



Die
Bundesregierung

Stellungnahme der Bundesregierung der Bundesrepublik Deutschland
zum Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz
und Vertrauen COM (2020) 65 final

Einleitung

Die Bundesregierung bedankt sich bei der Europäischen Kommission für die Vorlage des Weißbuchs zur Künstlichen Intelligenz sowie den Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung und die Möglichkeit hierzu Stellung zu nehmen.

Das Weißbuch umfasst wesentliche Stellgrößen, um die Potenziale Künstlicher Intelligenz (KI) zu erschließen und etwaigen Risiken zu begegnen. Die Bundesregierung verfolgt mit der nationalen KI-Strategie das Ziel, Deutschland und Europa zu einem führenden KI-Standort zu machen und so zur Sicherung der künftigen Wettbewerbsfähigkeit beizutragen. Die Bundesregierung teilt dabei die Zielvorstellung der Europäischen Kommission eines auf europäischen Werten und Regeln basierenden KI-Ökosystems, das der gesamten europäischen Gesellschaft und Wirtschaft die Vorteile dieser Technologie erschließt.

Schon heute sind KI-Systeme in Industrie und Dienstleistung, im dortigen Arbeitsalltag sowie im B2B-Bereich und in der Forschung gebräuchlich. Sie spielen eine zunehmende Rolle für den staatlichen Einsatz. Sie berühren das Leben vieler Menschen, beispielsweise bei virtuellen Assistenten, dem Einsatz von Spamfiltern, der Personalauswahl, dem Kredit scoring oder in der medizinischen Diagnostik. Während mit diesen stetig wachsenden Einsatzmöglichkeiten ein großer wirtschaftlicher, gesellschaftlicher und individueller Nutzen einhergehen kann, können mit ihnen Risiken verbunden sein. Ziel der Bundesregierung ist es, eine verantwortungsvolle, gemeinwohlorientierte und menschenzentrierte Entwicklung und Nutzung von KI sowie die Förderung von Wettbewerbsfähigkeit und Innovation in der Europäischen Union voranzubringen.

Für die Bundesregierung bedeutet das Ökosystem für Exzellenz einen Gleichklang aus innovativer Forschung, wettbewerbsfähigen Unternehmen, moderner Verwaltung und digital

kompetenten Menschen. Wir teilen die Einschätzung der EU-Kommission, dass der Einsatz von KI maßgeblich dazu beitragen wird, die Ziele des europäischen Green Deals zu erreichen, Klimaschutz und Wettbewerbsfähigkeit in noch stärkeren Gleichlauf zu bekommen, für eine effizientere und bürgerfreundlichere öffentliche Verwaltung zu sorgen, die Bewältigung von Pandemien zu unterstützen sowie insgesamt das gesellschaftliche und wirtschaftliche Wohlergehen im Sinne der UN-Nachhaltigkeitsziele zu fördern. Die Bundesregierung setzt sich daher für ein breit aufgestelltes Wertschöpfungsnetzwerk ein, um die Innovationspotenziale von KI-Technologien und die exzellente europäische KI-Expertise für unterschiedliche Akteure aller Größen und Branchen nutzbar zu machen. Die Chancen für die Wirtschaft sind groß, insbesondere wenn auch kleine und mittlere Unternehmen bei der Anwendung besonders unterstützt werden. Zudem bedarf es eines umfassenden Aufbaus von KI-Kompetenz. Durch ein Exzellenzökosystem kann sichergestellt werden, dass die Europäische Union ihre Vorreiterrolle im Bereich der Forschung sowie der sicheren und vertrauenswürdigen Technologiegestaltung weiter stärkt und die Chancen von KI-Systemen in den Dienst aller Menschen gestellt werden. Gerade die aktuelle COVID-19-Pandemie zeigt, dass KI einen wichtigen Beitrag zur Krisenbewältigung leisten kann.

Die Bundesregierung weist darauf hin, dass für die Ausgestaltung des Ökosystems für Exzellenz eine entsprechende Mittelausstattung in den relevanten Programmen des Mehrjährigen Finanzrahmens (insbesondere Digital Europe) unabdingbar ist.

Gleichzeitig brauchen wir eine europäische Ordnungspolitik für KI. Alle Akteure brauchen Planungs- und Rechtssicherheit und müssen KI-Anwendungen vertrauen können. Die menschenzentrierte und nachvollziehbare Entwicklung und Anwendung von KI-Systemen auf der Basis eines geeigneten Rechtsrahmens muss integraler Bestandteil und damit Markenzeichen einer „AI Made in Europe“ sein. Wie die COVID-19-Pandemie gezeigt hat, muss der Rechtsrahmen ausreichend Flexibilität besitzen, um Innovationen auch beschleunigen zu können, wenn es darum geht, große Schäden für die Gemeinschaft abzuwenden.

Das Ökosystem für Vertrauen basiert auf dem geltenden Recht, insbesondere auf den Vorgaben der Datenschutz-Grundverordnung bzw. der Richtlinie über den Datenschutz bei der Strafverfolgung. Allgemein müssen die Sicherheit und Achtung der Bürger- und Verbraucherrechte, insbesondere der Grundrechte (wie Handlungsfreiheit, informationelle Selbstbestimmung, Berufsfreiheit, Gleichbehandlung, effektiver Rechtsschutz) gewährleistet bleiben und zwar auch bei neuartigen Risiken, die auf bestimmte Besonderheiten von KI zurückgehen. Dabei sind die unterschiedlichen grundrechtlichen Anforderungen zu beachten, die zwischen

dem Einsatz von KI-Systemen im Bereich der staatlichen Eingriffsverwaltung und sonstigen KI-Anwendungsbereichen bestehen.

Um Risiken wirksam zu begegnen, sind konkrete Anforderungen an die Entwicklung und den Einsatz von KI-Systemen zu stellen. Hierzu gehören insbesondere ein risikoadäquates Maß an Transparenz und Nachvollziehbarkeit sowie, falls erforderlich, eine angemessene Kontrollstruktur und Überprüfbarkeit von KI-Anwendungen und ihren Ergebnissen.

Dabei ist die Frage zu beantworten, ob der derzeitige Rechtsrahmen der Produktsicherheit und Produkthaftung bei KI-Systemen, die in Produkte eingebettet sind, ausreicht oder neue Regelungen auch vor dem Hintergrund von Rechtssicherheit geschaffen werden müssen.

Schließlich können Normung und Standardisierung zur Beschleunigung von Entwicklungsprozessen, zur Rechtssicherheit für Unternehmen und zur weiteren Vertrauensbildung der Menschen in die Technologie beitragen.

Teil 1: Ein Ökosystem für Exzellenz

Die Bundesregierung begrüßt die vorgeschlagenen Maßnahmen zur Verwirklichung eines Ökosystems für Exzellenz, um Europas Spitzenposition in der Forschung zu behaupten, Innovationen zu fördern, die Anwendung von KI auszubauen und die Ziele des europäischen Green Deals zu erreichen. Die Maßnahmen sollten mit weiteren relevanten Strategien und Initiativen im Sinne eines Gesamtbildes eng verzahnt werden, etwa mit der Industrie- und KMU-Strategie, sowie der angekündigten Mobilitätsstrategie. Die in Europa vorhandenen Stärken in Forschung, Innovation, Industrie und Dienstleistungen müssen weiter ausgebaut und KI stärker in der Breite der Wirtschaft einschließlich KMU genutzt werden. Gleichzeitig kann KI zu einer CO₂-neutralen, ressourcenschonenden Wirtschaft beitragen.

A. Zusammenarbeit mit den Mitgliedstaaten

Eine enge Zusammenarbeit der Mitgliedstaaten ist unabkömmlich. Die Neufassung des koordinierten Plans ist notwendig und sinnvoll, um ihn an aktuelle Entwicklungen anzupassen und so auf drängende Herausforderungen zu reagieren. Insbesondere die Covid-19-Pandemie hat das gesellschaftliche Leben und die Wirtschaft vor große und neue Herausforderungen gestellt.

Die Anwendung der Künstlichen Intelligenz kann auch die Bewältigung von Pandemien unterstützen. In Bereichen wie der Diagnose- und Therapie-Assistenz, der Telemedizin, beim Schutz bestimmter Bevölkerungsgruppen und beim Finden eines Impfstoffes bietet KI bereits vielversprechende Lösungsansätze. Hierfür bedarf es eines Europäischen Gesundheitsdatenraums, der ein schnelles datenschutzkonformes Teilen, Verwenden und Analysieren von Daten ermöglicht. Dies muss europaweit weiter erforscht und eingesetzt werden.

Nach Auffassung der Bundesregierung sollte als Ziel der Weiterentwicklung des Koordinierten Plans die Schaffung eines verantwortungsvollen, nachhaltigen, gemeinwohlorientierten und menschenzentrierten europäischen KI-Ökosystems als Wertschöpfungsnetzwerk für Innovationen verfolgt werden. Unterschiedliche Akteure aller Größen und aller Branchen sollten dafür über Ländergrenzen hinweg miteinander vernetzt werden. Dazu gehört neben Wissenschaft, Forschung, Wirtschaft, Politik und Verwaltung auch die Zivilgesellschaft, deren Aufklärung und Beteiligung an der Entwicklung und Anwendung von KI wichtig für die Akzeptanz und das Vertrauen ist.

Deutschland hat, gemeinsam mit Frankreich, mit dem Projekt GAIA-X bereits einen operativen Grundstein für eine dezentrale europäische Dateninfrastruktur gelegt und will diesen zukünftig zusammen mit weiteren Mitgliedstaaten weiterentwickeln.

Um die Potenziale der Künstlichen Intelligenz voranzubringen, sind Investitionen essenziell. Dabei sollten Hebeleffekte erzielt werden, etwa durch flankierende Investitionen der Mitgliedstaaten und der Unternehmen. Die entsprechenden Programme der EU-Kommission im neuen mehrjährigen Finanzrahmen, etwa „Digitales Europa“ und „Horizont Europa“, aber auch aus den Europäischen Struktur- und Investitionsfonds müssen daher mit ausreichend finanziellen Mitteln ausgestattet werden.

