grundlagenforschung bietet sich das Institut für verschiedene Kooperationsprojekte an. So

[43] Siehe: Website der Universität Hamburg (2023): Network for Artificial Intelligence & Law (NAIL), https://www.jura.uni-hamburg.de/en/forschung/institute-forschungsstellen-und-zentren/institut-recht-oekonomik/internationale-kooperationen/nail.html (zuletzt aufgerufen am 28.02.2023)

[44] Siehe: Website der Bucerius Law School Hamburg (2022): Law & AI Research Group (LARG) an der Bucerius Law School, https://www.law-school.de/forschung-fakultaet/wissenschaftliche-initiativen/law-ai-research-group (zuletzt aufgerufen am 28.02.2023) (zuletzt aufgerufen am 28.02.2023)

[45] Siehe: Website der Bucerius Law School (2022): Center for Transnational IP, Media and Technology Law and Policy, https://www.law-school.de/international/research-faculty/institutes-centers/center-for-transnational-ip-media-and-technology-law-and-policy (zuletzt aufgerufen am 28.02.2023)

[46] Siehe: Website der Bucerius Law School (2022): Center for Legal Technology and Data Science, https://www.law-school.de/forschung-fakultaet/institute-und-zentren/center-for-legal-technology-and-data-science (zuletzt aufgerufen am 28.02.2023)

forscht man dort sowohl zu Partizipationsmodellen z.B. zur Integration öffentlicher Interessen in Regelsetzungsprozesse von Plattformen als auch zu Regulierungsansätzen für algorithmische Systeme.[47]

- Am Fachbereich Rechtswissenschaften der Universität Hamburg widmeten sich zum Beispiel Prof. Dr. Claudia Schubert sowie Prof. Dr. Hans Micklitz den Themen KI und Arbeitsrecht unter dem Projekttitel „Künstliche Intelligenz, Algorithmen und Plattformökonomie – Fairer Wettbewerb bei Waren und Dienstleistungen und die Zukunft der Arbeit".[48] Und am Zentrum für Recht in der digitalen Transformation (ZeRdiT)[49] an der Universität Hamburg forscht man zum Konnex Digitalisierung-Recht und arbeitet an Fragen zur Transformation des Rechts durch den digitalen Wandel.
- Am Fachbereich Rechtswissenschaften der Universität Hamburg gibt es im Rahmen der Schwerpunktausbildung darüber hinaus den Schwerpunktbereich VII: Information und Kommunikation u.a. Datenschutzrecht, Urheberrecht, Telekommunikationsrecht[50] , sowie am Fachbereich Informatik den Kernbereich „Human-Centered Computing".[51] Ferner gibt es in dem selben Fachbereich die Research Group Ethics in Information Technology (EIT)[52] unter der Leitung von Frau Prof. Dr. Judith Simon, die u.a. auch Mitglied der Datenethikkommission der Bundesregierung war.[53]
- An der Hochschule für Angewandte Wissenschaften (HAW) gibt es die dualen Studiengänge Public Management[54] sowie E-Government/Verwaltungsinformatik. Beteiligt sind u.a. vier Fachdisziplinen: Informatik, Wirtschaftswissenschaften, Rechtswissenschaften und Sozialwissenschaften.[55] Auch diese Studiengänge bieten keine unmittelbare Anlaufstelle für KMU, bereiten aber mit ihren integrierten Praxisphasen in der Hamburger Verwaltung auf den

[47] Siehe: Website des Leibniz Institut für Medienforschung Hans-Bredow-Institut (2019): Die Forschung des Instituts, https://leibniz-hbi.de/de/forschung (zuletzt aufgerufen am 28.02.2023)

[48] Siehe: Website der Universität Hamburg (2023): Aktuelle Forschungsvorhaben, https://www.jura.uni-hamburg.de/die-fakultaet/professuren/schubert/forschung/aktuell-forschungsvorhaben.html (zuletzt aufgerufen am 28.02.2023)

[49] Siehe: Website der Universität Hamburg (2023): Zentrum für Recht in der digitalen Transformation (Zerdit, https://www.jura.uni-hamburg.de/forschung/institute-forschungsstellen-und-zentren/digitalisierung-und-recht.html (zuletzt aufgerufen am 28.02.2023)

[50] Universität Hamburg (2021): Schwerpunktbereich VII: Information und Kommunikation, https://www.jura.uni-hamburg.de/media/studium/studiengang-rws/schwerpunktbereichsstudium/spb-07-info.pdf (zuletzt aufgerufen am 28.02.2023)

[51] Siehe: Website der Universität Hamburg (2023): Kernbereich "Human-Centered Computing", https://www.inf.uni-hamburg.de/research/hcc.html (zuletzt aufgerufen am 28.02.2023)

[52] Siehe Website der Universität Hamburg (2023): Ethics in it, https://www.inf.uni-hamburg.de/en/inst/ab/eit.html (zuletzt aufgerufen am 28.02.2023)

[53] Siehe Website des Bundesministerium des Inneren und für Heimat (2023): Mitglieder der Dathenethikkommission, https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/datenethikkommission/mitglieder-der-dek/mitglieder-der-dek-node.html (zuletzt aufgerufen am 28.02.2023)

[54] Siehe: Website der HAW Hamburg (2023): Department Public Management, https://www.haw-hamburg.de/public-management/ (zuletzt aufgerufen am 28.02.2023)

[55] Siehe: Website der HAW Hamburg (2023): Studiengänge, https://www.haw-hamburg.de/studium/studiengaenge-a-z/?graduation=Bachelor&subject=Wirtschaft+und+Verwaltung (zuletzt aufgerufen am 28.02.2023)

tatsächlichen Umgang mit KI-relevanten Fragen in der praktischen Arbeit vor. Die Praxisorientierung der Studiengänge ist vielversprechend, fokussiert sich aber in erster Linie auf die Ausbildung von Verwaltungsangestellten. Darüber hinaus bietet die HAW im Rahmen der sogenannten KI-Werkstatt ein Angebot für Studierende, sich längerfristig mit Themen rundum KI auseinanderzusetzen und im Zuge dessen weitere Kompetenzen im Umgang mit KI aufzubauen.[56]

Aus den vielfältigen Aktivitäten innerhalb der Bildungs-, Forschungs- und Wissenschaftslandschaft Hamburgs allein lassen sich bisher keine institutionalisierten Ansprechpartner:innen oder Beratungstools für KMU ableiten. Wenn auch an verschiedenen Stellen eine Öffnung der Wissenschaft hin zur Praxis stattfindet und Akteure wie ARIC e.V. oder auch die KI-Stakeholderrunde der Hamburger Senatskanzlei bemüht sind, einen kontinuierlichen Austausch verschiedenster Akteure zu organisieren und zu gewährleisten, so dienen diese jedoch nicht als Anlaufstellen für KMU in ihren unmittelbaren rechtlich motivierten Anwendungsfragen.

4.3 Ein Blick in das Beratungsangebot

In Hamburg bieten sich dennoch verschiedene Anlaufstellen für KMU an, um eine Beratung zum rechtssicheren Einsatz von KI in Unternehmen einzuholen. Viele dieser Angebote, in denen es aus Sicht der KMU auch um Fragen der Zertifizierung gehen müsste oder Test- und Validierungsverfahren möglich sein sollten, sind jedoch entweder sehr kostenintensiv und bedeuten für die Unternehmen eine unverhältnismäßige Belastung oder sie nehmen die rechtliche Perspektive kaum in den Blick. Ziel muss es jedoch sein, dass Entwickler:innen bzw. KMU den Einsatz von KI in all seinen Dimensionen, wie Kosten, Zeitabläufen oder eben auch rechtlichen Verpflichtungen frühzeitig und bestmöglich einschätzen lernen, um eine fundierte Entscheidung über den Einsatz der Technik schon zu Beginn der Entwicklungsphase zu ermöglichen. Einige Akteure in der Stadt haben bereits Angebote in diese Richtung entwickelt, um damit auch den Wirtschaftsstandort zu stärken. Die Anbieter:innen lassen sich unterscheiden zwischen Verbänden und einzelnen Initiativen sowie gewerblichen Anbietern und Körperschaften des öffentlichen Rechts. Einige ihrer Aktivitäten werden hier exemplarisch vorgestellt:

- Das Artificial Intelligence Center Hamburg (ARIC e.V.) ist ein eingetragener Verein, der an der Schnittstelle von Wirtschaft, Wissenschaft und Gesellschaft den verantwortungsvollen Einsatz von KI in der Metropolregion Hamburg fördert. Branchen- und themenübergreifend bündelt es Wissen, vernetzt Akteure und ist zentraler Ansprechpartner für Fragen rund um KI. Im Rahmen diverser Konsortialprojekte sowie Informations- und Beratungsangebote setzt es sich dafür ein, das Thema RAI in Hamburg voranzutreiben.
- Das Das Mittelstand-Digital-Zentrum stellt in Hamburg eine konkrete und praktische Unterstützung für KMU beim Einsatz Künstlicher Intelligenz zur Verfügung und arbeitet zu diesen Fragen in enger Kooperation mit der Handelskammer Hamburg. Eigene KI-Trainer:innen stellen in Informationsveranstaltungen Anwendungsfälle vor und ermöglichen so, den gegenseitigen Austausch zu fördern und aus den Erfahrungen Dritter zu lernen. Darüber hinaus findet eine

[56] Siehe: Website der HAW Hamburg: Fakultät Wirtschaft und Soziales, https://www.haw-hamburg.de/hochschule/wirtschaft-und-soziales/studium-und-lehre/digitale-medien/ki-werkstatt/ (zuletzt aufgerufen am 27.02.2023)

monatliche KI-Sprechstunde statt, in der KMU gezielt auf das eigene Unternehmen fokussierte Fragen an die Trainer:innen richten können.[57] Zudem können KMU sich im Rahmen von Umsetzungsprojekten von KI-Expert:innen begleiten lassen. Allerdings sind sowohl die Informationsveranstaltungen als auch die vom Mittelstand-Digital-Zentrum angebotenen Umsetzungsworkshops und -projekte auf wirtschaftliche Potentiale entlang der Lieferkette fokussiert und haben kaum die Rechtsperspektive im Blick. Darüber hinaus handelt es sich um eine zeitlich befristete Projektförderung, sodass nicht gewährleistet ist, dass das Angebot auf Dauer bestehen bleibt.

