Stellungnahme zum Abschlussbericht der DEK

Bitkom Stellungnahme zum Gutachten und den Empfehlungen der Datenethikkommission

02. April 2020

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Rebekka Weiß, LL.M.
Leiterin Vertrauen & Sicherheit
T +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

I. Zusammenfassung und Gesamteinschätzung

Am 23. Oktober 2019 legte die Datenethikkommission (DEK) der Bundesregierung Ihr Gutachten mit 75 Handlungsempfehlungen zum Umgang mit Daten und algorithmischen Systeme vor. Das Gutachten ist ein wichtiger Beitrag zur gesellschaftlichen Debatte über ethische Fragen im Umgang mit Daten und der Automatisierung von Prozessen und Entscheidungen mit Hilfe von Algorithmen. Die Frage, wie wir unseren Wertekanon in der digitalen Gesellschaft erhalten und zur Geltung bringen, bedarf eines vertieften gesellschaftlichen Dialogs, der durch die Arbeit der DEK vorangebracht wird.

Das Gutachten enthält viele richtige Empfehlungen und bedenkenswerte Impulse - insbesondere in Bezug auf den Umgang mit Daten. Sehr bedenklich ist jedoch die Einschätzung, zur Datenverarbeitung eingesetzte Algorithmen, also die Technik selbst, seien generell riskant und daher in der Breite regulierungsbedürftig. Zwar verfolgt das Gutachten einen risikobasierten Ansatz. Dieser wird jedoch so definiert, dass letztlich nicht zum Tragen kommt, was das Gutachten eigentlich selbst ausführt: nämlich, dass es maßgeblich davon abhängt, wo und wie Algorithmen zur Automatisierung von Prozessen und Entscheidungen eingesetzt werden und ob sich daraus überhaupt Risiken und mögliche Beeinträchtigungen ergeben können. Es wäre aus unserer Sicht wichtig gewesen, klarer zu betonen, dass Algorithmen und damit auch Anwendungen der Künstlichen Intelligenz nicht per se gefährlich oder risikobehaftet sind. Vertrauen in digitale Anwendungen und den Ausbau des Standortes Deutschland schaffen wir nicht, wenn selbst dem Algorithmus in einem Getränkeautomaten ein Schädigungspotenzial zugewiesen wird.

Eine allgemeine Regulierung auf dieser Basis führt zu Überregulierung und der Schaffung von Bürokratie, die niemandem nützt, aber die Ziele der KI-Strategie der Bundesregierung, die Entwicklung und den Einsatz von KI hierzulande zu fördern, konterkarieren könnte.

Die Chancen des KI-Einsatzes kommen im Gutachten durch Die Risikofokussierung und die entsprechende Regulierung zu kurz. Das ist angesichts der ohnehin schon mehrheitlich angstgetriebenen Debatte um Künstliche Intelligenz in Deutschland nicht zielführend. Es wäre für die weitere gesellschaftliche Debatte hilfreich und wichtig gewesen, mit aussagekräftigen Beispielen und Erklärungen das Thema in jede Richtung zu beleuchten und aufzuzeigen, dass mit KI in vielen Bereichen erhebliche Verbesserungen der Ist-Situation erzielt werden können.

II. Empfehlungen der DEK – Analyse und Bewertung

1. Einleitende Bitkom Einschätzung zu den Empfehlungen der DEK bezüglich Daten & Datennutzung

Im Folgenden Abschnitt finden sich Anmerkungen sowie Vorschläge hinsichtlich der einzelnen Empfehlungen der DEK. Aus unserer Sicht muss an die Arbeiten der DEK angeknüpft und der angestoßene Diskurs fortgesetzt werden. Viele Fragen wirft der Bericht auf ohne sie abschließend beantworten zu können. Hieran sollte nun angeknüpft werden, eine saubere Tatsachengrundlage und evidenzgestützte Aussagen abgeleitet werden. Die aus unserer Sicht offenen Fragen finden sich jeweils auch in den Bitkom Einschätzungen zu den einzelnen Forderungen. Vorab sollen an dieser Stelle eine grundsätzliche Bewertung und Einordnung erfolgen.