Die Bundesregierung befürwortet, dass bei der Neufassung des Koordinierten Plans das gesellschaftliche und ökologische Wohlergehen als wichtiger Grundsatz für KI herausgestellt wird. Bei der Entwicklung von KI sollte die Lösung gesellschaftlicher sowie ökologischer Herausforderungen möglichst frühzeitig in den Blick genommen werden (z.B. durch „Sustainability by Design“). KI-Anwendungen können entscheidend zur Erreichung der Ziele für nachhaltige Entwicklung der Agenda 2030 beitragen. Darüber hinaus sollte in allen Mitgliedsstaaten die Barrierefreiheit von KI-Anwendungen gewährleistet sein.

B. Die Arbeit der Forschungs- und Innovationsgemeinschaft fokussieren

Aktivitäten im Bereich der KI-Forschung sollten weiterhin im Rahmen des Koordinierten Plans zwischen den Mitgliedstaaten koordiniert werden. Eine Grundlage für nachhaltigen wirtschaftlichen Erfolg im Bereich KI ist auch die Forschung und Entwicklung als zentraler Bestandteil der Wertschöpfungskette. Grundlegende Fragen in der KI-Forschung beispielsweise zu Nachvollziehbarkeit, Erklärbarkeit, Robustheit und Sicherheit sind noch nicht geklärt und bedürfen weiterer Forschungsanstrengungen, um das gesamte Potenzial der KI besser ausschöpfen zu können.

Die bestehenden europäischen KI-Forschungszentren müssen stärker zusammenarbeiten und mit der Wirtschaft und Behörden kooperieren. Das vorgeschlagene Leitzentrum für Forschung, Innovation und Expertise sollte als Netzwerk dezentral organisiert sein. Es sollte sich sowohl der Grundlagenforschung als auch der anwendungsorientierten Forschung widmen, Nutzer eng einbinden und den Transfer in die Wirtschaft forcieren. Dabei sollte auf bestehenden europäischen KI-Netzwerken aufgebaut und diese in Richtung spezifischer Anwendungssektoren weiterentwickelt werden. Auch die Übertragung von Erkenntnissen zwischen verschiedenen Sektoren, insbesondere mit Blick auf die Schaffung von Vertrauen in übergreifende Standards der KI, könnte eine zentrale Rolle spielen.

Die Bundesregierung unterstützt die Förderung von europäischen Testzentren von Weltrang, die Investitionen bündeln sollen. Wichtig ist, dass die Testzentren von Forschungsprojekten als auch durch Unternehmen, insbes. KMU und ggf. der Verwaltung genutzt werden können. Idealerweise sollten die Testzentren zudem mit Reallaboren (regulatory sandboxes) kombiniert werden. Reallabore können auch auf Deregulierung abzielen, gleichwohl sind dabei Sicherheits- & Schutzstandards zu wahren.

C. Kompetenzen

Die Bundesregierung unterstützt den Ansatz der Kommission, einen möglichst großflächigen Kompetenzaufbau im Bereich KI zu erreichen, um den wissenschaftlichen Nachwuchs in Europa auszubilden, die breite Nutzung von KI in Gesellschaft und Wirtschaft weiter zu stärken und dem Fachkräftemangel entgegenzuwirken. Der Aufbau von Digitalkompetenzen muss vom Kindesalter an bis hin ins Erwachsenenalter gefördert werden. Dafür gilt es, KI-Kompetenz sowohl in der Ausbildung als auch in der Fort- und Weiterbildung umfassend zu vermitteln, insbesondere auch in KMUs. Dies schließt ethische, rechtliche, ökologische und soziale Kompetenzen ein. Beim Kompetenzaufbau ist insbesondere auf Diversität zu achten und darauf, mehr Frauen in diesem Bereich auszubilden und zu beschäftigen.

Der Aufbau von Netzwerken führender Universitäten und Hochschuleinrichtungen sollte im Rahmen des Programms „Digitales Europa“ verfolgt werden. Dabei sollen aufgrund ihrer Nähe und Bedarfsorientierung zu KMU auch Fachhochschulen berücksichtigt werden. Der Kompetenzaufbau sollte durch weitere Maßnahmen zur Unterstützung des wissenschaftlichen Nachwuchses wie Doktorandenprogramme sowie durch Weiterbildungsprogramme für Anwender ergänzt werden.

Dem Wandel, den der Einsatz von KI in der Arbeitswelt mit sich bringt, muss Rechnung getragen, und auch für Betriebsräte und Beschäftigte positiv gestaltet werden. Die Aktualisierung des Aktionsplans für digitale Bildung eignet sich dafür, die Mitgliedstaaten dabei zu unterstützen, Kapazitäten und Instrumente für digitale Bildung auch im Bereich von KI weiter auszubauen. Zur Stärkung von KI-Kompetenzen auf europäischer Ebene ist eine Vernetzung von nationalen KI-Lern-Plattformen und KI-Kursen erstrebenswert und diese auch für die breite Bevölkerung zugänglich zu machen.

D. Schwerpunkt auf KMU

Die Bundesregierung begrüßt den Schwerpunkt auf KMU. Die beschriebenen Maßnahmen müssen konsequent ausgeweitet werden, sodass möglichst viele KMU von den digitalen Innovationszentren erreicht werden. Keinesfalls sollte die Anzahl der geförderten digitalen Innovationszentren statisch auf die Mitgliedstaaten verteilt und auf nur ein Zentrum pro Land begrenzt werden. Flächenstaaten benötigen mehrere in der Fläche verteilte Zentren, um regional ansässige KMU zu erreichen.

Beim Einsatz von KI in KMU kann neben einem datengetriebenen auch ein prozessgetriebener Ansatz zielführend sein. Dafür werden zunächst Prozesse in Betrieben genau analysiert und dann daraus abgeleitet, wo gezielt Daten erfasst werden müssen und wo KI angewendet werden kann, um die Prozesse zu optimieren.

E. Partnerschaft mit dem privaten Sektor

Öffentlich-private Kooperationen sind ein wichtiges Element, um Entwicklungen hin zu einem integrierten europäischen Datenraum und letztlich einem europäischen KI-Ökosystem als Wertschöpfungsnetzwerk für Innovationen zu ermöglichen. Mit dem Projekt GAIA-X sind Regierungen, Unternehmen und verschiedene Organisationen Deutschlands und Frankreichs, aber auch weiterer Mitgliedstaaten bereits erste Schritte in Richtung einer privat-öffentlichen Kooperation gegangen.

Deutschland setzt sich zum Ziel, eine digitale Qualitätsinfrastruktur zur Entwicklung und, wo sinnvoll, Beurteilung von KI-Systemen zu etablieren und diese auch Nutzerinnen und Nut-

zern aus anderen Mitgliedstaaten zugänglich zu machen. Dies ist für die schnellere Zulassung von Produkten in regulierten Bereichen (Gesundheit, Sicherheit oder Mobilität) von hoher Bedeutung.

F. Die Nutzung von KI im öffentlichen Sektor fördern

KI birgt für hoheitliche Aufgaben und die öffentliche Verwaltung großes Potenzial und sollte in diesen Bereichen verstärkt zum Einsatz kommen. Die Bundesregierung unterstützt deshalb die Maßnahmen zur Förderung der Nutzung von KI im öffentlichen Sektor. Ausgangspunkt ist stets die Wahrung der Grundrechte. Zudem sollten Bürgerinnen und Bürger bei der Entwicklung und Anwendung von KI auf geeignete Weise informiert und beteiligt werden, um ihre Erfahrungen und Bedarfe berücksichtigen zu können. Zusätzlich zu den vorgeschlagenen Dialogen auf Sektorebene sollte auch ein Dialog über die Möglichkeiten und rechtlichen Grenzen für den Einsatz von KI für hoheitliche Aufgaben im Sicherheitssektor initiiert werden.

G. Den Zugang zu Daten und Recheninfrastrukturen sichern

Die Bundesregierung begrüßt wegen der Bedeutung von Daten für KI-Entwicklung und Anwendung die Verknüpfung des Weißbuchs mit der Europäischen Datenstrategie. Interoperabilität und die notwendige hohe Qualität der Daten müssen sichergestellt sein. Notwendig ist ferner die Verfügbarkeit hochwertiger Analysetools, um mit den Daten zu arbeiten. Gerade im Bereich des Gesundheitswesens sowie des Umwelt- und Naturschutzes, wo über die zunehmende Verbreitung von „Smart Devices“ Daten auch jenseits der öffentlichen Hand mit hohem Potenzial für die Gewährleistung der öffentlichen Daseinsvorsorge entstehen, bestehen große Chancen.

Die Bundesregierung bittet die Europäische Kommission zu prüfen, ob ein zweites IPCEI im Bereich der Mikroelektronik zielführend wäre. Im Rahmen des europäischen KI-Konzeptes sollte der Zugang zu kritischer Hard- und Software berücksichtigt werden und ein kompetitives Angebot europäischer Anbieter von Chip-Herstellern, Startups und Technologieunternehmen aufgebaut werden. Zudem vollzieht sich die Bereitstellung von Rechenleistung zunehmend über Cloudmodelle (hardware-as-a-service).

Das Programm „Digitales Europa“ als neues Sektorprogramm des nächsten mehrjährigen Finanzrahmens (MFR) sollte einen thematischen Schwerpunkt auf Hoch- und Höchstleistungsrechnern sowie auf KI legen. Sollte das Budget stark gekürzt werden, wäre die Durchführung von Schlüsselinitiativen zu KI, Daten und industrieller Wettbewerbsfähigkeit akut gefährdet und würde die Abhängigkeit von nicht-europäischen Technologie- und Infrastruk-

turanbietern fortschreiben. Dies könnte die Erholung der europäischen Industrie nach der Covid-19-Pandemie gefährden.