- Das Regionale Zukunftszentrum Nord (RZ), eine durch das Bundesministerium für Arbeit und Soziales und die EU gefördertes Projekt, ist ein wichtiger Ansprechpartner für KMU und unterstützt sie und deren Beschäftigte beim Einsatz von KI in Arbeits- und Geschäftsabläufen und bei internen Prozessen zum Wissensaufbau rundum KI sowie bei Entwicklungs- und Innovationsprozessen.
- Das Hamburger Informatik Technologie-Center (HITeC) ist am Fachbereich Informatik der Universität Hamburg angesiedelt und verfolgt als eingetragener Verein das Ziel, anwendungsorientierte Vorhaben durchzuführen, Kompetenzen aus der Informatik zu vermitteln, Kontakte zwischen Unternehmen und Studierenden herzustellen sowie bei Unternehmensgründungen zu unterstützen.[58]
- Das European Digital Innovation Hub (EDIH) ist Teil eines EU Flagship Projektes im Rahmen des EU-Programms „Digitales Europa" und soll sich als Anlaufstelle insbesondere für die Wirtschaft etablieren, um durch technische Unterstützung und die Möglichkeit von experimentellem Testen die Wettbewerbsfähigkeit europäischer Unternehmen zu verbessern. Ziel ist es, europaweit Drehkreuze für KI-Wissensaustausch und -Förderung zu gründen und ein ganzes Netzwerk zur Unterstützung der Transformation in Unternehmen und Verwaltung aufzubauen. In Norddeutschland ist ein bundesländerübergreifendes Konsortium aus Unternehmen und dem öffentlichen Sektor im Herbst 2022 an den Start gegangen. Unternehmen in Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein können nunmehr Unterstützungsangebote bei der digitalen Transformation anfordern. Als Zusammenschluss verschiedener Akteure (ARIC e.V., HITeC, Mittelstand Digital Zentrum, DigitalHubLogistics und weitere Partner) richten sich die Angebote des EDIH an Unternehmen aller Größen, insbesondere KMU, Midcaps, Scale-ups und an den öffentlichen Sektor. Deutschlandweit sind im Jahr 2022 14 solcher Konsortien gestartet, in 2023 werden weitere Zusammenschlüsse erwartet.[59]
- Verschiedene Rechtsanwaltskanzleien und große Unternehmensberatungen mit eigener Rechtsabteilung haben die Digitalisierung als ein lukratives Geschäftsfeld entdeckt und sind ebenfalls in der KMU-Beratung tätig. Sie unterstützen Unternehmen im Markt bei allen Fragen der Digitalisierung, von Big Data über Augmented Reality bis zu Künstlicher Intelligenz. Von diesen

[57] Siehe: Website der Handelskammer Hamburg: KI-Sprechstunde, https://www.ihk.de/hamburg/system/vst/1198812?id=376537&terminId=645764 (zuletzt aufgerufen am 28.02.2023)
[58] Siehe: Website des HITeC (2022), https://www.hitec-hamburg.de/ (zuletzt aufgerufen am 28.02.2023)
[59] Siehe: Website des Bundesministeriums für Wirtschaft und Klimaschutz: European Digital Innovation Hubs, https://www.de.digital/DIGITAL/Redaktion/DE/Dossier/european-digital-innovation-hubs.html (zuletzt aufgerufen am 28.02.2023)

gewerblich orientierten Akteuren werden beispielsweise neben der genuin juristischen Beratung auch mediale Formate, in denen sich mit der Schnittstelle Recht und Technologie auseinandergesetzt wird, angeboten.

4.4 Ein Blick auf die Prüforganisationen: Eine Zertifizierungsstelle für Hamburg

Das oben bereits erwähnte und von der Unternehmensberatung PWC und der Prüfgesellschaft DEKRA neu gegründete Unternehmen CertifAI sticht an dieser Stelle ein Stück weit heraus und wird daher gesondert vorgestellt. CertifAI wird in Hamburg zukünftig – vorbehaltlich der Genehmigung durch die Wettbewerbsbehörden – als Prüfungs- und Zertifizierungsstelle tätig werden und positioniert sich damit bereits jetzt im Markt, um auch nach Inkrafttreten des KI-Acts für die entsprechenden Konformitätsprüfungen zur Verfügung zu stehen. Ziel des Joint Ventures ist es, KI-Produkte von der Entwicklung bis hin zum Markteintritt zu begleiten und Unternehmen dabei zu unterstützen, Normen und regulatorische Vorgaben für KI basierte Produkte einzuhalten. Explizit wollen sie einen verantwortungsvollen Umgang mit KI fördern und dies mit einer kundenorientierten Beratung verbinden. Da sich CertifAI noch im Aufbau befindet, ist noch nicht abschließend absehbar, wie sich der Akteur gegenüber KMU als Ansprechpartner genau etablieren wird.

Vor dem Hintergrund, dass bisher wenig Angebote existieren, die genuin rechtliche Fragen zum Einsatz von KI in KMU in den Blick nehmen, erscheint eine gezielte Erweiterung des Angebots in dieser Hinsicht ratsam. Sollte sich mit CertifAI ein Akteur auf dem Markt etablieren, der auch für die aus dem KI-Act hervorgehenden Verpflichtungen zur Konformitätsprüfung als Ansprechpartner für KMU dient, so bleibt an dieser Stelle zu klären, inwiefern dies rechtskonform möglich ist. Beratung und Zertifizierung dürfen nach jetzigem Kenntnisstand laut KI-Act nicht in gleicher Hand liegen (Art. 30 Abs. 5 KI-Act Entwurf), sodass die derzeitige Einschätzung ist, dass hier verschiedene Anbieter:innen für die jeweiligen Teilbereiche werden zuständig sein müssen. Dass aber schon in der Entwicklungsphase neuer KI-Systeme die Anforderungen – sei es aus dem KI-Act oder abgeleitet aus dem Konzept der RAI – an vertrauenswürdige KI mitbedacht und Unternehmen in der Implementierung unterstützt werden, scheint von elementarer Bedeutung für die Akteure am Wirtschaftsstandort Hamburg. Hiermit können sich Hamburg und seine Unternehmen nicht nur im europäischen Wettbewerb positionieren, sondern sich auch als verantwortliche Akteure in der Debatte um einen demokratischen und rechtssicheren Einsatz Künstlicher Intelligenz etablieren. Ein ausgebautes und umfängliches KI-Ökosystem, zu dem auch Angebote der Konformitätsprüfung und Zertifizierung gehören, ist dafür unerlässlich.

5. Was auf Hamburger KMU und die Stadt mit dem KI-Act zukommt

Neben den oben dargestellten Anforderungen entlang der Risikostufen sowie den allgemein begründbaren Notwendigkeiten eines verantwortlichen Einsatzes Künstlicher Intelligenz in Hamburger KMU finden sich im vorliegenden Entwurf des KI-Acts durch die EU-Kommission auch Hinweise auf Erleichterungen und Unterstützungsleistungen, um die Innovationsfähigkeit innerhalb der EU explizit auch für KMU zu fördern. Der neu zu schaffende Rechtsrahmen soll damit nicht nur reglementierend wirken, sondern auch Räume bieten für gegenseitiges Lernen, für Förderung und Testung von Entwicklungsversuchen in frühem Stadium. Diese als Reallabor bezeichneten geschützten Räume

scheinen anschlussfähig an Aktivitäten und politische Ziele der Freien und Hansestadt Hamburg sowohl im Hinblick auf Entwicklungen im öffentlichen Sektor als auch in der KMU-Landschaft.

So haben sich in einem Positionspapier auch die Digitalminister:innen der Länder am 12.12.2022 dafür ausgesprochen, im Sinne des KI-Acts gezielte Innovationsförderung zu betreiben und über den KI-Act hinausgehende Angebote zu machen, um ein möglichst weites Spektrum an KI-Systemen in Reallaboren testen zu können.[60] Hamburg positioniert sich gemeinsam mit den anderen Ländern somit als grundsätzlicher Unterstützer einer KI-Regulierung, die jedoch nicht innovationshemmend wirken soll. Zugleich betonen sie, dass der europäische Binnenmarkt als Standort für eine vertrauenswürdige KI auf- und ausgebaut werden sollte. Davon versprechen sie sich grundsätzliche Standortvorteile auch innerhalb der EU.

Der Logik der Bedeutung von Testverfahren und Reallaboren auch für die Standortsicherung innerhalb Europas wurde auf europäischer Ebene insbesondere im gemeinsamen Standpunkt des Europäischen Rats Rechnung getragen. Dieser hat die Möglichkeit einer Testung von KI-Systemen unter realen Bedingungen und unter bestimmten Auflagen als für die Innovationsförderung im europäischen Binnenmarkt unerlässlich beschrieben. Hier weichen allerdings erneut Kommissions- und Ratsentwurf voneinander ab und es bleibt abzuwarten, inwiefern eine Einigung im weiteren Gesetzgebungsprozess aussehen wird. Ungeachtet der konkreten und von den europäischen Regulierungsbemühungen sowie -anforderungen noch unberührten Aktivitäten in Hamburg bietet der KI-Act jedoch verschiedene Ansätze, wie KMU gezielt unterstützt oder entlastet werden sollten.

5.1 KMU im KI-Act

Der KI-Act beinhaltet eine Reihe von Vorkehrungen, die spezifisch auf KMU ausgerichtet sind. Dazu gehören ein bevorzugter Zugang zu KI-Reallaboren, Informations- und Beratungsangebote mit Blick auf den KI-Act, ein reduzierter Preis für Konformitätsbewertungen, eine Unterstützung bei der Aufstellung von Verhaltenskodizes und eine Berücksichtigung der Unternehmensgröße und des wirtschaftlichen Überlebens bei der Bestimmung der Höhe von Sanktionen. Der Kompromisstext des Rates ergänzt einige weitere Erleichterungen für KMU.

Mit dem Inkrafttreten des KI-Acts und dem damit entstehenden, unmittelbar geltenden Recht in allen Mitgliedstaaten verpflichten sich diese laut KI-Act, KMU auch gezielt zu unterstützen und bestimmte Strukturen und Ansprechpartner:innen vorzuhalten, die die Innovationsfähigkeit des europäischen Standorts insgesamt stärken und zugleich einen verantwortlichen Umgang mit der Technologie sichern. Einige Auszüge des KI-Acts, die sich explizit auf KMU beziehen, werden im Folgenden beispielhaft zusammengefasst.

In erster Linie sollen Unternehmen und potentielle KI-Entwickler:innen darin unterstützt werden, ihre Systeme testen zu können und sie somit faktisch auch im Sinne der RAI zu optimieren. Hierfür werden die Mitgliedstaaten angehalten, Reallabore zu errichten. Niederschlag findet dies im Kommissionsentwurf

[60] Beschluss des Digitalministertreffens D16 (12.12.2022): Positionierung der Länder gegenüber der geplanten KI-Verordnung der Europäischen Union, https://im.baden-wuerttemberg.de/fileadmin/redaktion/m-im/intern/dateien/pdf/20221212_Positionierung_der_Laender_gegenüber_der_geplanten_KI-Verordnung_der_Europaeischen_Union.pdf (zuletzt aufgerufen am 16.02.2023)

ununter Art. 53 Abs. 1 a) KI-Act Entwurf). Insbesondere in Art. 55 KI-Act Entwurf finden sich darüber hinaus Erleichterungen und Unterstützungsmaßnahmen für KMU. So sieht der KI-Act Entwurf vor, dass KMU bevorzugten Zugang zu KI-Reallaboren erhalten und ganz im Sinne der hier vorliegenden Studie KMU für die Anforderungen eines verantwortlichen Einsatzes von KI bedarfsgerecht sensibilisiert werden sollen. Hierzu wird die mögliche Einrichtung eines eigenen Kommunikationskanals für die Zielgruppe KMU in den Raum gestellt, um Orientierung mit Blick auf den KI-Act zu geben und Fragen zu beantworten (Art. 55 a) KI-Act Entwurf). Außerdem sollen gemäß Art. 69 Abs. 4 KI-Act Entwurf) die besonderen Interessen und Bedürfnisse von Kleinanbieter:innen und Start-ups bei der Förderung und Erleichterung der Aufstellung von Verhaltenskodizes berücksichtigt werden. Schließlich sieht der Kommissionsentwurf zwei finanzielle Erleichterungen für KMU vor: Zum einen sollen KMU Konformitätsbewertungen zu einem reduzierten Preis in Anspruch nehmen können (Art. 55 Abs. 2 KI-Act Entwurf). Zum anderen soll die Unternehmensgröße und das wirtschaftliche Überleben von KMU und Start-ups bei der Bestimmung der Höhe möglicher Sanktionen berücksichtigt werden (Art. 71 Abs. 1 KI-Act Entwurf).