Die Empfehlungen 1 bis 35 des Abschlussgutachtens der DEK sind dem Themenkreis Daten, Datennutzung und Datenwirtschaft gewidmet. Wir begrüßen ausdrücklich, dass die DEK die Idee des Dateneigentums ablehnt und sich für bessere Nutzbarmachung von Daten über Open Data Initiativen ausspricht. Aus unserer Sicht wäre es für den gesamten Abschnitt sinnvoll gewesen, genau zu definieren, welche Datenkategorien die Empfehlungen jeweils erfassen sollen.

Bei der Debatte über einen Datenzugang begrüßen wir das Anliegen einer möglichst breiten Beteiligung an vorhandenen Daten, etwa bei Open Data Initiativen. Eine allgemeine Verpflichtung für Unternehmen, eigene Daten allgemein zur Verfügung stellen zu müssen, lehnen wir ebenso wie die Datenethikkommission ab. Die bisherigen Diskussionen um ein Datenzugangsrecht und die derzeitige regulatorische Lage mit der angestoßenen 10. GWB-Novelle zeigen, dass Datenzugangsregeln nur sehr punktuell greifen können und dürfen, um Innovationskraft, Datenschutz sowie Vertragsfreiheit und Marktentwicklungschancen in Einklang zu bringen. Ein Datenzugang sollte grundsätzlich auf dem Prinzip der Vertragsfreiheit und damit der Freiwilligkeit beruhen.

Wo die DEK aber eine weitergehende Regulierung im Bereich des Datenschutzes und der nicht-personenbezogenen Daten vorschlägt, ist aus unserer Sicht Zurückhaltung geboten. Die aktuellen Zahlen hinsichtlich der Umsetzung der DS-GVO zeigen, dass 95% der Unternehmen bereits die bisherigen Vorgaben nicht für 100%ig umsetzbar halten.[1] Dies hat auch bereits einen Vertrauensverlust sowohl bei Unternehmen als auch bei Verbrauchern bewirkt und zeigt den Bedarf bei Regulierungsvorhaben, das Augenmaß nicht zu verlieren und auf Praktikabilität zu achten.

Insbesondere bei neuen gesetzlichen Vorgaben zur Datennutzung sollte ein Aspekt nicht aus dem Blick geraten: Digitalisierung bedeutet, viele Vorgänge des alltäglichen Geschäfts- und Privatlebens in Daten abzubilden und durch die Verarbeitung dieser Daten abzuwickeln. Die Frage, ob und wie Daten verarbeitet werden dürfen oder nicht, ist daher entscheidend für Erfolg und Ausgestaltung der Digitalisierung. Die Herausforderung liegt darin, Regeln für die Datenverarbeitung so aufzustellen, dass einerseits das Recht des Einzelnen auf Datenschutz wirksam gewahrt wird und zum anderen nützliche und innovative Anwendungen entwickelt und umgesetzt werden können. Es gibt in Teilen der Bevölkerung Bedenken, ob das Recht auf Privatsphäre und Schutz der eigenen Daten in der digitalisierten Gesellschaft erhalten werden kann. Angst vor dem Verlust von Privatsphäre und selbstbestimmtem Handeln steht der positiven Rezeption und Akzeptanz neuer Technologien im Wege. Gleichzeitig besteht aufgrund dieser Bedenken die Gefahr einer Überregulierung sich gerade erst entwickelnder Technologien und Geschäftsfelder. Das kann zu einem Hindernis für die Ausschöpfung der Chancen durch die Digitalisierung werden und den wirtschaftlichen Erfolg am Standort Deutschland gefährden. Befürchtungen eines Kontrollverlusts sind zum Teil bedingt durch die Data Breaches oder andere Datenpannen. Hier gilt es durch Transparenz der Nutzung von Daten durch die Unternehmen und die umgesetzten Sicherungsmaßnahmen mehr Akzeptanz zu schaffen – und den gesetzten regulatorischen Rahmen auch umzusetzen bzw. die Durchsetzung zu verbessern. Eine verbesserte Ausstattung der Datenschutzaufsichtsbehörden könnte hier helfen – auch um die Beratung von Unternehmen sicherzustellen und so für mehr Vertrauen, Akzeptanz und Rechtssicherheit zu sorgen.