H. Internationale Aspekte

Die Bundesregierung begrüßt, dass die internationale Zusammenarbeit auf einem wertebasierten Ansatz beruht und weiterhin darauf ausgerichtet werden soll, eine an ethischen und ökologischen Prinzipien orientierte KI-Entwicklung und Nutzung unter Achtung der Menschenwürde und der Grundrechte, einschließlich der Partizipation und des Schutzes vor Diskriminierung, der Privatsphäre, der persönlichen Daten und der Barrierefreiheit zu fördern und diesen „europäischen“ Ansatz im Rahmen der internationalen Zusammenarbeit zu exportieren. Dabei sollten auch wirtschaftlich schwächere Staaten dabei unterstützt werden, die Vorteile von KI für lokale Innovation zu nutzen, etwa durch Open Data. Aus Gründen der europäischen und nationalen Sicherheit kann es angezeigt sein, den Zugang zu einigen ausgewählten Datensätzen unter Einhaltung der WTO-Regeln und der Bestimmungen der EU-Dual-use Verordnung zu verweigern. Internationale Geschäftsmodelle auf Basis von Datennutzung und KI müssen Planungssicherheit und Schutz erfahren, wenn sie den europäischen Ansatz verfolgen.

Teil 2: Ein Ökosystem für Vertrauen: KI-Regulierungsrahmen

Die Bundesregierung teilt die Einschätzung der Europäischen Kommission, dass KI sowohl Chancen als auch Risiken mit sich bringt. Im Interesse aller Beteiligten sind daher klare Regelungen sinnvoll, die das Vertrauen in KI stärken, die verschiedenen Belange angemessen ausgleichen, Raum für weitere technische und soziotechnische Entwicklungen lassen und deren Einführung beschleunigen können. Damit sich ein hohes Vertrauen in KI bilden kann, bedarf es einer menschenzentrierten, verantwortungsvollen und gemeinwohlorientierten Entwicklung und Nutzung von KI. Um den einheitlichen Binnenmarkt zu stärken, sollten erforderliche Regelungen auf EU-Ebene beschlossen werden und EU-weit gelten.

A. Problemstellung

Die Bundesregierung teilt die Analyse der Europäischen Kommission, dass bei der Nutzung von KI Risiken für Grundrechte von Bürgerinnen und Bürgern, zum Beispiel ungerechtfertigte Diskriminierungen, sowie in Bezug auf Sicherheits- und Haftungsfragen auftreten können.

Gleichzeitig weist sie darauf hin, dass es Bereiche gibt, wo der Einsatz von KI ein enormes Innovationspotenzial besitzt. Bei der Regulierung ist sorgfältig darauf zu achten, dass Innovationen gefördert und nicht gehemmt werden.

B. Mögliche Anpassungen des bestehenden EU-Rechtsrahmens

Die Europäische Kommission hebt in Teil 2 zu Recht hervor, dass für die Entwicklung und Nutzung von KI bereits europäische Rechtsvorschriften gelten, etwa im Hinblick auf Grundrechte, Verbraucherschutz sowie Produktsicherheit und -haftung. Allerdings berücksichtigen diese die im Weißbuch genannten spezifischen Risiken von KI-Anwendungen zum Teil noch nicht oder nicht angemessen, sodass Defizite bei der Anwendung und Durchsetzung dieser Rechtsvorschriften bestehen können.

Die Bundesregierung begrüßt den vorgeschlagenen Ansatz, den bestehenden EU-Rechtsrahmen dahingehend zu überprüfen, ob die geltenden Rechtsvorschriften den Risiken und Anforderungen von KI-Anwendungen gewachsen sind und wirksam durchgesetzt werden können und ggf. welche Anpassungen oder neue Rechtsvorschriften notwendig sind.

C. Anwendungsbereich eines künftigen EU-Rechtsrahmens

Zusätzlich zu den möglichen Anpassungen der bestehenden Rechtsvorschriften (z.B. im Produktsicherheits- und Produkthaftungsrecht) können daher je nach Ausgang der Prüfung eventuell auch neue, speziell auf KI ausgerichtete Rechtsvorschriften erforderlich sein.

Die Bundesregierung begrüßt grundsätzlich den skizzierten Ansatz für einen EU-Rechtsrahmen für KI, der den im KI-Weißbuch beschriebenen Chancen und Risiken von KI angemessen begegnet, Innovation fördert, Interessen fair ausgleicht und Überregulierung vermeidet. Dieser sollte, wie von der Europäischen Kommission vorgeschlagen, für Produkte und Dienstleistungen gelten, bei denen KI zum Einsatz kommt, und sowohl den Einsatz von KI durch staatliche Stellen als auch durch Privatpersonen und Unternehmen erfassen. Allerdings muss innerhalb eines solchen Ansatzes dem Umstand Rechnung getragen werden, dass eine KI-Nutzung durch die öffentliche Hand anderen rechtlichen Rahmenbedingungen als im Privatsektor unterliegt. Beispielsweise stellen sich im Bereich der Eingriffsverwaltung spezifische grundrechtliche Fragen für das „Ob“ und das „Wie“ eines staatlichen KI-Einsatzes, zum Beispiel im Bereich der biometrischen Fernidentifikation.

Von großer Bedeutung ist dabei die Definition von „KI“. Hier sollte eine Formulierung gefunden werden, die möglichst viele KI-Anwendungen erfasst. Die Definitionsansätze u.a. der Hochrangigen Expertengruppe gehen in die richtige Richtung, müssen aber für einen opera-

tionalisierbaren gesetzlichen Tatbestand präzisiert und konkretisiert werden und gleichzeitig der dynamischen Entwicklung im Bereich der KI gerecht werden.

Die Bundesregierung unterstützt die Ansicht der Europäischen Kommission, dass der Rechtsrahmen auf einem chancen- und risikobasierten Ansatz beruhen sollte, um die Verhältnismäßigkeit des regulatorischen Eingreifens zu gewährleisten. Allerdings bedarf die differenzierte Umsetzung eines risikobasierten Ansatzes einer weiteren Erörterung. Während die Europäische Kommission erwägt, Anforderungen nur für KI-Systeme mit „hohem Risiko“ vorzusehen, erachtet die Bundesregierung ein Klassifikationsschema aus mehr als zwei Stufen für angebracht. Da die Europäische Kommission selbst betont, dass bestimmte Aspekte weder durch bestehende horizontale noch durch sektorspezifische Rechtsvorschriften abgedeckt werden, ist es fraglich, ob für KI-Anwendungen mit geringerem als „hohem“ Risiko allein die bereits geltenden EU-Vorschriften ausreichen.

Die Bundesregierung bittet die Europäische Kommission daher, ein Klassifikationsschema für KI-Systeme gemeinsam mit den Mitgliedstaaten zu entwickeln. Ein nach Chancen und Risiken ausgerichteter Regulierungsansatz muss unterschiedliche Eigenschaften von KI-Systemen beachten. Das Klassifikationsschema muss einerseits berücksichtigen, dass es Anwendungen ohne Schädigungspotenzial gibt. Andererseits muss das Klassifikationsschema Abstufung für relevante Risiken und Schäden unter Beachtung von Schadenshöhe und Schadenswahrscheinlichkeit vorsehen. Relevante Risiken können etwa bestehen für Leben und Gesundheit, Vermögen, demokratische Prozesse, Umwelt, Klima, soziale, gesellschaftliche und wirtschaftliche Teilhabe. Die Klassifizierung muss daher sowohl unterschiedliche Risiken einer Anwendung in einem bestimmten Anwendungskontext zutreffend bestimmen als auch eine praktikable Zuordnung des KI-Systems durch den Rechtsanwendenden möglich machen, wobei Gemeinwohlinteressen und individueller Nutzen zu berücksichtigen sind und Innovationen nicht beeinträchtigt werden dürfen. Aus diesem Grund sollten auch Ausnahmetatbestände für Forschung und Entwicklung geprüft werden. Zudem sollten Anwendungen ohne Schädigungspotenzial keiner spezifischen Kontrolle unterliegen.

Die Europäische Kommission schlägt bezüglich der Definition eines KI-Systems mit „hohem Risiko“ vor, dieses Merkmal dahingehend zu konkretisieren, dass sowohl der "Sektor" als auch die "beabsichtigte Verwendung" eines KI-Systems "erhebliche Risiken" bergen müsse. In der Folge würden bestimmte risikobehaftete Verwendungen von vornherein nicht erfasst, wenn sie nicht bestimmten Sektoren unterfallen. Die Europäische Kommission schlägt "Ausnahmefälle" vor, die unabhängig von dem betreffenden Sektor als hoch-riskant eingestuft werden sollen. Die KI-Anwendungen, die die Europäische Kommission an dieser Stelle ver-

anschaulichend benennt (Systeme im Rahmen von Einstellungsverfahren, verbraucherrelevante Anwendungen, Anwendungen zur biometrischen Fernidentifikation), verdienen auch aus Sicht der Bundesregierung besondere Aufmerksamkeit. Dass die Europäische Kommission im Weißbuch es als notwendig ansieht, Ausnahmetatbestände zu bilden, erfordert aber, die vorgeschlagene kumulative Definition des Merkmals "hohes Risiko" zu überdenken und ggf. zu erweitern.

Neben der Berücksichtigung von Risiken für Sicherheit, Verbraucherrechte und Grundrechte ist es essenziell, daneben auch andere hochrangige Belange im Allgemeininteresse wie etwa Klima- und Umweltschutz ausdrücklich anzuerkennen und so das große Potenzial von „AI Made in Europe“ für den Green Deal auszuschöpfen.

Die Bundesregierung regt darüber hinaus an, für KI-Systeme mit hohem Risiko ein Register sowie eine Meldepflicht bei Unfällen bzw. Vorfällen in Form eines Vigilanzsystems zu schaffen. Da Sicherheitsbehörden aufgrund ihrer Aufgabenprofile fast ausschließlich KI-Systeme mit hohem Risiko einsetzen, wären sie durch ein Vigilanzsystem und der Betreuung des Registers übermäßig stark betroffen. Die in Abschnitt F. genannte zentrale Stelle für den KI-Einsatz in Sicherheitsbehörden sollte auch zentral für alle Sicherheitsbehörden als Registerstelle für diesen Sektor fungieren.