Im Kompromisstext des Rates werden die Unterstützungsmaßnahmen für kleine und mittlere Unternehmen an einigen Stellen ausgeweitet. Zum einen wird KMU in Art. 11 Abs. 1 KI-Act Ratsentwurf) die Möglichkeit eingeräumt, die Angaben der technischen Dokumentation in abweichender Form darzulegen, sofern die Unterlagen für den jeweiligen Zweck gleichwertig sind. Die auch schon im Kommissionsentwurf vorgesehenen Sensibilisierungsmaßnahmen (Art. 55 Abs. 1 b) KI-Act Entwurf) werden zudem durch den Rat um Schulungsmaßnahmen ergänzt. Auch eine Reihe weiterer Informations- und Beratungsleistungen soll für Kleinanbieter:innen und Kleinnutzer:innen zur Verfügung gestellt werden (Art. 55 Abs. 3 KI-Act Ratsentwurf). Damit wird die Kommission in der Ratsfassung stärker in die Pflicht genommen, wie sich vor allem in Art. 55 KI-Act Ratsentwurf zeigt. Mitgliedstaaten sind nach Art. 59 Abs. 7 KI-Act Entwurf darüber hinaus angehalten, selbst Beratung anzubieten, die sich gezielt an KMU und Start-ups richtet.

Mit der Formulierung, dass unter definierten Vorgaben auch eine „unbeaufsichtigte" Erprobung möglich ist, geht der Rat zudem auf die realen Bedingungen für Unternehmen ein. Er schlägt eine Ergänzung des Gesetzestextes um Art. 54 a) KI-Act Ratsentwurf und 54 b) KI-Act Ratsentwurf vor. Dabei sieht Art. 55 a) KI-Act Ratsentwurf für Kleinstunternehmen eine wesentliche zusätzliche Erleichterung vor: Für diese Unternehmen besteht nicht die Pflicht, ein Qualitätsmanagementsystem nach Art. 17 KI-Act Entwurf einzuführen. Der Rat begründet diese Entscheidung mit dem Argument, dass die Einführung eines Qualitätsmanagementsystems unverhältnismäßig angesichts der Größe der Akteure sei und der damit einhergehende Verwaltungsaufwand und die entstehenden Kosten für die Unternehmen verringert werden könnten, ohne das Schutzniveau und die Notwendigkeit der Einhaltung der Anforderungen für Hochrisiko-KI-Systeme zu beeinträchtigen (Art. 74 a) KI-Act Ratsentwurf). Diese Erleichterung greift jedoch nur, sofern das betroffene Kleinstunternehmen kein Partner- oder verbundenes Unternehmen hat, welches definitionsgemäß nicht zu KMU zählt. KMU ohne größere Partner:innen würden demnach befreit von aufwändigen Test- und Validierungsverfahren, vor, während und nach der Entwicklung des KI-Systems und müssten auch nicht alle Anforderungen an das Datenmanagement vollumfänglich erfüllen. Unter derselben Einschränkung gelten zudem für Kleinstunternehmen und KMU die Anforderungen und Pflichten für KI-Systeme mit allgemeinem Verwendungszweck gemäß Art 4 b) KI-Act Entwurf nicht. Schließlich geht der Ratstext über den Kommissionsentwurf hinaus, indem in Art. 71 KI-Act Ratsentwurf die Einschränkungen für die Höhe der Sanktionen für KMU spezifiziert werden.

Die Erleichterungen für KMU sind insgesamt dennoch nicht sehr weitreichend. KMU sind weiterhin wesentlich durch Anforderungen des KI-Acts betroffen. Zudem ist die Ausnahme im Hinblick auf die Qualitätsmanagementsysteme insofern nur begrenzt erleichternd, als dass weiterhin Art. 9 KI-Act Entwurf (Risikomanagement), Art. 61 KI-Act Entwurf (Beobachtung nach dem Inverkehrbringen durch die Anbieter und Plan für die Beobachtung nach dem Inverkehrbringen für Hochrisiko-KI-Systeme) und Art. 62 KI-Act Entwurf (Meldung schwerwiegender Vorfälle und Fehlfunktionen) einzuhalten wären.

Die genannten Bestandteile des KI-Acts zeigen jedoch eine erste Beratungs- und Zuständigkeitsstruktur auf, die den KMU in der Entwicklung und Implementierung von KI helfen kann und zugleich die Innovationsförderung vorantreiben soll. Sie bedeutet für Hamburg, dass auch hier vor Ort Strukturen aus- und aufgebaut werden sollten, die entsprechend den Anforderungen im KI-Act eine (Rechts-)Beratung für KMU zur Umsetzung der Verordnung vorhalten kann und darüber hinaus Anlaufstellen etabliert werden, die eine niedrigschwellige Auskunft gerade in der Anfangsphase der Entwicklung ermöglichen.

Für Hamburg bedeuten entsprechend insbesondere die Regelungen aus Art. 55 sowie Art. 59 KI-Act Ratsentwurf, dass die Stadt nicht nur gut beraten ist, eine Konformitätsbewertungsstelle vor Ort zu etablieren, sondern auch auf KMU zielende Beratungsangebote vorzuhalten, die die Einhaltung der Regeln des KI-Acts ermöglichen, ohne den Innovationsprozess zu hemmen. Auch die Bundesländer unterstreichen mit ihrem Beschluss vom 12. Dezember 2022, dass sie in diesem Sinne insbesondere für Innovation und Forschung eine bestmögliche Umgebung wünschen und sich daher dafür aussprechen, „...Forschungs-, Erprobungs- und Entwicklungstätigkeiten im Zusammenhang mit KI-Systemen vom Anwendungsbereich der Verordnung auszunehmen ...".[61]

5.2 Checkliste für Hamburger KMU

Hamburger KMU müssen ihre KI-Anwendungen in Zukunft in die Risikokategorien nach KI-Act einordnen können, um die für sie geltenden Anforderungen erfüllen zu können. Im Folgenden wird ein dreistufiges Prüfverfahren in Form einer Checkliste skizziert, das KMU eine systematische Selbsteinschätzung ermöglichen soll.

Über die Einrichtung von Beratungsstellen und Reallaboren hinaus, kann als praktisches Tool für KMU eine Checkliste als Orientierungshilfe dienen, welche Anforderungen bei der Entwicklung und Implementierung auf die Akteure zukommen. Sie soll den Einsatz von KI-Systemen nicht nur erleichtern und Hinweise geben zu einer rechtssicheren Gestaltung, sondern ihn insgesamt wahrscheinlicher machen. Daher wird im Folgenden die Idee und Systematik einer Checkliste vorgestellt, die sich jedoch – anders als zuvor entlang des Konzepts von RAI argumentiert – ausschließlich an den Vorgaben des Verordnungsentwurfs zum KI-Act der EU-Kommission orientiert.

Vorrangiges Ziel des Entwurfes (vgl. Checkliste im Anhang) ist es, KMU dabei zu unterstützen, ihre eigene Betroffenheit durch den KI-Act systematisch einordnen zu können. Insbesondere vor dem Hintergrund, dass die endgültige Fassung des KI-Acts zum Zeitpunkt der Verfassung dieser Studie noch nicht bekannt ist, steht der Inhalt der Checkliste unter Vorbehalt. Zudem sollte die Checkliste im Sinne der Nutzer:innenfreundlichkeit und Übersichtlichkeit perspektivisch in digitaler Form umgesetzt werden.

[61] ebenda

Die Checkliste ist so konzipiert, dass KMU für geplante oder bereits bestehende KI-Anwendungen anhand von Fragen zum konkreten Anwendungsfall feststellen können, welche Anforderungen durch den KI-Act an ihre geplante oder bestehende Anwendung gestellt werden. Aufgrund der Kontextspezifität, die dem risikobasierten Ansatz des KI-Acts zugrunde liegt, ist die Checkliste ebenfalls als Instrument für jeweils einen konkreten Anwendungsfall konzipiert. Da zwei im Wesentlichen ähnliche technische Implementierungen in Abhängigkeit des Einsatzkontextes der KI nach dem KI-Act vollkommen unterschiedlich zu bewerten sein können, ist eine allgemeine, anwendungsfallunspezifische Nutzung der Checkliste nicht sinnvoll.

Die Checkliste prüft einen gegebenen Anwendungsfall nach dem folgenden Schema:

- Zunächst geht es darum festzustellen, ob die technische Lösung nach Definition des KI-Acts als KI einzustufen ist. Ist dem nicht so, so muss das KMU den KI-Act rein rechtlich nicht weiter beachten. Handelt es sich hingegen um eine technische Lösung, die unter die KI-Definition fällt, so muss das KMU den nächsten Abschnitt der Checkliste durchlaufen.
- Im zweiten Schritt geht es darum zu prüfen, in welche der vier Risikokategorien der gegebene Anwendungsfall einzuordnen ist. Anhand von Fragen können Anwendungsfälle in die Kategorien „verbotene KI", „Hochrisiko-KI" oder „geringes Risiko" eingeordnet werden. Die minimale Risiko Kategorie ergibt sich nach dem Ausschlussprinzip, wenn keine der anderen Kategorien zutrifft; diese ist auch im KI-Act nicht weiter spezifiziert. Im Fall des minimalen Risikos erwachsen keine Anforderungen an das KMU. Im Fall des verbotenen Risikos ist die KI-Entwicklung/ -Nutzung entsprechend einzustellen. Fällt die KI in die geringe Risikokategorie, werden die Anforderungen (im Wesentlichen Transparenzpflichten) an die KMU als Ergebnis der Checkliste genannt. Ist der Anwendungsfall des KMU als Hochrisiko-KI einzustufen, so muss der nächste Abschnitt der Checkliste durchlaufen werden.
- Im dritten Abschnitt der Checkliste gilt es zu prüfen, welche Rolle das KMU in Bezug auf die KI einnimmt, da für Hochrisiko-KI in Abhängigkeit der Rolle unterschiedliche Rechte und Pflichten erwachsen. Die möglichen Rollen umfassen Anbieter:innen, Produkthersteller:innen, Bevollmächtigte, Einführer:innen, Händler:innen und Nutzer:innen. Zu bedenken ist außerdem, dass sich die Rollenzuordnung ändern kann, insbesondere wenn eine von einem KMU eingekaufte KI-Lösung durch weiteres Training wesentlich verändert wird, sodass das KMU nicht länger als Nutzer, sondern als Anbieter einzustufen ist und damit deutlich höheren Anforderungen seitens des KI-Acts unterliegt.
- Als Ergebnis der Checkliste werden die Anforderungen an das KMU in Abhängigkeit von Risikokategorie und Rolle dargestellt. Insbesondere hier liegt mit Blick auf die unterschiedlichen Kombinationsmöglichkeiten ein wesentlicher Vorteil einer digitalen Umsetzung der Checkliste. Aus Gründen der Übersichtlichkeit wird deshalb auf eine Aufführung der möglichen Kombinationen im Anhang verzichtet.