[1] https://www.bitkom.org/Presse/Presseinformation/Zwei-Drittel-der-Unternehmen-haben-DS-GVO-groesstenteils-umgesetzt und Studie durch Bitkom Research hier: https://www.bitkom.org/sites/default/files/2019-09/bitkom-charts-pk-privacy-17-09-2019.pdf.

Empfehlung 1:
Die DEK empfiehlt Maßnahmen gegen ethisch nichtvertretbare Datennutzungen. Dazu gehören etwa Totalüberwachung, die Integrität der Persönlichkeit verletzende Profilbildung, gezielte Ausnutzung von Vulnerabilitäten, sog. Addictive Designs und Dark Patterns, dem Demokratieprinzip zuwiderlaufende Beeinflussung politischer Wahlen, Lock-in und systematische Schädigung von Verbrauchern sowie viele Formen des Handels mit personenbezogenen Daten.

Bitkom Einschätzung:
Wir stimmen in diesem Punkt mit der DEK überein. Diese Empfehlung richtet sich jedoch nach unserem Verständnis vor allem an den Staat. Soweit sich diese Empfehlung an die Wirtschaft richtet, wird sie – nicht zuletzt über eigene Codes of Conducts mit effektiven Durchsetzungsmechanismen und aufsetzend auf den regulatorischen Rahmen– umgesetzt. An einigen Stellen könnte auch darüber nachgedacht werden, bestehende Selbstregulierung in eine Ko-Regulierung zu überführen. Im Übrigen setzt die DS-GVO bereits zwingende auch ethische Vorgaben.

Empfehlung 2:
Sowohl das Datenschutzrecht als auch die übrige Rechtsordnung (u. a. Zivilrecht, Lauterkeitsrecht) enthalten bereits eine Fülle von Instrumenten, die gegen derartige Datennutzungen eingesetzt werden können. Gemessen an Breitenwirkung und Schädigungspotenzial werden diese Instrumente indessen bislang nicht in ausreichender Weise genutzt – insbesondere gegenüber marktmächtigen Unternehmen. Dieses Vollzugsdefizit hat verschiedene Ursachen, die es systematisch anzugehen gilt.

Bitkom Einschätzung:
Werden bei der Datennutzung Marktungleichgewichte festgestellt, die in unakzeptabler Weise durch marktmächtige Unternehmen ausgenutzt werden, sollte der Gesetzgeber vorrangig im Kartellrecht gegensteuern. Dies geschieht auch aktuell mit der 10. GWB-Novelle. Für personenbezogene Daten sind im Übrigen die Vorgaben der DS-GVO zu beachten, die nicht zuletzt auch der Entstehung von neuen Datenmonopolen entgegenwirken. Außerhalb der genannten Rechtsgebiete gibt es bisher noch keine ausreichende Evidenz für konkrete Defizite im geltenden Recht. Aus den Ausführungen der DEK ergeben sich solche Defizite jedenfalls nicht zwingend.

Empfehlung 3:

Neben der Schärfung des Bewusstseins bei handelnden Akteuren (z. B. Aufsichtsbehörden) für die bereits bestehenden Möglichkeiten ist dringend eine Konkretisierung und punktuelle Verschärfung des geltenden Rechtsrahmens angezeigt. Dazu gehören etwa eine spezielle Normierung von datenspezifischen Klauselverboten, Schutz- und Treuepflichten, Deliktstatbeständen und unlauteren Geschäftspraktiken sowie die Schaffung eines weitaus konkreteren Rechtsrahmens für Profilbildungen und Scoring wie auch für den Datenhandel.

Bitkom Einschätzung:

Um eine Verschärfung des geltenden Rechtsrahmens außerhalb des Kartellrechts zu rechtfertigen, reichen die bisherigen Hinweise auf angebliche Marktverzerrungen nicht aus. Sehr kritisch zu bewerten sind Vorschläge zur Verschärfung des geltenden deutschen AGB-Rechts. Schon bisher halten Unternehmen das deutsche AGB-Recht für die Belange der digitalen Wirtschaft für wenig geeignet und weichen daher zunehmend für ihre Vertragsbeziehungen auf ausländische Rechtsordnungen aus. Außerdem sind die Vorgaben der DS-GVO natürlich auch für die Ausgestaltung von Vertragsbeziehungen zwingend zu beachten. Die Fortentwicklung des Vertragsrechts für die Belange der digitalisierten Wirtschaft bedarf einer sorgfältigen und ausgewogenen Analyse. Keinesfalls dürfen über den Umweg des AGB-Rechts allgemeine Datenteilungspflichten für Unternehmen eingeführt werden. Vor der Einführung neuer Regelungen für Scoring und Profilbildung sollte zunächst auch die weitere Fallpraxis auf Basis des geltenden Rechts, insbesondere der DS-GVO abgewartet werden. Zeigen sich hier Lücken bzw. Missbrauchspotentiale sollten weitere Rahmenbedingungen geprüft werden und ggf. in Zusammenarbeit mit den Branchen durch Selbstregulierung adressiert werden. So könnten die sektorspezifischen Besonderheiten adäquate Berücksichtigung finden und eine frühzeitige Reaktion des Marktes erfolgen, die wiederum Auswirkungen auf die weiteren Anbieter hätte (race to the top). CoCs sind aus unserer Sicht auch hier ein probates Mittel. Die genannten Anreize sollten für diejenigen geschaffen werden, die sich freiwillig branchenspezifischer Datenteilung unterwerfen. Grds. sollte man bei CoCs aber auch beachten, dass diese kein reiner „Papiertiger“ sein dürfen, insb. wenn signifikante Anreize (Rechtsfolgen und Vorteile) aus der Einhaltung resultieren. Andernfalls besteht Missbrauchspotential.

Empfehlung 4:

Um die Wirkungskraft der Aufsichtsbehörden zu erhöhen, bedürfen diese einer weitaus besseren personellen und sachlichen Ausstattung. Sofern es nicht gelingt, die Abstimmung unter den deutschen Datenschutzaufsichtsbehörden zu verstärken und zu formalisieren und so die einheitliche und kohärente Anwendung des Datenschutzrechts zu gewährleisten, ist eine Zentralisierung der Datenschutzaufsicht für den Markt in einer – mit einem weiten Mandat

ausgestatteten und eng mit anderen Fachaufsichtsbehörden kooperierenden – Behörde auf Bundesebene zu erwägen. Die Zuständigkeit der Landesdatenschutzbehörden für den öffentlichen Bereich soll hingegen unangetastet bleiben.

Bitkom Einschätzung:

Die bessere Ausstattung der Aufsicht begrüßen wir. Die personelle Aufstockung sollte zugleich auch für mehr individuelle Beratung und Unterstützung der Verantwortlichen genutzt werden. Eine möglichst einheitliche, kohärente Anwendung und Interpretation der Vorschriften unterstützen wir ausdrücklich und nachdrücklich. Dies muss auch auf europäischer Ebene gelten, was eine konsequente Anwendung und Nutzung des Kohärenzmechanismus bedeuten muss. Parallelrechte bzw. Aufsichtsstrukturen sind im Sinne dieser Kohärenz zu vermeiden und die jeweiligen Zuständigkeiten klar voneinander abzugrenzen.

Empfehlung 5:

Die Anerkennung von „Dateneigentum" im Sinne eines dem Sacheigentum oder dem geistigen Eigentum nachgebildeten Ausschließlichkeitsrechts an Daten würde nach Auffassung der DEK bestehende Probleme nicht lösen und stattdessen eine Reihe neuer Probleme schaffen. Sie wird daher nicht empfohlen. Die DEK empfiehlt auch nicht die Anerkennung genereller wirtschaftlicher Verwertungsrechte an personenbezogenen Daten, wie sie etwa durch Verwertungsgesellschaften geltend gemacht werden könnten.

Bitkom Einschätzung:

Die in dieser Empfehlung geäußerten Ansichten zu „Dateneigentum" und wirtschaftlicher Verwertung personenbezogener Daten werden von Bitkom geteilt und unterstützt.[2]

Empfehlung 6:

Wenngleich die plakative Bezeichnung zur allgemeinen Bewusstseinsbildung beigetragen hat, plädiert die DEK dafür, von der Bezeichnung von Daten als „Gegenleistung" abzusehen. Unabhängig von der künftigen Auslegung des sog. Koppelungsverbots durch die Aufsichtsbehörden und den EuGH fordert die DEK, dass Verbrauchern jeweils zumutbare Alternativen gegenüber der Freigabe von Daten zur auch kommerziellen Nutzung angeboten werden müssen (z. B. entsprechend ausgestaltete Bezahlmodelle).