D. Arten von Anforderungen

Die Bundesregierung teilt die Auffassung der Europäischen Kommission, dass Aspekte, die bereits durch bestehende horizontale oder sektorspezifische Rechtsvorschriften abgedeckt sind, weiterhin durch diese Rechtsvorschriften geregelt bleiben sollten. Das oben vorgeschlagene Klassifikationsschema sollte für das jeweilige Risiko angemessene Anforderungen beinhalten. Ein solcher möglicher erweiterter EU-Rechtsrahmen für KI sollte ggf. noch um spezifische Anforderungen ergänzt werden.

Allgemein begrüßt die Bundesregierung den Katalog von Anforderungen, den die Europäische Kommission in Bezug auf Trainingsdaten, Aufbewahrung von Daten und Aufzeichnungen, Bereitstellung von Informationen, Robustheit und Genauigkeit, menschliche Aufsicht sowie biometrische Fernidentifikationssysteme formuliert. Das jeweils konkrete Erfordernis, die Reichweite und konkrete gesetzliche Ausgestaltung der Anforderungen bedürfen indes noch weiterer Ausarbeitung. Darüber hinaus sollte geprüft werden, ob und ggf. welche weiteren Aspekte als verbindliche Anforderungen rechtlich verankert werden sollten (etwa Vorgaben zu „Energieeffizienz“ und Verbote bestimmter KI-Anwendungen).

Neben konkreten Anforderungen hält die Bundesregierung es im Sinne einer prinzipienbasierten Regulierung für zielführend, dass unionsweit harmonisierte zentrale Grundsätze und Prinzipien für eine vertrauenswürdige KI formuliert werden (etwa im Hinblick auf Transparenz, Nachvollziehbarkeit, Überprüfbarkeit, Nicht-Diskriminierung, Möglichkeit der menschlichen Letztentscheidung, Robustheit, Sicherheit, Rechenschaftspflichten, Folgenabschätzung, Barrierefreiheit). Die Harmonisierung derartiger Grundsätze und Prinzipien könnte die einheitliche Auslegung und Anwendung der Vorschriften erleichtern. Außerdem könnten sie der von der Europäischen Kommission zu Recht betonten Konkretisierung durch Normung und Standardisierung einen Orientierungsrahmen vorgeben.

Bei der Auferlegung von Anforderungen sind insbesondere KMU nicht unverhältnismäßig zu belasten.

Der Rechtsrahmen könnte ferner auch grundlegende Vorgaben zu den subjektiven Rechten von Nutzern / Verbrauchern vorsehen. Dazu gehört insbesondere eine detaillierte Regelung zu Betroffenenrechten sowie Vorgaben zur Rechtsdurchsetzung etwa in Gestalt von Vermutungs- und Beweislastregelungen.

Zu den im KI-Weißbuch genannten Anforderungen im Einzelnen:

a) Trainingsdaten

Die Bundesregierung begrüßt zunächst ausdrücklich den Vorschlag, dass für Trainingsdaten von KI-Systemen verbindliche rechtliche Anforderungen in Betracht gezogen werden. Sie hält dies für den richtigen Anknüpfungspunkt, da Trainingsdaten eine wesentliche Grundlage für die Entwicklung insbesondere von lernenden Systemen bilden. Dafür sollten konsistent auch Anforderungen für Test- und Evaluierungsdaten in Betracht gezogen werden.

Aus Sicht der Bundesregierung kann dies je nach Klassifizierung des KI-Systems auch Qualitätsparameter und -anforderungen für Trainings-, Test- und Evaluierungsdaten beinhalten, damit entsprechende KI-Systeme mit quantitativ ausreichenden und qualitativ hochwertigen Datensätzen entwickelt werden. Wichtige Indikatoren sind dabei bspw. die inhaltliche Korrektheit, Aktualität, Repräsentativität und Vollständigkeit der Datensätze. Dabei müssen grundsätzlich immer der Zielkontext des Systems und die Anwendungsumgebung berücksichtigt werden, um darüber zu entscheiden, ob die Quantität und Qualität von Datensätzen den Anforderungen genügt. Im Bereich Forschung und Entwicklung muss dabei berücksichtigt werden, dass Trai-

ningsdatensätze nicht immer den o.g. Ansprüchen etwa an Vollständigkeit und Repräsentativität genügen können, die Entwicklung einer geeigneten Datenbasis selbst Teil von Forschung und Entwicklung sein kann und ausreichend Spielräume für die Weiterentwicklung der Systeme gegeben sein müssen.

Bei der Nutzung von KI-Systemen können Risiken mit Blick auf grundrechtsrelevante Ungleichbehandlungen auftreten, wenn etwa Trainingsdaten gesellschaftliche Ungleichheiten abbilden und diese dadurch fortgeschrieben und gegebenenfalls verstärkt werden. Nicht repräsentative Trainingsdatensätze oder solche, die strukturelle Ungleichbehandlungen abbilden, aber auch Fehler bei der Programmierung oder fehlende bzw. unzureichende Qualitätssicherungen können Diskriminierungsstrukturen perpetuieren und Individuen benachteiligen. Um Vertrauen zu stärken, muss die Wirkungsweise von KI-Systemen möglichst transparent und nachvollziehbar sein.

Grundsätzlich unterstützt die Bundesregierung das Bestreben, die Sicherheit von KI-Systemen durch geeignete Anforderungen an Trainings-, Test- und Evaluierungsdaten zu optimieren. Insoweit wird eine Überschneidung mit der Anforderung bzgl. Robustheit und Genauigkeit gesehen. Auf die beispielhafte Erwägung seitens der Europäischen Kommission, Trainings-, Test- und Evaluierungsdaten müssten alle Szenarien abdecken, die für die Vermeidung gefährlicher Situationen relevant sind, gibt die Bundesregierung allerdings zu bedenken, dass Menschen immer nur von erkennbaren und realistischen Risiken ausgehen können. Es könnte daher angemessen sein, die Anforderung dahingehend zu konkretisieren, dass lediglich erkennbare und realistische Szenarien abgedeckt werden müssen.

Der Ansatz der Europäischen Kommission, in erforderlichen Fällen durch verbindliche Anforderungen u.a. an die Repräsentativität/Ausgewogenheit von Datensätzen dem Diskriminierungspotenzial von KI-Systemen wirksam zu begegnen, wird von der Bundesregierung ausdrücklich unterstützt. Bewertungsgrundlage dafür, ob diese Anforderungen berücksichtigt wurden, kann auch das Ergebnis des jeweiligen KI-Systems sein, so dass ein Zugriff auf den Trainings-, Test- und Evaluierungsdatensatz als solchen nicht stets erforderlich ist. Dies setzt jedoch voraus, dass für das Einsatzszenario geeignete Verfahren zur Prüfung der Ergebnisse auf Repräsentativität und Ausgewogenheit zur Verfügung stehen.

b) Aufbewahrung von Daten und Aufzeichnungen

Die Bundesregierung unterstützt grundsätzlich die Vorschläge zur Dokumentation, Aufzeichnung und Aufbewahrung von Daten. Verbindliche Anforderungen können einen wichtigen Beitrag zu Transparenz, Nachvollziehbarkeit und Erklärbarkeit von KI-Systemen leisten. Sie ermöglichen zudem eine wirkungsvolle Überwachung und Durchsetzung durch die zuständigen Aufsichtsbehörden.

Sofern eine Verpflichtung zur Aufbewahrung von Datensätzen selbst erforderlich ist, setzt diese Anforderung eine hohe Datenintegrität und Datensicherheit voraus. Es bedarf effektiver IT-Sicherheitsvorgaben, die unerlaubten Zugriff, unerlaubte Nutzung oder Manipulation der Daten verhindern. Der Zugang zu und die Nutzung der aufbewahrten Datensätze müssen an formal prüfbare rechtliche Vorgaben gebunden werden.

Aus dem KI-Weißbuch heraus ist bislang nicht ersichtlich, in welchen „bestimmten begründeten Fällen“ eine Verpflichtung zur Aufbewahrung der Datensätze als solche bestehen sollte. Vor allem in der Strafverfolgung ist die Aufbewahrung von Trainings-, Test- und Evaluierungsdaten unentbehrlich, um mögliche Verzerrungen und Fehlentscheidungen nachvollziehen zu können. Auch der „begrenzte, angemessene Zeitraum“, währenddessen die Datensätze aufbewahrt werden müssen, bedarf näherer Konkretisierung.

In erforderlichen Fällen sollten Anforderungen an die Art und Weise der Dokumentation gestellt werden. Zur Bewahrung der Nachvollziehbarkeit muss eine Revisionssicherheit implementiert werden, die die unterschiedlichen Versionsstände von Trainings-, Test- und Evaluierungsdaten aber auch der Software selber abbildet. Weiterhin muss durch organisatorische und technische Maßnahmen sichergestellt werden, dass nur berechtigte Personen Zugriff auf Trainingsdaten, algorithmische Modelle, Protokolle und etwaige Evaluierungen haben.

c) Bereitstellung von Informationen

Die Bundesregierung begrüßt grundsätzlich die formulierte Anforderung, dass bestimmte Informationen zu KI-Systemen einem noch näher zu definierenden Kreis von Personen mit berechtigtem Interesse – u.a. Verbraucherinnen und Verbrauchern, Bürgerinnen und Bürgern, Betreibern von KI-Systemen, Aufsichtsbehörden – bereitgestellt werden müssen.

Diese Anforderung leistet einen wichtigen Beitrag zu Transparenz, Nachvollziehbarkeit und Überprüfbarkeit von KI-Systemen. Denn derzeit ist häufig nicht eindeutig erkennbar, ob ein Produkt oder eine Dienstleistung überhaupt ein KI-System verwendet, und wenn ja, nach welchen Kriterien das KI-System operiert.