Darüber hinaus gibt es im Prozess der Prüfung verschiedene Phasen, in denen sich – wie gerade bereits kursorisch beschrieben – Rollenzuweisungen ändern können oder durch eine Weiterentwicklung der KI erneute Prüfprozesse erforderlich werden. Vor diesem Hintergrund sind bei Durchlaufen der Checkliste verschiedene Hinweise als Output zu erwarten, die entsprechend auf die verschiedenen Anforderungen in Bezug auf Rolle und Zeitpunkt des Entwicklungs- und Vermarktungsprozesses eingehen. So lässt sich über die oben genannten Schritte hinaus folgendes festhalten:

1) In der Phase der Inbetriebnahme eines KI-Systems kann der:die Adressat:in der in der Checkliste genannten Sorgfaltspflichten wechseln, da der:die Kund:in, der:die das System verwendet, durchaus in die Lage versetzt werden kann, das System weiterzuentwickeln. Es gibt demnach auch spezifische Sorgfaltspflichten, die sich auf das Training der KI beziehen. Methodisch spricht man hier z.B. von der Validierung der Trainingsdaten bzw. einem Datenqualitätsmanagement, um zu gewährleisten, dass die Daten etwa korrekt und biasfrei sind – auch bei einem erneuten oder erweiterten Training.
2) Ein zweites Pflichtelement ist es, zu testen, ob die Verwendung der Daten bzw. die Funktion der Daten den Vorstellungen aus der Design- bzw. Konzeptionsphase entsprechen, dass also die Prognoseentscheidung mit einem hinreichenden Grad an Wahrscheinlichkeit dem entspricht, was bei einer händischen Berechnung herauskäme.
3) Zudem sind die angemessenen Instruktionspflichten nach dem Produktsicherheitsgesetz einzuhalten wie u.a. Betriebsanleitung mit Informationen über die sachgerechte Nutzung, Eigenschaften und Sicherheitsinformationen. Die Produkt- und Marktbeobachtung ist in der Phase der Implementierung von KI besonders relevant, da die KI sich nach Inverkehrbringung weiterhin verändern kann. Der:die Hersteller:in muss vor Inverkehrbringen sowie in der Phase des Betriebs eine Produkt- und Marktbeobachtung vornehmen und Faktoren ermitteln, die ggf. zu einer fehlehrhaften Nutzung führen können. Hierbei geht es sowohl um eine passive Marktbeobachtung (bspw. Entgegenahme von Reklamationen) als auch um eine aktive Marktbeobachtung (bspw. Informationsbeschaffung über das Produkt im Markt, wie einer Unfallanalyse u.ä.).

In der letztendlichen Umsetzung der Checkliste ist im Sinne der Nutzer:innenfreundlichkeit zu erwägen, ob es einen alternativen Einstiegspunkt über die Einordnung als Nutzer:in von KI geben sollte, da hier nur im Fall von Hochrisiko-KI zwingend rechtliche Pflichten erwachsen. Ein vollständiges Durchlaufen der Checkliste wäre ein entsprechend unverhältnismäßiger Aufwand im Vergleich zu den aus dem KI-Act entstehenden Pflichten. In Abhängigkeit des weiteren Gesetzgebungsprozesses sind außerdem Ergänzungen und Änderungen zu erwarten. Beispielsweise sind aus dem gemeinsamen Standpunkt des Rates von Dezember 2022 die Sonderrolle von KI-Entwicklung/-Nutzung zu Forschungszwecken sowie die Konkretisierung, die private/nicht-berufliche Nutzung/Entwicklung von KI vom Geltungsbereich des KI-Acts ausgenommen worden (siehe hierzu auch 2.2 der vorliegenden Studie). Diese Anpassungen können für die tatsächliche Entwicklung und Anwendung von KI-Systemen in der Praxis durchaus relevante Punkte werden, sofern sie sich in der Kompromissfindung zwischen den am Gesetzgebungsprozess beteiligten Akteuren durchsetzen.

5.3 Technische Lösungen im Sinne einer RAI

Die Herausforderungen, die der Einsatz von KI im Mittelstand mit sich bringt, können zum Teil mit verschiedenen technischen Lösungen, im Sinne der RAI, gelöst werden. Orientierung bieten die aus bereits bestehenden Normungsansätzen bekannten Kriterien: Fairness & Nachhaltigkeit, Erklärbarkeit & Transparenz, Robustheit & Sicherheit sowie Governance bzw. Qualitätssicherung / Validierung und Verifikation.

Aufgrund der systemimmanenten Komplexität von KI, kann der KI-Act lediglich einen bestimmten Teil einer Risikominimierung abdecken, der zum vertrauensvollen Einsatz von KI verhilft. Um den KMU einen

weiteren Ansatz zur Risikominimierung zu bieten, bedarf es einer Kombination aus der Erfüllung des zukünftig geltenden Rechts (KI-Act) mit der Erfüllung der in Kapitel 3 beschriebenen RAI-Kriterien. Für KMU, die sich also an den Anforderungen einer RAI im Entwicklungsprozess orientieren wollen und eine praktische Übersetzung des theoretischen Konzepts einer RAI wünschen, werden im Folgenden einige Kriterien einer RAI als praktische, technische Lösungsansätze vorgestellt. Diese Lösungsansätze bieten (auch unter Berücksichtigung der Checkliste) die Möglichkeit, ethische sowie rechtliche Fragen bereits vor Inverkehrbringung des KI-Systems zu antizipieren und sie möglicherweise zu klären. Sie orientieren sich entlang der Kriterien oder Leitideen von RAI, die zuvor in Kapitel 3 vorgestellt wurden: *Fairness & Nachhaltigkeit, Erklärbarkeit* (inkl. Transparenz), *Robustheit & Sicherheit* sowie *Governance* in Bezug auf *Qualitätssicherung und Verifikation*. Bestimmte Maßnahmen, wie etwa das Testen, können dabei auf mehrere Oberziele von RAI einzahlen, wie etwa *Robustheit*, *Erklärbarkeit* und *Governance*.

Allerdings muss die Darstellung derartig zum Teil rein normativer Konzepte und Ideen als gesellschaftlich kontingent betrachtet werden. Begriffe wie „Fairness" oder „Bias-Freiheit" können nur gesellschaftlich definiert werden und verändern sich über die Zeit in ihrem Gehalt dynamisch. Hier bedarf es einer kontinuierlichen gesellschaftlichen Debatte und eines – unter Umständen im geplanten Unterausschuss des KI-Ausschusses auf europäischer Ebene (siehe Kapitel 2.3 der vorliegenden Studie) angelegten – institutionalisierten Prozesses, in dem künftig geklärt werden kann, welche Formen von Risiken die Gesellschaft gewillt ist zu tragen und wie sich diese in bestimmte Kriterien übersetzen lassen. Eine abschließende Definition von „gerecht" oder „vorurteilsfrei" in technische Lösungen wird es daher kaum geben können. Die folgenden Darstellungen sind insofern lediglich als Annäherungen zu verstehen, die ein Bewusstsein für Möglichkeiten öffnen, wie mit ethischen Fragen im Entwicklungs- und Anwendungsprozess einer KI umgegangen werden kann und was dies praktisch im Entwicklungsprozess bedeutet.

- *Fairness & Nachhaltigkeit*

Zur Vermeidung eines sogenannten Bias (Voreingenommenheit), der auf verzerrte Trainingsdaten zurückzuführen ist und unter Umständen zu Diskriminierungen verschiedener Personengruppen führen kann, muss die Verteilung der Daten-Cluster von einem Menschen vorgenommen werden. Zur Vermeidung eines Bias (z.B. bei Personen) müssen z.B. alle Personengruppen in gleicher Anzahl im Trainingsdatensatz repräsentiert werden. Dies ist besonders bei großen Datenmengen zu beachten (insbesondere bei Verwendung von nicht überschaubaren Datenmengen). In diesem Fall muss bei der Qualitätssicherung ein erhöhter Aufwand betrieben werden und mit möglicherweise unterrepräsentierten Randgruppen das Verhalten des Systems getestet werden, um in der Folge eine Gleichbehandlung sicherzustellen.

Für eine Beurteilung, ob dem System ein Bias antrainiert wurde, braucht es dabei fachliche Unterstützung durch Personen, die die Funktionsweise der unterliegenden Systeme (Algorithmen) kennen. In diesem Bereich muss zwingend interdisziplinär, fachübergreifend und gleichberechtigt zusammengearbeitet werden, auch um die oben genannten gesellschaftlichen Entwicklungen stets mit reflektieren und die Systeme entsprechend anpassen zu können. Hierzu haben sich bereits Organisationen wie „Women in AI" und „Equal AI" gegründet, die das Ziel verfolgen, dem Thema Bias-Freiheit in KI-Systemen zu mehr Aufmerksamkeit zu verhelfen.

- *Erklärbarkeit / Transparenz*

Um eine hinreichende Transparenz eines Systems herzustellen, muss das Verhalten/die Entscheidung des Systems erklärbar, nachvollziehbar und wiederholbar sein. Um dies bei einem KI-System sicherzustellen, verwendet man den wissenschaftlichen Forschungszweig der Informatik – *Explainable AI*. Fachlich gehört dieser Prozess zum Testing. Generell gilt: Bei vielen KI-Verfahren/Algorithmen kann die Erklärbarkeit vollständig hergestellt werden (beispielweise bei Entscheidungsbäumen). Hierfür ist das übliche Testvorgehen ausreichend. Erklärbarkeit und Transparenz sind daher auch eng mit der Robustheit (s.u.) und dem Testing (siehe im Anhang die konkreten Schritte für Prozesse und Normen des Software Engineerings) verknüpft. Bei Systemen mit einem hohen Risiko im Anwendungsfall, wird meist ein mathematischer Beweis (z.B. durch die Herleitung über Gleichungssysteme) gefordert. Diese KI-Verfahren werden als White Box-Verfahren bezeichnet, da ihr Verhalten vorhersagbar und beweisbar ist und damit als transparent bezeichnet werden kann.

Anders verhält es sich im Fall sogenannter Black Box-Verfahren. Diese sind mathematisch nicht beweisbar. Hierzu zählen meist Verfahren, die künstliche neuronale Netze (Deep Learning, Reinforcement Learning etc.) enthalten. In diesen Verfahren kann keine vollständige Transparenz und Erklärbarkeit der Entscheidungsfindung des Systems sichergestellt werden. Die Funktionsfähigkeit kann hier nur durch Annäherung mit erhöhtem Testaufwand erfolgen. Es werden die Methoden des sogenannten Black Box-Testing herangezogen.

Beim Black Box-Testing werden überwiegend Testverfahren angewandt, die auf dem Grundsatz des „Ursache- Wirkungsgrads“ beruhen. Es steht dabei die Frage im Zentrum, ob das Ergebnis nach einer Eingabe logisch und erklärbar ist. Was aber nicht heißt, dass die Entscheidungsfindung des KI-Systems erklärbar wäre. Hierfür muss eine Teststrategie und ein Testdatensatz bereitgehalten werden, den das KI-System nicht kennt und der nicht in das Training eingeflossen ist. Diese Testdaten müssen im Voraus von Menschen bewertet und klassifiziert werden, damit eine Aussage über die Funktionsfähigkeit möglich ist.[62] Wie bei allen Softwaretests sollten auch die Grenzfälle und Negativtests mit einbezogen werden.