[2] Siehe hierzu im Detail die Bitkom-Position zu Rechten an Daten: https://www.bitkom.org/Bitkom/Publikationen/Rechtsfragen-digitalisierten-Wirtschaft-Rechte-Daten

Bitkom Einschätzung:

Personenbezogene Daten sind schon aufgrund der Vorgaben durch die DS-GVO kein allgemein marktgängiges Wirtschaftsgut. Auch zivilrechtliche Regelungen zur Erfassung von Daten als Gegenleistung sehen wir kritisch – die derzeitigen Umsetzungsarbeiten zur Richtlinie über digitale Inhalte und der darin enthaltene Vorschlag zur Regelung von Daten als Gegenleistung im Zivilrecht zeigen, welche Spannungsfelder sich zum Teil zwischen Datenschutzrecht und Zivilrecht bilden und wie viele Geschäftsmodelle hiervon betroffen sind. Ein alternatives verpflichtendes Bezahlmodell stellt aus unserer Sicht einen unverhältnismäßigen Eingriff in die unternehmerische Freiheit dar, die jedenfalls alle werbebasierten Geschäftsmodelle im Internet empfindlich trifft. Unternehmen ein bestimmtes Geschäftsmodell vorzuschreiben, bedarf einer besonderen Rechtfertigung, die hier nicht gegeben ist. Ein verpflichtendes Bezahlmodell vorzuschreiben stellt weder ein legitimes Mittel dar, noch ist es erforderlich oder angemessen. Zudem suggeriert sie dem Nutzer/Verbraucher fälschlicherweise, dass die Dienste “ohne Werbung” dieselbe Funktionalität und dieselbe User-Experience haben. Schließlich führt die Durchsetzung zu weiteren staatlichen Eingriffen, da auch die Preisgestaltung nach Ansicht der DEK staatlichen Vorgaben folgen müsste.

Die DS-GVO hat einen klaren Rahmen hinsichtlich entsprechender Rechtsgrundlagen für Datenverarbeitungen und Einwilligungen geschaffen. Vor welchem Hintergrund den Anbietern eine Pflicht aufzuerlegen sei, hier ihre Modelle zweigeteilt anzubieten ist für uns nicht ersichtlich. Zudem betrifft die Zweiteilung auch eine noch nicht ausreichend untersuchte gesellschaftspolitische Dimension: kostenpflichtige (aber datensparsamere) Geschäftsmodelle können sich ggf. nicht alle Bürger leisten, was zu einer Aufspaltung der Nutzergruppen der jeweiligen Modelle führen wird.

Empfehlung 8:

Die DEK empfiehlt der Bundesregierung, Fragen rund um den „digitalen Nachlass“ mit dem Urteil des BGH von 2018 nicht als erledigt anzusehen. Die praktisch lückenlose Aufzeichnung von digital geführter Kommunikation, die in vielen Fällen an die Stelle des flüchtig gesprochenen Wortes tritt, und ihre Aushändigung an Erben bedeutet eine neue Dimension von Gefährdung für die Privatheit. Ihr sollte mit einer Reihe von Maßnahmen begegnet werden, welche neue Pflichten von Diensteanbietern, Qualitätssicherung bei Angeboten digitaler Nachlassplanung sowie nationale Regelungen zum postmortalen Datenschutz umfassen.

Bitkom Einschätzung:

Bitkom beteiligt sich aktiv an der Kommunikation und Aufklärung der Bevölkerung rund um das Thema „Digitales Erbe".[3] Aus unserer Sicht darf jedoch die Verantwortung für einen ethisch-verantwortungsvollen Umgang mit dem digitalen Nachlass ihrer Kunden nicht allein bei den Anbietern abgeladen werden. Jedenfalls muss der Gesetzgeber den Anbietern klare Richtlinien an die Hand geben, in welchen Fällen höchstpersönliche Informationen eines Verstorbenen gelöscht werden sollen, und in welchen Fällen Hinterbliebene Zugang zu den Informationen erhalten sollen. Überlegenswert wäre ggf. die Einführung eines „Erbscheins für digitale Belange". Jedenfalls muss den Erben die Möglichkeit bleiben, auf sie übergehende Vermögenspositionen geltend machen zu können, auch wenn dazu z.B. persönliche Passwörter oder sonstige besondere Kennzeichen des Verstorbenen notwendig sind.