Nach Ansicht der Bundesregierung bedarf es indes einer weiterführenden Prüfung, wie die von der Europäischen Kommission vorgeschlagenen Informationen über die Fähigkeiten und Grenzen von bestimmten KI-Systemen konkretisiert werden können. Für die zur Information Verpflichteten soll kein unangemessen hoher Erfüllungsaufwand verbunden sein und nicht unverhältnismäßig in deren Rechtspositionen, insbesondere Berufs- und Geschäftsgeheimnisse, eingegriffen werden. Für die Berechtigten ist auf verständliche und niedrighschwellig zugängliche Informationen zu achten.

Die Bundesregierung stimmt der Europäischen Kommission zu, dass über datenschutzrechtlich schon heute notwendige Kennzeichnungen hinaus zusätzliche Pflichten zur Kennzeichnung, dass Menschen mit einem KI-System interagieren und nicht mit einem Menschen, erforderlich sein können.

d) Robustheit und Genauigkeit

Der Europäischen Kommission ist zuzustimmen, dass KI-Systeme technisch solide und präzise sein müssen, um vertrauenswürdig zu sein. Dies wird durch Beachtung von Standards und Prinzipien in der Architektur von KI-Systemen und der fortlaufenden Qualitätssicherung von KI-Systemen sichergestellt.

Die Bundesregierung hält Anforderungen an die Robustheit und Genauigkeit von bestimmten KI-Systemen grundsätzlich für sinnvoll. Allerdings kommt es auf die konkrete Ausgestaltung derartiger Anforderungen an. In jedem Fall muss gewährleistet sein, dass durch Sicherheits- und Schutzstandards die Entwicklung innovativer KI-Systeme nicht in unangemessener Weise behindert wird.

Für die Evaluierung der Robustheit von KI-Systemen sollten nach Ansicht der Bundesregierung grundsätzlich realistische Einsatzszenarien dienen. Eine Betrachtung von theoretisch denkbaren Szenarien, die dazu führen könnte, dass eine KI nicht einzusetzen wäre, soll aber möglich sein.

Die Bundesregierung weist zudem darauf hin, dass der Aspekt der Informationssicherheit – verstanden als Schutz sowohl vor zufälligen Fehlern, z.B. durch unerwarte-

te Nutzereingaben, als auch vor gezielter Manipulation durch Angreifer – eine stärkere Berücksichtigung finden sollte, als bislang durch das KI-Weißbuch erfolgt. Die Bundesregierung hält einen verpflichtend hohen IT-Sicherheitsstandard für KI-Systeme mit hohem Risiko für unabdingbar. Andernfalls drohen erhebliche Risiken in den von der Kommission beschriebenen Feldern (u.a. Schäden für Leib und Leben, Beeinträchtigung von Grundrechten, Diskriminierung).

Zentral ist die Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit des KI-Systems über dessen gesamten Lebenszyklus als solches. KI-Systeme klassifizieren Daten vielfach anhand von anderen Merkmalen anders als das ein Mensch tun würde und schaffen dadurch für den Menschen schwer erkennbare Angriffsmöglichkeiten. Bei der Entwicklung von KI-Systemen sollte daher die Erkennung von Angriffen im Rahmen einer Risikobewertung mitgedacht werden. Für Klassen von Algorithmen, bei denen Erklärbarkeit nur eingeschränkt oder gar nicht zu erreichen ist, bedarf es demensprechend rechtlicher und technischer Vorkehrungen, die insbesondere auch den Anforderungen der IT-Sicherheit genügen. Insbesondere ist dabei die Komplexität heutiger KI-Modelle zu berücksichtigen, die mit Millionen von trainierbaren Parametern und ebenso zahlreichen möglichen Eingaben mit klassischen Verfahren der IT-Sicherheit nicht beherrschbar sind. Daher sind bedarfsabhängig neue Verfahren für die Informationssicherheit von KI-Systemen zu entwickeln. Schließlich müssen KI-Systeme vor Angriffen mit dem Ziel der Extraktion von Daten sowie der Injektion von korrumpierenden Daten geschützt werden.

e) Menschliche Aufsicht

Die Bundesregierung unterstützt grundsätzlich das Vorhaben der Europäischen Kommission, Anforderungen an die menschliche Aufsicht von KI-Systemen zu entwickeln, einschließlich einer Möglichkeit der menschlichen Letztentscheidung, sofern wegen sektorspezifischer Belange darauf nicht möglicherweise verzichtet werden kann (z.B. zukünftig beim autonomen Fahren).

Die Bundesregierung nimmt die beschriebenen Wege der Ausübung menschlicher Aufsicht zustimmend zur Kenntnis. Das KI-Weißbuch enthält keine Spezifizierung, unter welchen Umständen welche Form menschlicher Aufsicht als Anforderung verbindlich vorgeschrieben werden sollte. Die Vorschläge zu Anforderungen an menschliche Aufsicht von KI-Systemen gilt es daher weiterzuentwickeln.

Dabei wird zu beachten sein, dass der Mensch die Ergebnisse des KI-Systems hinterfragen kann. Daher sind die Einwirkungsmöglichkeiten in den Nutzungsprozessen explizit abzubilden. So kann sichergestellt werden, dass zu jedem Zeitpunkt ein Mensch in der Lage sein soll, das System erforderlichenfalls außer Kraft zu setzen oder dessen Funktionsweise zu verändern.

f) Besondere Anforderungen an bestimmte KI-Anwendungen, z. B. für die biometrische Fernidentifikation

Die Bundesregierung begrüßt, dass Systeme für biometrische Fernidentifikation aufgrund ihrer besonderen Risiken für die Freiheitsrechte der Bürgerinnen und Bürger besondere Aufmerksamkeit erfahren. Die Diskussion über das grundsätzliche „Ob“ des Einsatzes solcher Systeme und damit möglicher Verbote läuft noch; soweit sie eingesetzt werden sollen, sind zuvor klare gesetzliche Anforderungen zu formulieren.

Die Bundesregierung gibt ferner zu bedenken, dass das grundsätzliche datenschutzrechtliche Verbot der Verarbeitung biometrischer Daten nur die Verwendung solcher Systeme begrenzt. Aufgrund der Tiefe der möglichen Eingriffe in grundrechtlich geschützte Güter ist darüber hinaus eine abgestufte Regulierung beim Inverkehrbringen von solchen Systemen zu prüfen, die durch eine Verbraucherin oder einen Verbraucher über das eigene mobile Endgerät eingesetzt werden können.

E. Adressaten

Die Europäische Kommission benennt die verschiedenen Akteure, die am Lebenszyklus eines KI-Systems beteiligt sind und als Verpflichtete der Anforderungen in Betracht kommen. Die Bundesregierung begrüßt den Vorschlag, dass die einzelnen Anforderungen zuerst jeweils dem Akteur auferlegt werden sollen, der am ehesten in der Lage ist, den potenziellen Risiken zu begegnen. Dies erscheint auch aus Gründen der Verhältnismäßigkeit geboten.

F. Einhaltung und Durchsetzung

Die Bundesregierung unterstützt den Vorschlag, für KI-Systeme mit hohem Risiko das Durchlaufen eines objektiven Konformitätsbewertungsverfahrens verbindlich vorzuschreiben. Dieses sollte durchgeführt werden, bevor Produkte oder Dienstleistungen, bei denen KI-Systeme mit hohem Risiko zum Einsatz kommen, auf dem EU-Binnenmarkt in Verkehr gebracht werden, oder wenn derartige, im Verkehr befindliche Produkte oder Dienstleistungen wesentliche Änderungen erfahren. Zu Recht weist die Europäische Kommission auf die Not-

wendigkeit wiederholter Bewertungen von sich weiterentwickelnden lernfähigen KI-Systemen hin.

Die Bundesregierung teilt auch den Ansatz, dass für Produkte und Dienstleistungen, für die im Rahmen des bestehenden Rechts sowie der Qualitätsinfrastruktur bereits Konformitätsbewertungsmechanismen existieren, auf diese bestehenden Mechanismen zurückgegriffen werden kann. Es müssten dann lediglich die materiellen Anforderungen angepasst werden. Für andere Produkte oder Dienstleistungen kann es der Einführung neuer Bewertungsmechanismen bedürfen. Dabei gilt es sicherzustellen, dass die Akteure erforderliche Genehmigungen an einer Stelle erhalten können („One-Stop-Shop“). Für hoheitliche Aufgaben im Sicherheitsbereich könnte die Einrichtung einer zentralen Stelle zur Zertifizierung bzw. Konformitätsbewertung etwaiger bei den Sicherheitsbehörden eingesetzter KI-Systeme geprüft werden.

Als Maßstab einer Konformitätsbewertung eignen sich aus Sicht der Bundesregierung die in Abschnitt D formulierten Anforderungen; keine von ihnen müsste von vornherein aus der Konformitätsbewertung ausgenommen werden; auch die Anforderung nach vorzulegenden Informationen scheint für ein Konformitätsbewertungsverfahren geeignet zu sein.

Für Unternehmen sind Konformitätsbewertungsverfahren ein bewährter Mechanismus, um Rechtssicherheit über die Vereinbarkeit eines Produkts oder einer Dienstleistung mit EU-Recht zu erlangen. Gleichzeitig sind derartige Verfahren zeit- und kostenintensiv. Die Bundesregierung teilt daher die Auffassung der Europäischen Kommission, dass insbesondere für KMU und den Dritten Sektor geeignete Mittel (Unterstützungsstrukturen, Online-Instrumente) zur Verfügung gestellt werden sollen, um den Verwaltungsaufwand zu begrenzen. Gleichzeitig sollte die paritätische Teilnahme von KMU an Normierungsgremien unterstützt werden. Letzteres gilt auch für die organisierte Zivilgesellschaft.