Bei Hochrisikosystemen werden oft hybride KI-Verfahren verwendet. Bei dieser Vorgehensweise wird das KI-System in den Grenzfällen durch mathematisch beweisbare Algorithmen in seiner Entscheidungsfreiheit begrenzt, um fatale Fehleinschätzungen des KI-Systems zu verhindern. Black Box-KI-Verfahren sind zurzeit noch der Forschungsgegenstand vieler Organisationen. Als Leitlinie können nur sogenannte Frameworks herangezogen werden, wie beispielweise das „Testing Framework for Black Box AI Models“ (IEEE, Print ISBN:978-1-6654-1219-3 / DOI: 10.1109/ICSE-Companion52605.2021.00041). Bei KI-Systemen, die auf Black Box-Verfahren beruhen, wird dringend empfohlen, diese Systeme von Dritten und unabhängigen Expert:innen prüfen zu lassen. Die Beurteilung der Funktionsweise von Black Box-Verfahren bedarf zurzeit leider noch jahrelange Erfahrung in diesem Bereich und darf keinesfalls vernachlässigt werden.

[62] Automatisierte Tests können hier nur Anhaltspunkte liefern und zeigen nur einen Trend der Funktion in der Entscheidungsfindung des KI-Systems auf. Hierzu wird oft das sog. *Fuzzing* benutzt, wobei das System mit Zufallsdaten oder synthetischen Daten über lange Zeit getestet wird. Dies lässt aber keine qualitative Aussage der Entscheidungsfindung zu.

- *Robustheit & Sicherheit*

Im Hinblick auf die Gewährleistung von Robustheit und Zuverlässigkeit eines Systems gilt grundsätzlich, dass es nach den Regeln und Normen des Software Engineerings zu entwickeln ist (S*afety and Security by design*).[63] Bei der Einführung eines neuen Systems muss dabei zwischen fertigen Software-Produkten und einer Neuentwicklung unterschieden werden. Basiert das KI-System auf einem fertigen Produkt muss darauf geachtet werden, dass dieses Produkt zwingend nach den Vorgaben des Software Engineering entwickelt wurde (kenntlich bisher durch *ISO* oder ggf. *IEEE*-Zertifizierungen). Bei der Vergabe von Aufträgen sollte überprüft werden, ob der:die Auftragnehmer:in die im Anhang unter *Prozesse und Normen des Softwareengineerings* dargelegten Prozesse tatsächlich anwendet. Wird dagegen eine Neuentwicklung angestrebt, müssen die Vorgehensmodelle erst geschaffen werden, um zu garantieren, dass die Vorgaben eingehalten werden. Dieser Punkt wird aus Unwissenheit oder Budgetmangel oft vernachlässigt, wodurch die Robustheit und Zuverlässigkeit eines Systems nicht garantiert werden kann.

- *Governance: Qualitätssicherung / Validierung und Verifikation*

Das sogenannte Testing ist ein Vorgehen im Qualitätsmanagement von Software und wird über die ISO/IEC 25000 bis ISO/IEC 25064 definiert. Die meisten der oben aufgezeigten Problemstellungen fallen fachlich in den Bereich der Qualitätssicherung bzw. des Softwaretestings. Aufgrund der Komplexität moderner KI-Systeme ist eine Software nie fehlerfrei, da die Komplexität ins Unendliche steigen kann. Es kann lediglich die Fehlerzahl reduziert werden.[64] Gerade bei KI-Systemen ist deshalb das Testen umso wichtiger, damit fatales Fehlverhalten verhindert oder zumindest auf ein Minimum reduziert wird. Als Schätzwert sollte die Entwicklungszeit die gleichen Ressourcen wie das Testen bekommen. Bei der Einhaltung der entsprechenden ISO-Norm ist die Qualitätssicherung in der Regel gewährleistet. Auch das Vorgehen der Entwickler:innen kann gute Hinweise auf ein ausreichendes Testen geben. Wird eine Software im sogenannten „Pair Programming“ entwickelt, gibt es eine definierte Vorgehensweise nach dem „Vier Augen Prinzip“ (ISBN 978-0-321-27865-4, Kap. 10, S. 58). Bei Hochrisikoanwendungen wird oft auch das „Triple Programming (Extreme Programming - XP)” verwendet, wobei das Testen in die tägliche Software-Entwicklung integriert ist.

[63] Safety und Security by Design beschreibt die Betrachtung aller Sicherheitsaspekte entlang des Produktlebenszyklus von technischen Systemen – und zwar vom Beginn der Entwicklung an, nicht erst im Test oder im laufenden Betrieb.

[64] Pol, Koomen, Spillner (2020): Management und Optimierung des Testprozesses: Praktischer Leitfaden für erfolgreiches Software-Testen mit TPI und TMap, (1) erläutern Testen wie folgt:
„Tests sind nicht die einzige Maßnahme im Qualitätsmanagement der Softwareentwicklung, aber oft die letztmögliche. Je später Fehler entdeckt werden, desto aufwändiger ist die Behebung, woraus sich der Umkehrschluss ableitet: Qualität muss (im ganzen Projektverlauf) implementiert und kann nicht 'eingetestet' werden.“
„Beim Testen in der Softwareentwicklung wird i. d. R. eine mehr oder minder große Fehleranzahl als 'normal' unterstellt oder akzeptiert. Hier herrscht ein erheblicher Unterschied zur Industrie: Dort werden im Prozessabschnitt 'Qualitätskontrolle' oft nur noch in Extremsituationen Fehler erwartet.“

Zusammenfassend lässt sich festhalten, dass einige der Herausforderungen, die der Einsatz von KI-Systemen im Mittelstand mit sich bringt, perspektivisch durch technische Methoden und Ansätze lösbar sind. Dennoch bleiben Fragen offen. Insbesondere die Fehlertoleranz hinsichtlich eines Systems stellt ein relevantes Thema und eine zum Teil auch gesellschaftlich zu klärende Frage dar. Darüber hinaus besteht ein unter Innovationsgesichtspunkten vielfach diskutiertes Spannungsfeld zwischen der Gewährleistung eines, im Sinne der RAI, sicheren KI-Systems einerseits, und der Anforderung an die Offenlegung der Quellcodes andererseits. Bislang gibt es keine universell geltenden und hinreichend funktionierenden Methoden, die KI-Systeme gleichzeitig in ihrer Funktion sicher gestalten und externe Angriffe umfassend bekämpfen. Ratsam ist es demnach, wie oben beschrieben, verschiedene Ansätze zu kombinieren und insbesondere die Lücken, die durch den rechtlichen Rahmen (KI-Act) offenbleiben, mithilfe der Kriterien der RAI und darauf aufbauender möglicher technischer Lösungsansätze zu schließen.

6. Handlungsempfehlungen

In Hamburg gibt es bereits zahlreiche KI-Nutzer:innen und -Entwickler:innen, die die Technik in verschiedensten Branchen anwenden und entwickeln. Mit einer außerordentlich hohen Dichte an Hochschulen und einer ausgeprägten KI-Forschungsgeschichte bietet die Stadt gute und wichtige Voraussetzungen, um sich als KI-Standort weiter zu etablieren. Durch die Unterstützung verschiedener Netzwerkakteure kann darüber hinaus der Austausch untereinander weiter gefördert werden und sich die Stadt international als Standort für KI-Entwicklung und -Anwendung empfehlen. Um sich darüber hinaus auch als Standort für einen verantwortlichen Einsatz von KI zu etablieren, bedarf es nicht nur einer weitreichenderen Forschung, die die Schnittstelle zwischen Technik, Recht und Ethik in den Blick nimmt, sondern auch konkreter institutioneller Vorkehrungen, die die Branche in Hamburg noch gezielter unterstützt. Eine derartige Förderung kann nicht nur Impulse im Rahmen einer zukunftsorientierten Wirtschaftspolitik setzen, sondern auch zur Sicherung des Wirtschaftsstandorts Hamburg beitragen und Arbeitsplätze langfristig sichern. Um diese Zukunftsfestigkeit zu gewährleisten, sollten nach den Ergebnissen der vorliegenden Studie immer auch die rechtlichen Herausforderungen durch den KI-Act und die Anforderungen des Konzepts einer RAI berücksichtigt werden. So kann ein bestmögliches Umfeld für die Entwicklung und den Einsatz einer verantwortlichen KI im oben dargestellten Sinn geschaffen werden.

Die Mitgliedsstaaten der EU sind nach KI-Act wie dargestellt angehalten, KMU bestmöglich mit Beratungs- und Sensibilisierungsmaßnahmen sowie Reallaboren zu unterstützen. Die Bedingungen in Hamburg sind nach unserer Analyse hierfür gut. Hamburg könnte für Norddeutschland einen entscheidenden Platz in der Innovations- aber auch Aufsichtsstruktur einnehmen und bereits vorhandene Standortvorteile nutzen sowie ausbauen:

- Mit dem Mittelstand-Digital-Zentrum, das in enger Kooperation mit der Handelskammer Hamburg arbeitet, gibt es für KI-interessierte KMU eine wichtige Anlaufstelle in der Stadt, die mit Hilfe von KI-Trainer:innen Unterstützung bei konkreten Anwendungsfragen anbietet.
- Mit dem Artificial Intelligence Center ARIC hat Hamburg einen überregional beachteten Akteur, der sich insbesondere auch auf dem Feld des verantwortungsvollen Einsatzes von KI engagiert und ein breit gefächertes Angebot an Vernetzungs- und Beratungsleistungen vorhält.

- Mit CertifAI siedelt sich derzeit in Hamburg eine Prüf- und Zertifizierungsstelle für KI an, die KI-Systeme auf die Einhaltung regulatorischer Vorgaben testen wird.
- Mit verschiedenen Reallaboren, z.B. in den Bereichen Mobilität oder Energie, hat Hamburg bereits Erfahrung in der Erprobung verschiedener technischer Lösungen, die zukünftig systematisch um die Komponente KI ergänzt werden könnten.[65]

An diese Angebote, die neben weiteren Akteuren und Institutionen das KI-Ökosystem der Stadt prägen, lässt sich anknüpfen. Es bietet sich an, derartige Strukturen auszubauen und auf eine belastbare institutionelle Basis zu stellen, also vor Ort eine nach KI-Act notwendige Infrastruktur vorzuhalten, um insbesondere Start-ups von komplexen Prozessen rund um Genehmigungsverfahren zu entlasten und darüber hinaus das Konzept einer RAI zu fördern und den Standort auch für zukünftige Investor:innen attraktiv zu machen.

Um allerdings dennoch existierende Investitionshemmnisse abzubauen, mögliches fehlendes Wissen über rechtliche Anforderungen auszugleichen und die Sorge vor einem „Zuviel an Bürokratisierung" zu nehmen, schlagen wir auf Grundlage der obigen Analyse und im Abgleich mit den sich verändernden rechtlichen Rahmenbedingungen folgende Handlungsempfehlungen vor:

Unsere Empfehlung: Das KI-Ökosystem dort stärken, wo bereits anschlussfähige Strukturen bestehen.