Ferner wird darüber nachzudenken sein, welche Ausnahmen von einer grundsätzlich vorgeschriebenen Konformitätsbewertung geboten sein können. Um die Innovationsfähigkeit im Bereich KI zu stärken, könnten z.B. geeignete Öffnungsklauseln für Forschung und Wissenschaft (Reallabore) in Erwägung gezogen werden. Außerdem könnte es angemessen sein, dass die reine Evaluation von KI-Systemen (etwa im Rahmen von Anwendbarkeitsstudien, Marktsichtungen oder Laborforschung) entweder keiner oder nur einer eingeschränkten Prüfung unterzogen wird. Darüber hinaus könnte eine Öffnungsklausel für Situationen geprüft werden, in denen eine zeitnahe, ggf. befristete Markteinführung aus Gründen des öffentlichen Wohls geboten erscheint (etwa für außergewöhnliche Krisensituationen wie einer Pandemie), soweit die Risiken überschaubar erscheinen.

Die Europäische Kommission weist zu Recht darauf hin, dass die Einführung eines vorgelagerten Konformitätsbewertungsverfahrens für KI-Systeme mit „hohem Risiko“ die Überwachung der Einhaltung aller bestehenden rechtlichen Anforderungen und deren Durchsetzung durch nationale Behörden unberührt lässt.

Zuständig für die behördliche Überprüfung sollten bereits bestehende nationale Aufsichtsbehörden sein. Wo bisher keine staatliche Aufsicht vorhanden ist, sollten Mitgliedstaaten verpflichtet werden, Behörden aufzubauen oder existierende Behörden mit Zuständigkeiten auszustatten.

Bezüglich der Einführung wirksamer Rechtsbehelfe verweist die Bundesregierung auch auf die Ausführungen in Teil 3 der Stellungnahme.

G. Freiwillige Kennzeichnung für risikoarme KI-Anwendungen

Die Bundesregierung begrüßt den Vorschlag eines freiwilligen Zertifizierungssystems für risikoarme KI-Anwendungen. Die Teilnahme sollte allerdings nicht nur Unternehmen, sondern auch öffentlichen Organisationen, Behörden und Vereinen offenstehen. Die Bundesregierung hält eine Befristung für notwendig, so dass Teilnehmende ihr Gütesiegel regelmäßig erneuern müssen. Das Gütesiegel sollte von europaweit anerkannten Stellen zuerkannt und von den Behörden der Mitgliedstaaten kontrolliert sowie im Binnenmarkt gegenseitig anerkannt werden.

Ferner bedarf es wirkungsvoller, rechtlich durchsetzbarer Sanktionen, wenn Teilnehmende die Anforderungen nicht erfüllen bzw. das Gütesiegel missbräuchlich nutzen.

H. Governance

Die Bundesregierung unterstützt grundsätzlich die Überlegungen zum Aufbau einer europäischen Governance-Struktur für KI in Form eines Rahmens für die Zusammenarbeit der zuständigen nationalen Behörden. Eine enge Zusammenarbeit ist eine wichtige Ergänzung, um den Rechtsrahmen in grenzüberschreitenden Fällen durchzusetzen, einen regelmäßigen Austausch von Informationen und bewährten Verfahren zu gewährleisten, Beratung im Bereich der Normung und Zertifizierung zu leisten und die Umsetzung des Rechtsrahmens zu fördern, beispielsweise durch Herausgabe von Leitlinien, Stellungnahmen und die Bereitstellung von Fachwissen.

Aus Sicht der Bundesregierung sollte sichergestellt sein, dass die Mitgliedstaaten jeweils eine koordinierende Institution benennen können, welche die Maßnahmen des europäischen

Netzwerks auf nationaler Ebene koordiniert und die jeweiligen nationalen Behörden einbezieht und bei ihren Aufgaben unterstützt.

Teil 3: Sicherheit und Haftung

A. Einführung

Die Bundesregierung begrüßt die umfangreiche Analyse des Produktsicherheits- und zivilrechtlichen Haftungsrechts hinsichtlich der KI, IoT und der Robotik. Sie teilt die Einschätzung, dass die „Haftungsrahmen in der Union [...] bisher gut“ funktionieren¹ und „grundsätzlich die bestehenden Haftungs Vorschriften der Union und der Mitgliedstaaten auch für neue Technologien geeignet“² sind. Zugleich wird die Einschätzung geteilt, dass das Aufkommen neuer digitaler Technologien in Bezug auf Produktsicherheit und -haftung neue Herausforderungen bergen kann. Rechtlich muss Geschädigten dieser Technologien das gleiche Schutzniveau gewährleistet werden wie Geschädigten traditioneller Technologien. Wie der Bericht aus Sicht der Bundesregierung zutreffend beschreibt, können sich die Herausforderungen digitaler Technologien insbesondere aus der gegenwärtigen und zunehmenden Vernetzung von Produkten (Konnektivität), ihrer Autonomie und Datenabhängigkeit, ihrer technischen Opazität und Komplexität sowie zunehmend komplexen Wertschöpfungsketten ergeben.³ Daraus ergeben sich insbesondere neue Herausforderungen für Datenschutz, Qualität, Sicherheit und Vertrauenswürdigkeit von KI und dem Versprechen „KI Made in Europe“ und damit einhergehend Herausforderungen einerseits für eine Qualitätsinfrastruktur - bestehend aus Messwesen, Normung und Standardisierung, Akkreditierung, Konformitätsbewertung, und Marktüberwachung - sowie für die funktionale Sicherheit von KI-basierten Produkten und Anwendungen. Soweit in dem Bericht Reformen erwogen oder Reformbedarf gesehen wird, erscheinen punktuelle Anpassungen für den Bereich des Haftungsrechts – dort wo sie erforderlich sind – grundsätzlich angemessen.

¹ Bericht, S. 14. (Hinweis: Die Seitenzahlen beziehen sich auf die deutsche Sprachfassung des Berichts).

² Bericht, S. 20.

B. Stellungnahme zum Bereich Sicherheit

Die Europäische Kommission stellt in ihrem Bericht als übergeordnetes Ziel eines rechtlichen Sicherheits- und Haftungsrahmens heraus, dass Produkte mit neuen Technologien sicher, zuverlässig und beständig funktionieren müssen.

Sicherheit ist eine unabdingbare Basis für Vertrauen und Akzeptanz in die neuen Technologien und trägt damit zur Wettbewerbsfähigkeit bei. Die Frage ist, ob der derzeitige Rechtsrahmen geeignet ist, ein ausreichendes Maß an Sicherheit zu gewährleisten.

Die vorliegenden Produktsicherheitsvorschriften, einschließlich sektorspezifischer Bestimmungen, die durch nationale Rechtsvorschriften und einschlägige Normen ergänzt werden, sind auch auf KI-Anwendungen anwendbar. Das mit den derzeitigen Produktsicherheitsvorschriften der Union festgelegte Sicherheitskonzept steht mit einem erweiterten Sicherheitskonzept zum Schutz von Verbraucherinnen und Verbrauchern und Nutzerinnen und Nutzern im Einklang. Es werden jegliche Risiken umfasst, die von dem Produkt ausgehen; dazu zählen nicht nur mechanische, chemische und elektrische Risiken, sondern auch Cyberrisiken und Risiken im Zusammenhang mit dem Verlust der Konnektivität von Produkten. Es ist im weiteren Prozess zu bewerten, ob sie angemessen durchgesetzt werden können, um den von KI-gestützten Produkten und Dienstleistungen ausgehenden Risiken zu begegnen.

Bei der Frage der Sicherheit von KI-Systemen nennt die KOM richtigerweise folgende zu beachtende Merkmale: Komplexität, Autonomie, große Datenmengen, Algorithmen, Opazität, Konnektivität/Offenheit (Security). Dazu ist im Einzelnen folgendes anzumerken:

I. Konnektivität/Offenheit (Security)

Das heutige Produktsicherheitskonzept umfasst auch Cyberrisiken und Risiken aus dem Verlust der Konnektivität. Die Rechtsvorschriften der Produktsicherheit richten sich dabei an den Hersteller des Produkts und umfassen Konstruktion und Bau, nicht jedoch den Betrieb eines Produkts. Gerade bei den Cyberrisiken ist aber eine intensive Abstimmung zwischen allen Akteuren [(Komponenten-)Hersteller und Integratoren auf der einen Seite und Betreiber auf der anderen Seite] erforderlich. Da es sich hier aber um zwei getrennte Rechtsbereiche handelt (Produktsicherheitsrecht / Binnenmarkt einerseits, betrieblicher Arbeitsschutz andererseits), bestehen Zweifel, ob diese erforderliche Abstimmung im Themenfeld Cybersicherheit im Produktsicherheitsrecht allein gelingen kann.

Die Aussage im Bericht, dass die Anwendungsbereiche um explizite Bestimmungen ergänzt werden sollten, erscheint nicht schlüssig. Vielmehr sollten eben nicht die jeweiligen Anwendungsbereiche geändert/ergänzt werden, sondern, wo es notwendig ist, die jeweiligen grundlegenden Anforderungen (Anforderungen an Bau, Konstruktion und Programmierung).

Der Betrieb eines KI-Systems, eines IoT-Gerätes oder eines robotischen Systems ist dauerhaft nur dann sicher möglich, wenn bei neu gefundenen Sicherheitslücken zeitnah Sicherheitsupdates erstellt und installiert werden. Für eine sichere Integration der Produkte bei den Anwendern sollten Hersteller Mindestanforderungen an die IT-Systeme angeben. Außerdem sollten die Produkte grundsätzlich nach dem neuesten Stand der Technik entwickelt werden, unter Berücksichtigung des gesamten Produktlebenszyklus, einschließlich der Informationssicherheit. Für eine sichere Integration der Produkte bei den Anwendern sollten Hersteller Mindestanforderungen an die IT-Systeme angeben. Dies würde die Sicherheit der Verbraucher erheblich verbessern.

II. Autonomie

Bereits heute deckt die Risikobeurteilung die vorhersehbare Verwendung ab, jedoch sind KI-Systeme nicht immer vorhersehbar und können ihre Eigenschaften nach dem Inverkehrbringen noch ändern.