Konkret heißt das, dass Services zentral gepoolt werden und die aufzubauenden Strukturen mit dem Fokus auf die Förderung von Zielgruppen im Bereich der KMU sowie der Start-ups folgende Leistungen umfassen sollten:

A. <u>Kompetenzaufbau & Experimentierräume zur Standortsicherung:</u>

a. **Stärkung eines zentral gesteuerten Beratungsangebots** mit Ansprechpartner:innen, die Entwicklungs- und Innovationsprozesse von Beginn an begleiten

i. Zielgruppen können sowohl KMU, Reallabore als auch Vertreter:innen der Stadt sein

ii. Absicherung durch eine institutionelle und langfristige Förderung, ergänzt durch Projektmittel und potentiell eigene Einnahmen

iii. Beratungsangebot mit interdisziplinärem Team unter Einbeziehung juristischer Expertise

b. **Aus- und Aufbau weiterer Experimentierräume und Reallabore** unter Berücksichtigung KI-relevanter Infrastruktur, inkl. ausreichender Rechenkapazitäten

[65] Im RealLabHH z.B. wurden Mobilitätskonzepte für die Stadt Hamburg erprobt und darauf aufbauend ein Leitfaden erstellt. Das Projekt des RealLabHH geht auf die Initiative der Nationalen Plattform Zukunft der Mobilität (NPM) zurück, lief bis Ende 2021 und wurde vom BMDV mit insgesamt 19,2 Millionen Euro gefördert.

sowie unter Integration nicht nur technischer, sondern auch juristischer Expertise

c. **Finanzierung einer Schnittstellenfunktion** in den behördlichen Strukturen der Stadt für langfristiges Monitoring politischer und rechtlicher Prozesse und zur Gewährleistung des Austauschs zwischen Stadt und den Akteuren vor Ort

d. **Ausbau von Train-the-Trainer Modellen:** Schulungsangebote für Multiplikator:innen (z.B. Kammern, Verbände) die Ansprechpartner:innen von KMU sind, so dass Investitionsentscheidungen besser vorbereitet und getroffen werden können

e. **Entwicklung neuer Förderfonds** für einzelne Zielgruppen, insbesondere KMU & Start-ups

B. Wissenstransfer, auch mit niedrigschwelligen Angeboten

a. **Checkliste** als erstes Prüfmodul für juristische Fragen

b. **Aufbau einer Online-Plattform** mit integrierter digitaler Checkliste und darüber hinausgehenden Angeboten, wie z.B. weiteren „Checklisten" zu Prozessen und Normen des Software-Engineerings, Fragestellungen zu Zertifizierungsstellen und -modalitäten, verschiedenen Ansprechpartner:innen, etc.

c. **Ausbau von Fortbildungen & Workshops** für Mitarbeitende und die Leitungsebene von KMU zu rechtlichen Fragestellungen und Umsetzungsmöglichkeiten

d. **Systematischer Austausch** mit Wissenschaft und Forschung sowie angrenzenden Beratungsinstituten unter besonderer Berücksichtigung rechtlicher Fragen

Anhang 1 Entwurf der Checkliste nach KI-Act

Der Checkliste liegt der Entwurf des KI-Acts vom 21.4.2021 zu Grunde. Es ist davon auszugehen, dass es im weiteren Normgebungsverfahren zu Änderungen kommen wird, sodass die Checklist entsprechend anzupassen wäre.

1. Ist es KI gemäß KI-Act-Definition?

[Art. 3 Abs. 1 & Anhang I]

Zutreffendes bitte ankreuzen:

	1. **Handelt es sich um eine Software, die mit einer oder mehreren der folgenden Techniken und Konzepten entwickelt worden ist? Zutreffendes bitte ankreuzen:**	
	A. Handelt es sich um maschinelles Lernen • mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen • unter Verwendung einer breiten Palette von Methoden, einschließlich des tiefen Lernens (Deep Learning)?	
	B. Handelt es sich um Logik- und wissensgestützte Konzepte, einschließlich • Wissensrepräsentation, • induktiver (logischer) Programmierung, • Wissensgrundlagen, • Inferenz- und Deduktionsmaschinen, • (symbolischer) Schlussfolgerungs- und Expertensysteme?	
	C. Handelt es sich um • statistische Ansätze, • Bayessche Schätz-, Such- und Optimierungsmethoden?	
	2. Kann die Software im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse (z.B. Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen) hervorbringen, die das Umfeld beeinflussen, mit dem sie interagieren?	

Wurde bei 1. & 2. ein Kreuz gesetzt, handelt es sich um KI im Sinne des KI-Act und Sie müssen die darin festgehaltenen Anforderungen erfüllen. Weiter zu Punkt 2. der Checkliste.
Wurde in keinem oder nur einem der Felder ein Kreuz gesetzt, fällt ihr System nicht unter die KI-Definition des KI-Act und Sie können die Checkliste beenden.

2. Welche Risikokategorie?

Der KI-Act verfolgt einen risikobasierten Ansatz, bei dem Anwendungen, die einen höheren potentiellen Schaden oder Nachteil für Menschen nach sich ziehen können, höheren rechtlichen Anforderungen unterliegen. Es wird zwischen den folgenden vier Risikokategorien unterschieden:

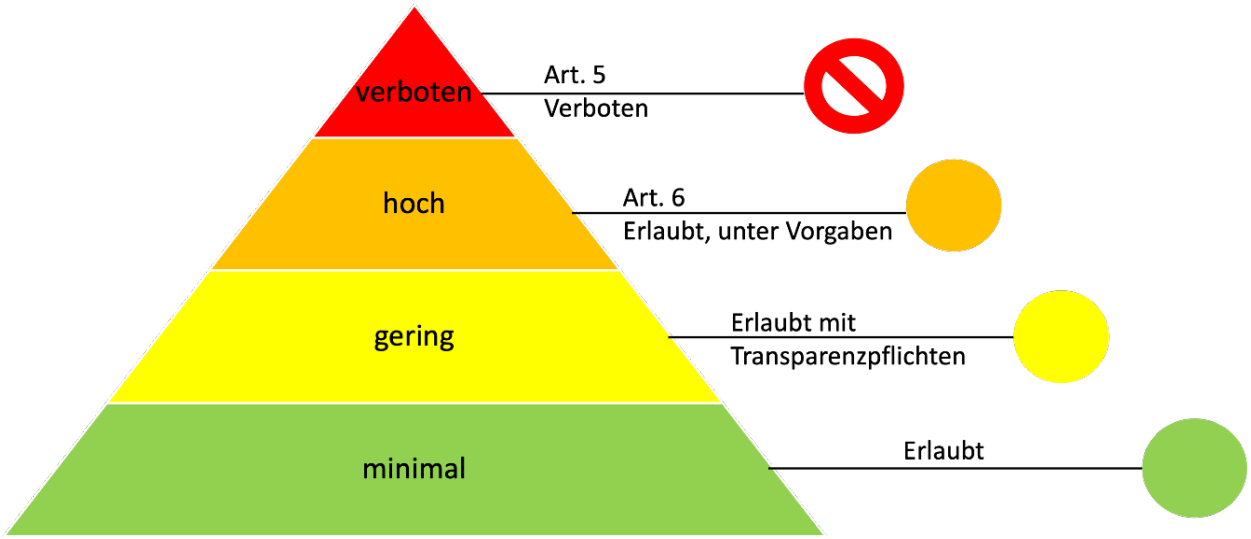


Abb.1.: Eigene Darstellung: Der risikobasierte Ansatz nach KI-Act

<u>Verbotene KI-Systeme</u> (Art. 5 KI-Act)

KI-Systeme, die zu folgenden Zwecken eingesetzt werden können, sind verboten:

Die unterschwellige Beeinflussung von Personen zu deren (potentiellen) Schaden Beeinflusst das Produkt unterschwellig das Verhalten einer Person, außerhalb deren Bewusstseins in einer Weise so wesentlich, dass es dieser oder eine andere Person physischen oder psychischen Schaden zufügt oder zufügen könnte?	
Das Ausnutzen der Schutzbedürftigkeit bestimmter Personengruppen Beeinflusst das Produkt das Verhalten einer Person, die einer schutzbedürftigen Personengruppe angehört in einer Weise, die die Schwäche oder Schutzbedürftigkeit (bspw. bei körperlicher oder geistiger Behinderung) ausnutzt und dieser oder einer anderen Person psychischen oder physischen Schaden zufügt oder zufügen könnte?	
Behördliche Bewertung oder Klassifizierung natürlicher Personen Handelt es sich um ein Produkt, welches zur behördlichen Bewertung oder Klassifizierung von der Vertrauenswürdigkeit natürlicher Personen, aufgrund von Verhaltensweisen oder Persönlichkeitsmerkmalen? Resultiert daraus eine Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder ganzer Personengruppen in sozialen Zusammenhängen, die sich von den Umständen unterscheiden, unter denen die Daten ursprünglich erzeugt oder erfasst wurden?	

Resultiert daraus eine ungerechtfertigte oder unverhältnismäßige Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder ganzer Personengruppen in Bezug auf deren soziales Verhalten?	
Strafverfolgung in öffentlichen Räumen mit biometrischen Echtzeit-Identifizierungssystemen Handelt es sich bei dem Produkt um ein biometrisches Echtzeit-Fernidentifizierungssystem, welches in öffentlichen Räumen zu Strafverfolgungszwecken, ausgenommen der folgend aufgelisteten, eingesetzt wird? Mit Ausnahme von folgenden Zwecken: • Gezielte Suche nach bestimmten potenziellen Opfern von Straftaten oder nach vermissten Kindern • Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder eines Terroranschlags • Erkennen, Aufspüren, Identifizieren oder Verfolgen eines Täters oder Verdächtigen einer Straftat im Sinne des Art. 2 Abs. 2 des Rahmenbeschlusses 2002/584/JI des Rates, der in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht ist.	
Biometrische Echtzeit-Fernidentifizierungssysteme Für die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme gelten besondere Ausnahmen. Diese werden an dieser Stelle nicht aufgeführt und können nachgelesen werden (Titel II, Art. 5 Abs. 1 d), Abs. 2 KI-Act)	

Wurde bei einem dieser Felder ein Kreuz gesetzt, handelt es sich um ein verbotenes KI-System. Das Inverkehrbringen, die Inbetriebnahme oder die Verwendung ist verboten (Titel II, Art. 5. KI-Act) Die Checkliste ist an dieser Stelle zu beenden.
Wurde kein Kreuz gesetzt, gilt es zu prüfen, welche der übrigen Risikokategorien zutreffen.

<u>Hochrisiko-Anwendungen</u>

Handelt es sich bei dem KI-System um eine Hochrisiko-Anwendung gemäß KI-Act (Anhang III, gemäß Art. 6 Abs. 2?

Im Wesentlichen gilt es zu prüfen, ob ein KI-System in die Hochrisikokategorie fällt oder nicht. Denn tut sie das nicht, ist sie entweder verboten oder die Anforderungen sind sehr gering. Zur Abschätzung des Aufwandes ist also die entscheidende Trennlinie Hochrisiko oder nicht (Anhang III, gemäß Art. 6 Abs. 2 KI-Act)

Zutreffendes bitte ankreuzen:

Biometrische Identifizierung und Kategorisierung natürlicher Personen Soll das KI-System bestimmungsgemäß für die biometrische Echtzeit-Fernidentifizierung und nachträgliche biometrische Fernidentifizierung natürlicher Personen verwendet werden?	
Verwaltung und Betrieb kritischer Infrastrukturen	

Soll das KI-System bestimmungsgemäß als Sicherheitskomponente in der Verwaltung und im Betrieb des Straßenverkehrs sowie in der Wasser-, Gas-, Wärme- und Stromversorgung verwendet werden? *[Def. Sicherheitskomponente in TITEL I, Art. 3, 14 KI-Act]*	
Allgemeine und berufliche Bildung Soll das KI-System bestimmungsgemäß für Entscheidungen über den Zugang oder die Zuweisung natürlicher Personen zu Einrichtungen der allgemeinen und beruflichen Bildung verwendet werden?	
Soll das KI-System bestimmungsgemäß für die Bewertung von Schülern in Einrichtungen der allgemeinen und beruflichen Bildung und für die Bewertung der Teilnehmer an üblicherweise für die Zulassung zu Bildungseinrichtungen erforderlichen Tests verwendet werden?	
Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit: Soll das KI-System bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden (insbesondere für die Bekanntmachung freier Stellen, das Sichten oder Filtern von Bewerbungen und das Bewerten von Bewerbern in Vorstellungsgesprächen oder Tests)?	
Soll das KI-System bestimmungsgemäß für Entscheidungen über Beförderungen und über Kündigungen von Arbeitsvertragsverhältnissen, für die Aufgabenzuweisung sowie für die Überwachung und Bewertung der Leistung und des Verhaltens von Personen in solchen Beschäftigungsverhältnissen verwendet werden?	
Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen: Soll das KI-System bestimmungsgemäß von Behörden oder im Namen von Behörden verwendet werden, um zu beurteilen, ob natürliche Personen Anspruch auf öffentliche Unterstützungsleistungen und -dienste haben und ob solche Leistungen und Dienste zu gewähren, einzuschränken, zu widerrufen oder zurückzufordern sind?	
Soll das KI-System bestimmungsgemäß für die Kreditwürdigkeitsprüfung und Kreditpunktebewertung natürlicher Personen verwendet werden (Ausnahme: KI-Systeme, die von Kleinanbietern für den Eigengebrauch in Betrieb genommen werden)?	
Soll das KI-Systeme bestimmungsgemäß für die Entsendung oder Priorisierung des Einsatzes von Not- und Rettungsdiensten, einschließlich Feuerwehr und medizinischer Nothilfe, verwendet werden?	
Strafverfolgung: Soll das KI-System bestimmungsgemäß von Strafverfolgungsbehörden für individuelle Risikobewertungen natürlicher Personen verwendet werden, um das Risiko abzuschätzen, dass eine natürliche Person Straftaten begeht oder erneut begeht oder dass eine Person zum Opfer möglicher Straftaten wird?	
Soll das KI-System bestimmungsgemäß von Strafverfolgungsbehörden als Lügendetektoren und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustands einer natürlichen Person verwendet werden?	
Soll das KI-Systeme bestimmungsgemäß von Strafverfolgungsbehörden zur Aufdeckung von Deepfakes gemäß Art. 52 Abs. 3 KI-Act verwendet werden?	
Soll das KI-Systeme bestimmungsgemäß von Strafverfolgungsbehörden zur Bewertung der Verlässlichkeit von Beweismitteln im Zuge der Ermittlung oder Verfolgung von Straftaten verwendet werden?	
Soll das KI-Systeme bestimmungsgemäß von Strafverfolgungsbehörden zur Vorhersage des Auftretens oder erneuten Auftretens einer tatsächlichen oder potenziellen Straftat auf der	

Grundlage des Profils natürlicher Personen gemäß Art. 3 Abs. 4 der Richtlinie (EU) 2016/680 oder zur Bewertung von Persönlichkeitsmerkmalen und Eigenschaften oder vergangenen kriminellen Verhaltens natürlicher Personen oder von Gruppen verwendet werden?	
Soll das KI-Systeme bestimmungsgemäß von Strafverfolgungsbehörden zur Erstellung von Profilen natürlicher Personen gemäß Art. 3 Absatz 4 der Richtlinie (EU) 2016/680 im Zuge der Aufdeckung, Ermittlung oder Verfolgung von Straftaten verwendet werden?	
Soll das KI-Systeme bestimmungsgemäß zur Kriminalanalyse natürlicher Personen eingesetzt werden und es den Strafverfolgungsbehörden ermöglichen, große komplexe verknüpfte und nicht verknüpfte Datensätze aus verschiedenen Datenquellen oder in verschiedenen Datenformaten zu durchsuchen, um unbekannte Muster zu erkennen oder verdeckte Beziehungen in den Daten aufzudecken?	
Migration, Asyl und Grenzkontrolle: Soll das KI-System bestimmungsgemäß von zuständigen Behörden als Lügendetektoren und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustands einer natürlichen Person verwendet werden?	
Soll das KI-System bestimmungsgemäß von zuständigen Behörden zur Bewertung eines Risikos verwendet werden (einschließlich eines Sicherheitsrisikos, eines Risikos der irregulären Einwanderung oder eines Gesundheitsrisikos, das von einer natürlichen Person ausgeht, die in das Hoheitsgebiet eines Mitgliedstaats einzureisen beabsichtigt oder eingereist ist)?	
Soll das KI-System bestimmungsgemäß von zuständigen Behörden zur Überprüfung der Echtheit von Reisedokumenten und Nachweisunterlagen natürlicher Personen und zur Erkennung unechter Dokumente durch Prüfung ihrer Sicherheitsmerkmale verwendet werden?	
Soll das KI-Systeme bestimmungsgemäß zuständige Behörden bei der Prüfung von Asyl- und Visumanträgen sowie Aufenthaltstiteln und damit verbundenen Beschwerden im Hinblick auf die Feststellung der Berechtigung der den Antrag stellenden natürlichen Personen unterstützen?	
Rechtspflege und demokratische Prozesse: Soll das KI-System bestimmungsgemäß Justizbehörden bei der Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften und bei der Anwendung des Rechts auf konkrete Sachverhalte unterstützen?	

Wurde in einem der Felder ein Kreuz gesetzt, kann weiter zu Punkt 3. der Checkliste gegangen werden.

Wurde kein Kreuz gesetzt, gilt es zu prüfen, ob das KI-System eine Sicherheitskomponente eines Produkts oder in einem Teil eines Produktes darstellt, oder welche der übrigen Risikokategorien zutreffen.

Handelt es sich bei dem KI-System um eine Sicherheitskomponente in einem Produkt oder um einen Teil eines Produktes, das den Harmonisierungsvorschriften der Union unterliegt (Anhang II)? *[Def. Sicherheitskomponente in TITEL I, Art. 3, 14 KI-Act]*

Maschinen Handelt es sich bei dem Produkt um Maschinen gemäß Richtlinie 2006/42/EG? z.B. **Sensorik Anwendungen** in Mikrocontrollern, Embedded GPUs, Smartphones und Co?	
Spielzeug Handelt es sich bei dem Produkt um Spielzeug gemäß Richtlinie 2009/48/EG?	

Sportboote und Wassermotorräder Handelt es sich bei dem Produkt um Sportboote und Wassermotorräder gemäß Richtlinie 2013/53/EU?	
Aufzüge Handelt es sich bei dem Produkt um Aufzüge gemäß Richtlinie 2014/33/EU?	
Geräte und Schutzsysteme zur bestimmungsgemäßen Verwendung in explosionsgefährdeten Bereichen Handelt es sich bei dem Produkt um Geräte und Schutzsysteme zur bestimmungsgemäßen Verwendung in explosionsgefährdeten Bereichen gemäß Richtlinie 2014/34/EU?	
Funkanlagen Handelt es sich bei dem Produkt um Funkanlagen gemäß Richtlinie 2014/53/EU?	
Druckgeräte Handelt es sich bei dem Produkt um Druckgeräte gemäß Richtlinie 2014/68/EU?	
Personenschutzausrüstung Handelt es sich bei dem Produkt um Personenschutzausrüstung/ persönliche Schutzausrüstung gemäß der Richtlinie 2016/425/EU?	
Medizinprodukte Handelt es sich bei dem Produkt um ein Medizinprodukt gemäß der Richtlinie 2017/745/EU?	
In-vitro-Diagnostika Handelt es sich bei dem Produkt um ein In-vitro-Diagnostika gemäß der Richtlinie 2017/746/EU?	

Handelt es sich bei dem KI-System um eine Sicherheitskomponente in einem Produkt oder selbst um ein Produkt, das folgenden Harmonisierungsvorschriften der Union unterliegt (Titel I, Art. 2 Abs. 2 KI-Act sowie Anhang II B)? *[Def. Sicherheitskomponente in TITEL I, Art. 3, 14 KI-Act]*

Zivilluftfahrt Verordnung (EG) Nr. 300/2008: gemeinsamen Vorschriften für die Sicherheit in der Zivilluftfahrt	
Genehmigung und Marktüberwachung von Fahrzeugen und Kraftfahrzeugen Verordnung (EU) Nr. 168/2013 des Europäischen Parlaments und des Rates vom 15. Januar 2013 über die Genehmigung und Marktüberwachung von zwei- oder dreirädrigen und vierrädrigen Fahrzeugen	
Genehmigung und Marktüberwachung von land- und forstwirtschaftlichen Fahrzeugen Verordnung (EU) Nr. 167/2013 des Europäischen Parlaments und des Rates vom 5. Februar 2013 über die Genehmigung und Marktüberwachung von land- und forstwirtschaftlichen Fahrzeugen	
Schiffsausrüstung Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates vom 23. Juli 2014 über Schiffsausrüstung	
Interoperabilität des europäischen Eisenbahnsystems Richtlinie (EU) 2016/797 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Interoperabilität des Eisenbahnsystems in der Europäischen Union	

Genehmigung und Marktüberwachung von Kraftfahrzeugen, Kraftfahrzeuganhänger und anderen Systemteilen technischer Einheiten Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates vom 30. Mai 2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern	
Zivilluftfahrt und Flugsicherheit Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates vom 4. Juli 2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit	

Wurde in einem der Felder ein Kreuz gesetzt, gilt Titel IV, Art. 84 KI-Act (Titel I, Art. 2 Abs. 2 KI-Act sowie Anhang II B). An dieser Stelle kann die Checkliste beendet werden.

Wurde in der bisherigen Checkliste noch kein Kreuz gesetzt, gilt es zu prüfen, welche der übrigen Risikokategorien zutreffen:

Geringes Risiko

Beabsichtigen Sie die Entwicklung, das Inverkehrbringen oder die Inbetriebnahme eines KI-Systems mit folgenden Eigenschaften: Interaktion mit Menschen Das KI-System ist zur Interaktion mit natürlichen Personen bestimmt Handelt es sich um ein KI-System, welches für die Interaktion mit natürlichen Personen bestimmt ist?	
Emotionserkennung und biometrische Kategorisierung Das KI-System wird zur Erkennung von Emotionen oder zur Assoziierung von (gesellschaftlicher) Kategorien anhand biometrischer Daten eingesetzt	
Deepfakes Das KI-System erzeugt oder manipuliert Bild-, Ton- oder Videoinhalte, die wirklichen Personen, Gegenständen, Orten oder anderen Einrichtungen oder Ereignissen merklich ähneln und einer Person fälschlicherweise als echt oder wahrhaftig erscheint ("Deepfake")?	