Im Rahmen der Risikobeurteilung während des Entwicklungs-/Konstruktionsprozesses sind die Rahmenbedingungen, z. B. Steuerungsgrößen, Datenschutzanforderungen und erforderliche sicherheitstechnische Maßnahmen festzulegen. Das trifft auch auf KI-Systeme zu. Situationen, in denen die Eingrenzungen der Ergebnisse (Definition eines zulässigen Ergebnisbereiches) der KI-Systeme nicht vollständig im Voraus bestimmt werden können, sind aktuell nicht bekannt, auch nicht bei den derzeit bereits eingesetzten Systemen, die auf Nutzung maschineller Lernverfahren basieren. Dabei ist jedoch zu unterscheiden zwischen austrierten Modellen und maschinellen Lernverfahren, die während des Betriebes weiterlernen.

Der Vorschlag eines neuen Risikobewertungsverfahrens für autonomes Verhalten, das vom Hersteller nicht vorhersehbar ist sowie Vorschriften zur menschlichen Aufsicht gehen über den heutigen Anwendungsbereich des Produktsicherheitsrechts hinaus. Jedoch erscheint der Vorschlag notwendig und sinnvoll. Hier muss über eine stärkere Verknüpfung der Rechtsbereiche Bereitstellung von Produkten und Betrieb nachgedacht werden. Dabei sollte auch von Beginn an die notwendige Qualitätsinfrastruktur entwickelt und bereitgestellt werden sowie die Kompetenzen für Behörden aufgebaut werden. Auch hierbei sind sektorspezifische Belange zu beachten, etwa beim autonomen Fahren.

III. Datenabhängigkeit

Es ist eine umfassende Betrachtung von vorliegenden Anforderungen an die funktionale Sicherheit und an die Informationssicherheit bei der Risikobeurteilung erforderlich. Entscheidend sind hierbei die Genauigkeit und Relevanz der Daten. Darüber hinaus ist es notwendig, die Bereitstellung von Referenzdaten, Benchmarktests und die Überprüfung von Algorithmen

anhand von qualitätsgesicherten, vertrauenswürdigen Referenzdaten zur Verfügung zu stellen. Grundsätzlich wird die Aussage unterstützt, dass die Datenqualität während der gesamten Nutzungsdauer gewährleistet sein muss. Es ist aber zu beachten, dass dies nur vom Betreiber geleistet werden kann, der wiederum kein Wirtschaftsakteur im Sinne des Produktsicherheitsrechts ist.

IV. Opazität

Die Lern-, Arbeits- und Entscheidungsprozesse von KI-Systemen sind teilweise schwer nachzuvollziehen. Transparenz ist jedoch ein zentraler Baustein für das Vertrauen in KI-Systeme. Der Vorschlag zur Offenlegung von Algorithmen und Trainingsdaten gegenüber den Behörden im Falle von Unfällen wird daher begrüßt. Dies sollte jedoch nicht nur auf Unfälle beschränkt werden, sondern grundsätzlich auch im "begründeten Einzelfall" möglich sein. Die Transparenzanforderungen an KI Systeme sollten zudem auch die menschliche Aufsicht – dort wo erforderlich - ermöglichen. Zur Erreichung dieser Ziele ist Grundlagenforschung zu Erklärbarkeit von KI-Methoden notwendig.

V. Komplexität

Das Produktsicherheitsrecht trägt der Interaktion verschiedener Geräte bereits heute Rechnung. Software ist wesentlicher Bestandteil von KI-Systemen. Diesbezüglich adressiert das Produktsicherheitsrecht integrierte Software, meist jedoch nicht eigenständige Software. Sofern eigenständige Software die Sicherheit eines Produkts beeinflusst, muss diese auch im Produktsicherheitsrecht adressiert werden.

Die Aussage, dass wenn die vom Hersteller ursprünglich vorgesehene bestimmungsgemäße Verwendung aufgrund des autonomen Verhaltens geändert und die Einhaltung der Sicherheitsanforderungen beeinträchtigt wird und infolge dessen das gesamte Produkt als ein neues Produkt angesehen werden sollte, ist kritisch zu sehen. Für den Fall, dass aufgrund einer Software-Änderung ein neues Produkt entstanden ist, muss dieses Produkt vollumfänglich dem Stand der Technik entsprechen, da ein neues Inverkehrbringen vorliegt. Dies muss bei der Betrachtung einer Software-Änderung mitberücksichtigt werden.

Die Forderung nach expliziten Bestimmungen zur Zusammenarbeit zwischen Wirtschaftsakteuren und Betreibern begegnet wieder dem Problem, dass das Produktsicherheitsrecht heute bei der Inbetriebnahme endet, der Betreiber also nicht adressiert werden kann.

C. Wechselwirkungen zwischen der Produktsicherheit und der Produkthaftung

Die Bundesregierung teilt zunächst die Auffassung, wonach KI-Systeme konzeptuell integrierte Schutz- und Sicherheitsvorkehrungen aufweisen sollten, damit sie in jeder Phase

nachprüfbar sicher sind. Dabei ist eine abgestufte Betrachtungsweise differenziert nach praktikablen Risikoklassen erforderlich. Produktsicherheitsvorschriften, die spezifische und verbindliche Grundanforderungen statuieren, und Konformitätsbewertungsverfahren, in denen die Einhaltung dieser Standards geprüft werden, sind wichtige Steuerungsmechanismen, um Risiken von KI von vornherein auf ein gesellschaftlich akzeptiertes Maß zu begrenzen.

Im Zusammenhang mit der Inverkehrgabe von KI-Systemen ist es daher nach Auffassung der Bundesregierung vorrangig, allgemeingültige verbindliche Anforderungen für deren Sicherheit und Zulassung zu bestimmen. Dabei sollte besonders sorgfältig geprüft werden, wie mit KI-Systemen umgegangen wird, die durch Selbstlernfunktionen in der Lage sind, ihr „Verhalten“ eigenständig anzupassen. Aus Sicht der Bundesregierung darf der Prozess des Selbstlernens nicht unkontrolliert erfolgen bzw. nicht zu unkontrollierbaren Ergebnissen führen. In einem Konformitätsbewertungsverfahren zu prüfende Sicherheitsvorkehrungen, in bestimmten Fällen auch eine fortlaufende menschliche Aufsicht, müssen gewährleisten, dass der Lernprozess nachvollziehbar ist. Ebenfalls muss gewährleistet werden, dass eine Maschine keine anderen Aktionen ausführt, die von denen abweichen, die von den Herstellern ursprünglich beabsichtigt waren und folglich von den Nutzerinnen und Nutzern berechtigterweise erwartet werden.

Es besteht insoweit auch eine Wechselwirkung zwischen den Produktsicherheits- bzw. Zulassungsstandards und dem Haftungsrecht. Je höher die Anforderungen an die Sicherheit und Zulassung von KI-Systemen sind, desto weniger Haftungsfälle treten einerseits ein. Verbindliche Sicherheitsstandards sind andererseits wesentlich für die Bestimmung der an KI-Systeme berechtigterweise zu stellenden Sicherheitserwartungen, die ihrerseits Maßstab dafür sind, ob ein KI-System fehlerhaft im Sinne der Produkthaftungsrichtlinie ist.

D. Produkthaftungsrichtlinie

I. Produktbegriff (Artikel 2 Produkthaftungsrichtlinie)

Der in Artikel 2 Satz 1 der Produkthaftungsrichtlinie definierte Produktbegriff ist grundsätzlich umfassend angelegt. Die Bundesregierung kann die Überlegungen der Europäischen Kommission zur weiteren Präzisierung des Produktbegriffs nachvollziehen, hält es dabei aber für entscheidend, dass Software – durch eine Klarstellung in der Produkthaftungsrichtlinie – unabhängig von einer Verbindung mit verkörperten Gegenständen als Produkt im Sinne der Richtlinie qualifiziert werden kann. Auch erscheint es richtig, dass Hersteller von fehlerhaften Produkten für die durch diese verursachten Schäden einzustehen haben, ohne dass es darauf ankommt, ob das konkrete Produkt verkörpert ist.

Selbst wenn durch die Integration von Software die bisher weitgehend klaren Grenzen zwischen „Produkt“ und „Dienstleistung“ verschwimmen könnten, sollte demgegenüber klar sein, dass das Regelungssystem der Produkthaftungsrichtlinie auch weiterhin nur für Produkte, nicht aber für Dienstleistungen gilt.

II. Begriff des Inverkehrbringens (Artikel 6 Absatz 1 Buchstabe c und Absatz 2, Artikel 7 Buchstabe b und e Produkthaftungsrichtlinie)

Aus Sicht der Bundesregierung ist zunächst darauf hinzuweisen, dass etwaige Rechtsänderungen im Haftungsrecht mit Blick auf selbstlernende KI-Systeme erst dann vorgenommen werden sollten, wenn die Marktreife und die technische Ausgestaltung absehbar sind, damit sich das Haftungsrecht zum Zeitpunkt der Markteinführung entsprechender Produkte nicht als ungenügend oder unpassend erweist. Dieser Zeitpunkt ist aus Sicht der Bundesregierung bei selbstlernenden KI-Systemen derzeit noch nicht erreicht.

Vor dem Hintergrund, dass Produkte, die mit KI ausgestattet sind, ihre Eigenschaften durch sog. Selbstlerneigenschaften künftig unter Umständen während ihres typischen Produktlebenszyklus selbstständig verändern könnten und Produkte ihre Eigenschaften schon heute auch nach ihrem Inverkehrbringen durch Softwareaktualisierungen verändern, unterstützt die Bundesregierung die Erwägung der Europäische Kommission, den Begriff des „Inverkehrbringens“ zu überprüfen und gegebenenfalls einen Vorschlag zur Anpassung dieses Begriffs an die heutigen Gegebenheiten zu unterbreiten. Es sollte in diesem Zusammenhang aber auch diskutiert werden, inwieweit bereits bei der Inverkehrgabe ein Produktfehler vorliegt, wenn sich ein Produkt, das mit KI ausgestattet ist, durch Selbstlerneigenschaften so verändern kann, dass es andere Aktionen ausführt, als vom Hersteller ursprünglich beabsichtigt und vom Nutzer folglich berechtigterweise erwartet wurde.