Wurde in dieser Checkliste ein Kreuz gesetzt, gilt die Pflicht zur Offenlegung der Tatsache (Titel IV, Art. 52 KI-Act). Die KI-Systeme müssen so konzipiert und entwickelt werden, dass natürlichen Personen mitgeteilt wird, dass es sich um ein KI-System handelt.

Wenn bis hierhin kein Kreuz gesetzt wurde, fällt man nach dem Ausschlussverfahren in die minimale Risikokategorie und muss keine der Anforderungen nach dem KI-Act erfüllen (kann aber freiwillig).
Die Checkliste kann an dieser Stelle beendet werden.

3. Welche Rolle?

Rechte und Pflichten in Bezug auf Hochrisiko-KI-Systeme unterscheiden sich nach Rollen [Titel III, Kapitel 3 KI-Act]. Ein Akteur kann je nach Tätigkeit mehrere Rollen einnehmen, bzw. die Rollen können bei Änderung der Tätigkeiten wechseln.

Zutreffendes ankreuzen:

Anbieter [Titel III, Kapitel 3, Art. 16-23 KI-Act] Unter Anbieter fallen folgende Akteure: Natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, die ein KI System entwickeln oder entwickeln lassen, um es unter ihrem eigenen Namen oder ihrer eigenen Marke – entgeltlich oder unentgeltlich – in Verkehr zu bringen. Natürliche oder juristische Personen, Behörden oder sonstige Stellen, die wesentliche Änderungen an einem KI System vorgenommen haben. Natürliche oder juristische Personen, Behörden oder sonstige Stellen, die die Zweckbestimmung eines bereits im Verkehr befindlichen KI Systems verändert haben oder verändern werden.	
Produkthersteller [Art. 24 KI-Act] Zu Produktherstellern zählen natürliche oder juristische Personen, die Produkte herstellen oder entwickeln und herstellen lassen und diese unter ihrem eigenen Namen oder ihrer eigenen (Handels-)Marke vermarkten oder für ihre eigenen Zwecke verwenden. Darunter fallen Produkte folgender Rechtsakte: • Maschine (Richtlinie 2006/42/EG) • Spielzeug (Richtlinie 2009/48/EG) • Sportboote & Wassermotorräder (Richtlinie 2013/53/EU) • Aufzüge (Richtlinie 2014/33/EU) • Geräte und Schutzsysteme zur bestimmungsgemäßen Verwendung in explosionsgefährdeten Bereichen (Richtlinie 2014/34/EU) • Funkanlagen (Richtlinie 2014/53/EU) • Druckgeräte (Richtlinie 2014/68/EU) • Seilbahnen (Verordnung (EU) 2016/424) • persönliche Schutzausrüstungen (Verordnung (EU) 2016/425) • Geräte zur Verbrennung gasförmiger Brennstoffe (Verordnung (EU) 2016/426) • Medizinprodukt (Verordnung (EU) 2017/745) • In-vitro-Diagnostika (Verordnung (EU) 2017/746)	

Bevollmächtigte [Art. 25 KI-Act] Bin ich eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI Systems schriftlich dazu bevollmächtigt wurde, in seinem Namen die in der KI Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen?	
Einführer [Art. 26, 28 KI-Act] Bin ich eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI System, das den Namen oder die Marke einer außerhalb der Union ansässigen oder niedergelassenen natürlichen oder juristischen Person trägt, in der Union in Verkehr bringt oder in Betrieb nimmt?	
Händler [Art. 27, 28 KI-Act] Bin ich eine natürliche oder juristische Person in der Lieferkette, die ein KI-System ohne Änderungen seiner Merkmale auf dem Unionsmarkt bereitstellt, mit Ausnahme des Herstellers oder des Einführers?	
Nutzer [Art. 28, 29 KI-Act] Bin ich eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI System in eigener Verantwortung oder verwendet, es sei denn, das KI System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet?	
Sonstige Dritte [Art. 28 KI-Act] Bringe ich ein Hochrisiko-KI-System unter meinem Namen oder meiner Marke in Verkehr oder nehme es in Betrieb? Bin ich eine natürliche oder juristische Person, die die Zweckbestimmung eines sich bereits im Verkehr befindenden oder in Betrieb genommenen Hochrisiko-KI-Systems verändert? Bin ich eine natürliche oder juristische Person, die eine wesentliche Änderung an einem Hochrisiko-KI-System vornimmt?	
Kleinanbieter Bin ich eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, bei der es sich um ein Kleinst- oder Kleinunternehmen im Sinne der Empfehlung 2003/361/EG und ein KI-System entwickelt oder entwickeln lässt, um es unter meinem Namen oder den meiner Marke in Verkehr zu bringen oder in Betrieb zu nehmen?	

Wenn Sie ein oder mehrere Kreuze gesetzt haben, gehen Sie weiter zu 4.

Wenn Sie bei „Sonstige Dritte“ ein Kreuz gesetzt haben, zählen Sie als neuer Anbieter des Produkts und unterliegen den Anbieterpflichten gemäß Art. 16 KI-Act.

4.Was muss ich tun? (Output)

An dieser Stelle würden nun die Anforderungen stehen, die sich aus dem Durchlaufen der Checkliste ergeben haben. In analoger Form ist dies zu unübersichtlich, weshalb an dieser Stelle darauf verzichtet wird und in digitaler Form ausgearbeitet werden sollte.

Anhang 2 Prozesse und Normen des Software Engineering

Das *Software Engineering* sollte mindestens folgende *Kernprozesse* und *Vorgehensmodelle* befolgen:

(Die angegeben Normen sind als Hinweis zu verstehen, da diese sich schnell ändern oder es äquivalente Normen anderer Organisationen gibt)

1. Planung

- Anforderungserhebung (definiert durch IEEE)
- Lastenheft (Anforderungsdefinition) (IEEE 830-1998)
- Pflichtenheft (Mit technischen Ansätzen verfeinertes Lastenheft VDI-Richtlinie 3694)
- Aufwandsschätzung (z. B. mittels Function-Point-Verfahren oder COCOMO)
- Vorgehensmodell (ISO/IEC 12207)

2. Analyse

- Mock-up
- Prozessanalyse / Prozessmodell (ISO/IEC 12207)
- Systemanalyse
- Strukturierte Analyse (SA)

3. Entwurf

- Softwarearchitektur (IEEE 1471:2000 oder International Software Architect Qualification
- Board (iSAQB))
- Strukturiertes Design (SD)
- Fundamental Modeling Concepts (FMC)

4. Programmierung

- Normierte Programmierung (DIN 66260) oder
- Objektorientierte Programmierung (OOP IEEE 830)

5. Validierung und Verifikation (ISO/IEC 250xx)

- Modultests (Low-Level-Test)
- Integrationstests (Low-Level-Test)
- Systemtests (High-Level-Test)
- Akzeptanztests (High-Level-Test)

6. Anforderungsmanagement

- Minimum: ISO/IEC 15504 (SPICE)

7. Projektmanagement (ISO 21500:2012; deutsche Norm als DIN ISO 21500:2016-02)

- Risikomanagement
- Projektplanung
- Projektverfolgung und -steuerung

8. Qualitätsmanagement (IATF 16949:2016 oder ISO 9001:2015)

- SPICE (Software Process Improvement and Capability Determination ISO/IEC 15504-5
- Incident Management (ITIL 4)
- Problem-Management (ISO/IEC 15504)
- Softwaremetrik (Messung von Softwareeigenschaften, min. Restfehler, MTBF, Tests)

- Statische Analyse (Berechnung von Schwachstellen)
- Software-Ergonomie (Arbeitsstättenverordnung (ArbStättV) sowie in der Norm EN ISO 9241)

9. Konfigurationsmanagement (ISO/IEC 24765, ISO 10007, NIST, ITIL)

- Versionsverwaltung
- Änderungsmanagement / Veränderungsmanagement
- Releasemanagement
- Application-Management (ITIL)

10. Softwareeinführung

- Iterative Einführung

11. Dokumentation

- Technische Dokumentation (VDI 4500)
- Softwaredokumentation (veraltet, gute Leitlinie: DIN 66230, DIN 66231, DIN 66232)
- Ggf. Systemdokumentation (Weiterentwicklung und Fehlerbehebung)
- Betriebsdokumentation (Betreiber/Service, gesetzlich vorgeschrieben, je nach Geschäftszweig)
- Bedienungsanleitung (Anwender EN 82079-1)
- Verfahrensdokumentation (Beschreibung rechtlich relevanter Softwareprozesse EN 82079, GoBD, HGB, AO)

Anhang 3 Glossar

Begriff	Erklärung
KI	Unter KI versteht man im Allgemeinen einen Teilbereich der Informatik, wobei Softwareprogramme in der Lage sind, bestimmte Aufgaben zu erledigen, für die es ansonsten menschliches intelligentes Handeln braucht. Zur KI werden sowohl Verfahren des maschinellen Lernens als auch eine Reihe wissensbasierter Verfahren ("Expertensysteme") verstanden. Definition im KI-Act im Endeffekt richtungsgebend
Maschinelles Lernen	Teilbereich von KI, bei dem das intelligente Verhalten nicht etwa vom Menschen einprogrammiert wird, sondern über viele Beispieldaten erlernt wird. Bsp. Bilderkennung
Algorithmen	Algorithmus ist ein allgemeinerer, nicht IT-spezifischer Begriff, unter dem eine Verarbeitungsvorschrift (Abfolge von Anweisungen) verstanden wird. So sind beispielsweise auch Kochrezepte oder Notenblätter Algorithmen, da sie dazu anleiten, einzelne Zutaten oder Noten so zu verarbeiten und zu kombinieren, dass danach das gewünschte Gericht oder Musikstück erstellt werden kann. In der Informatik stellen Algorithmen eine Verarbeitungsvorschrift für Maschinen dar, die anhand dieser aus Eingaben die gewünschten Ausgaben berechnen. Ein Algorithmus folgt logischen und mathematischen Gesetzen.
Deepfake	Anwendungen von KI, bei denen Medieninhalte (v.a. Audio & Video) manipuliert oder künstlich erstellt werden.
Black Box	KI-Verfahren, die mathematisch nicht beweisbar sind. In diesen Verfahren kann keine vollständige Transparenz und Erklärbarkeit der Entscheidungsfindung des Systems gewährleistet werden. Darunter fallen bspw. künstliche neuronale Netze.
White Box	KI-Verfahren, die mathematisch beweisbar sind. In diesen Verfahren kann eine Transparenz und Erklärbarkeit gewährleistet werden. Dazu zählen bspw. Entscheidungsbäume.
Bias	Eine systematische Verzerrung, die die Entscheidungsfindung beeinflusst. Im Zusammenhang mit KI-Anwendungen häufig aufgrund unausgeglichener Trainingsdatensätze, wodurch die Entscheidungsfindung in eine bestimmte Richtung verzerrt wird. Beispielsweise die Benachteiligung bestimmter Personengruppen, die aus soziokulturellen Gründen bereits unfaire Diskriminierung erfahren, wie bspw. Frauen oder Personen ethnischer Minderheiten.
Reinforcement Learning	Lernmethode, bei der gewünschtes Verhalten über häufiges Wiederholen mit Feedback (Belohnung und Bestrafung) antrainiert wird