Schließlich sollte es Ziel jeder Rechtsänderung sein, die berechtigten Interessen von potentiell Geschädigten und Herstellern zu einem angemessenen Ausgleich zu bringen. Um einen angemessenen Ausgleich der berechtigten Interessen von potentiell Geschädigten und Herstellern zu gewährleisten, wird auch mit einzubeziehen sein, inwiefern etwa der Hersteller funktionserhaltende Sicherheitsaktualisierungen bereitgestellt, den Geschädigten hiervon in Kenntnis gesetzt hat und Geschädigte in Folge dessen selbst Obliegenheiten treffen können.

III. Modifikationen der Beweislast (Artikel 4 Produkthaftungsrichtlinie)

Die bestehende Beweislastverteilung in Artikel 4 der Produkthaftungsrichtlinie kann aus Sicht der Bundesregierung auch im Hinblick auf KI-Systeme grundsätzlich zu angemessenen Lösungen führen.

Die Bundesregierung weist in diesem Zusammenhang darauf hin, dass grundsätzlich in die bestehende materielle Beweislastverteilung nur eingegriffen werden sollte, wenn praktische Beweisschwierigkeiten klar hervorgetreten sind. Sollten mit Blick auf die im Bericht genannten neuen Technologien hierfür Anzeichen bestehen, müsste dies zunächst näher empirisch untersucht werden. Sollten sich diese Anzeichen nicht bestätigen, bestehen Zweifel an der Erforderlichkeit entsprechender Anpassungen.

Sollte sich die Europäische Kommission für eine Modifikation der Beweislastverteilung im Sinne des Vorschlags der New Technologies Formation (NTF) der Expert Group on Liability and New Technologies aussprechen, muss zunächst darauf hingewiesen werden, dass die Bestimmung des Maßstabs der berechtigten Sicherheitserwartungen eine Rechtsfrage ist, welche die Parteien nach deutschem Beweisrecht ohnehin nicht zu beweisen haben. Was die Einhaltung des Maßstabs der berechtigten Sicherheitserwartung angeht, könnte eine Beweislastumkehr im Fall eines non liquet problematisch sein, da nun der Hersteller haften müsste, ohne dass der Haftungsgrund – die Fehlerhaftigkeit des Produkts – überhaupt feststeht. Die Anknüpfung einer Beweislastverteilung an die Schwierigkeiten oder die Kosten einer Beweiserbringung wären eine Neuerung, die mit der Dogmatik des Beweisrechts nicht im Einklang steht. Schließlich kann auch in analogen Fällen die Beweisführung aus rechtlichen oder tatsächlichen Gründen schwierig sein. Hier helfen bei komplexen Sachverhalten von den Gerichten beauftragte Sachverständige. Diese Mechanismen stehen aufgrund der Opazität mancher digitaler Systeme jedoch vor neuen Herausforderungen.

E. Weitere Harmonisierung des nationalen Haftungsrechts

Die Bundesregierung teilt den wichtigen Grundsatz, dass Opfer von Unfällen, an denen neue digitale Technologien beteiligt sind, keinen geringeren haftungsrechtlichen Schutz genießen dürfen, als Opfer von Unfällen aufgrund vergleichbarer herkömmlicher Technologien. Dieses Ziel verfolgen die Haftungsrechte der Mitgliedstaaten allerdings schon heute. Aus Sicht der Bundesregierung muss auch darauf geachtet werden, dass Kompetenzfragen bei harmonisierenden Eingriffen in das eigenständige nationale Haftungsrecht nicht außer Acht gelassen werden. Ebenso ist zu berücksichtigen, dass entsprechende Eingriffe die Kohärenz der nationalen Haftungsrechte stören können.

I. Einführung einer Gefährdungshaftung für die Betreiber von „KI-Anwendungen mit einem spezifischen Risikoprofil“

Die Einführung einer Betreiberhaftung für gefährliche Gegenstände ist aus Sicht der Bundesregierung zunächst ein nachvollziehbarer Gedanke. Eine solche sieht das deutsche Recht bereits heute für bestimmte Gegenstände vor, etwa in § 7 Abs. 1 StVG – auch bei Kraftfahr-

zeugen mit automatisierter oder autonomer Fahrfunktion – oder in § 33 Abs. 1 LuftVG – beispielsweise für Drohnen – vor. Für durch Drohnen verübte Drittschäden finden sich zudem auch entsprechende völkervertragsrechtliche Regelungen, denen einige Mitgliedstaaten beigetreten sind.

Eine Gefährdungshaftung des Betreibers sollte aber grundsätzlich nur dann in Betracht gezogen werden, wenn von dem jeweiligen Gegenstand eine besondere Gefahr ausgeht, keine ausreichende Herstellerhaftung besteht und mit dem Gegenstand typischerweise Personen in Berührung kommen, die sich der Gefahr des Gegenstands unfreiwillig ausgesetzt haben. Die Gefährlichkeit eines Gegenstands wird aber auch künftig grundsätzlich von seiner Art (z.B. einem Kraftfahrzeug) abhängen. Aus diesem Grund besteht seitens der Bundesregierung Zurückhaltung gegenüber einer horizontalen Rechtsharmonisierung, die nicht den entsprechenden gefährlichen Gegenstand selbst in den Blick nimmt, sondern die Art seines Betriebs. Würde entsprechend vorgegangen werden, bestünde zudem die Gefahr, dass für denselben Gegenstand – z.B. herkömmliche und autonome Kraftfahrzeuge – auf Jahrzehnte hin unterschiedliche Haftungsregelungen Anwendung fänden.

Daneben erscheint auch die Binnenmarktförderung durch eine unionsweit einheitliche Gefährdungshaftung des Betreibers – anders als bei der durch die Produkthaftungsrichtlinie harmonisierten Produkthaftung des Herstellers – zweifelhaft. Weiterhin dürfte eine innovationshemmende Fragmentierung des Binnenmarkts durch eine Fortentwicklung des nationalen Betreiberhaftungsrechts nicht drohen, da diese Fragmentierung die traditionellen Technologien schon heute betrifft und entsprechend gewichtige Innovationshemmnisse dort bislang nicht bekannt geworden sind.

II. Modifikation der Beweislastverteilung für die Betreiber von „allen anderen KI-Anwendungen“

Aus Sicht der Bundesregierung sollten Fragen der Beweislast im nationalen Betreiberhaftungsrecht grundsätzlich auch weiterhin der Kompetenz des nationalen Gesetzgebers überlassen bleiben. Die Beweislast ist nach deutschem Rechtsverständnis mit dem jeweiligen Haftungsanspruch verknüpft, so dass eine Harmonisierung allein der materiellen Beweislast zu Inkohärenzen führen dürfte.

F. Zusammenfassende Bewertung zu Sicherheit und Haftung

Da Produkte heute meist in den Anwendungsbereich mehrerer Produktsicherheitsvorschriften fallen, ist es essenziell, einheitliche Anforderungen zu definieren, die sowohl an KI-Anwendungen gerichtet sind, als auch an Cybersicherheit für alle vernetzbaren Produkte (Hardware und Software).

Diese einheitlichen Anforderungen sollten für den Bereich der Produktsicherheit bevorzugt in einem horizontalen Rechtsakt mit der Möglichkeit sektorspezifischer Ausnahmen festgelegt sein. Damit würden abweichende Regelungen in den grundlegenden Rechtsvorschriften vermieden. Sektorspezifische Konkretisierungen können z.B. für den Gesundheitsbereich erforderlich werden, um den besonderen Anforderungen des Gesundheitswesens (v.a. in Bezug auf personenbezogene Daten) gerecht zu werden. Diese Anforderungen könnten dann in Einklang mit dem bestehenden Binnenmarktkonzept durch harmonisierte Normen untersetzt werden.

Insgesamt sprechen wir uns für den Bereich Sicherheit dafür aus, dass eine differenzierte Risikoklassifizierung essenzielle Voraussetzung dafür ist, Zulassung und Kontrolle dort, wo sie risikoadäquat sind, effektiv umzusetzen.

Die Merkmale von KI, IoT und Robotik sollten zwischen personenbezogener und nicht-personenbezogener Anwendung unterscheiden und um die Merkmale Fairness/Diskriminierungsfreiheit und Datenschutz erweitert werden. Weiterhin werden ergänzende übergreifende Merkmale wie Nachhaltigkeit, Zuverlässigkeit und Impact (Systemrelevanz) vorgeschlagen.

In der konkreten Ausgestaltung einer künftigen Governance von KI-Anwendungen können auch die Vorschläge weiterer Expertinnen und Experten in die Diskussion miteinbezogen werden.

Das zivile Haftungsrecht kann schon heute Schäden, die durch KI, IoT und Robotik verursacht werden, grundsätzlich angemessen bewältigen. Stellen sich durch diese Technologien neue rechtliche Herausforderungen, müssen allerdings Modifikationen geprüft werden, um auf die zunehmende Konnektivität und Komplexität digitaler Systeme rechtlich sachgerecht zu reagieren. Eine punktuelle Überarbeitung der Produkthaftungsrichtlinie erscheint insofern sachgerecht. Eine Harmonisierung der nationalen Haftungsrechte ist hingegen derzeit nicht erforderlich: Wie in vielen MS so ist auch das deutsche Haftungsrecht hoch entwickelt und gewährt dem Geschädigten einen umfassenden Schutz auch dann, wenn der schadensursächliche gefährliche Gegenstand digital betrieben wird. Ein unionsrechtliches Eingreifen könnte hingegen zu Inkohärenzen mit dem nicht harmonisierten mitgliedstaatlichen Recht führen, die es zu vermeiden gilt.