Empfehlung 9:

Die DEK empfiehlt der Bundesregierung, die Sozialpartner einzuladen, ausgehend von den bereits in Tarifverträgen bestehenden Beispielen guter Übung eine gemeinsame Linie für gesetzliche Konkretisierungen des Beschäftigtendatenschutzes zu entwickeln. Dabei sollten auch die Belange von Personen in unüblichen Beschäftigungsformen berücksichtigt werden.

Bitkom Einschätzung:

Der Rahmen der DS-GVO reicht bereits aus, um den Beschäftigtendatenschutz zu regeln. Darüber sind auch bereits schon die Personen in „unüblichen Beschäftigungsformen" erfasst.

Die Datenschutzverordnung sieht in Artikel 88 für den Beschäftigtendatenschutz ausdrücklich eine Öffnungsklausel für eine nationale Regelung sowie Kollektivvereinbarungen vor. Der Bundestag hat Ende April 2017 bei der Reform des deutschen Bundesdatenschutzgesetzes im § 26 auch eine Neuregelung des Beschäftigtendatenschutzes verabschiedet. Eine solche, über die DS-GVO hinausgehende, spezielle Regelung des Beschäftigtendatenschutzes braucht es aus Sicht des Bitkom nicht. Denn die Regeln der DS-GVO schützen alle Betroffenen innerhalb und außerhalb eines Arbeitsverhältnisses. D.h. die allgemeinen Prinzipien des Datenschutzes finden Anwendung und schützen die Arbeitnehmer hinreichend. Zudem stehen der betrieblichen Mitbestimmung in diesem Bereich

[3] Siehe z.B. https://www.bitkom.org/Presse/Presseinformation/Die-wenigsten-regeln-ihren-digitalen-Nachlass.html

https://www.bitkom.org/Presse/Presseinformation/Bitkom-zum-BGH-Urteil-ueber-digitales-Erbe.html

https://www.bitkom.org/Presse/Presseinformation/Neun-von-zehn-Internetnutzern-haben-ihren-digitalen-Nachlass-nicht-geregelt.html

weitgehende Rechte zu, sodass Arbeitnehmer hierdurch einen zusätzlichen Schutz erhalten.

Durch die Digitalisierung der Wirtschafts- und Produktionsprozesse fallen viel mehr Daten an, als es früher der Fall war. Diese dienen jedoch – falls sie überhaupt einen Personenbezug aufweisen – der Steuerung und Optimierung von Maschinen und Prozessen. Regelungen für den Arbeitnehmerdatenschutz dürfen den Möglichkeiten der Industrie 4.0 und auch den Vorteilen, die moderne IT-Lösungen für Arbeitnehmer bieten (z.B. im Rahmen der mobilen Arbeit) nicht zuwiderlaufen.

Empfehlung 11:

Die DEK fordert, dem erheblichen Vollzugsdefizit des geltenden Rechts betreffend den Schutz von Kindern und Jugendlichen im digitalen Raum abzuhelfen. Insbesondere sollten Technologien – einschließlich eines effektiven Identitätenmanagements – sowie Standardoptionen entwickelt und verpflichtend vorgesehen werden, welche einen zuverlässigen Schutz der Kinder und Jugendlichen gewährleisten und zugleich familienadäquat sind, indem sie Erziehungsberechtigte weder überfordern noch eine übermäßige Überwachung im privaten Bereich ermöglichen oder gar hierzu animieren.

Bitkom Einschätzung:

Bitkom unterstützt ausdrücklich das Ziel der Bundesregierung, Kinder und Jugendliche vor schädlichen Online-Inhalten zu schützen, sowie ihnen einen altersgerechten Zugang zu digitalen Diensten zu ermöglichen.[4] Wir halten es für erforderlich, zunächst die Rechtsdurchsetzung zu verbessern bevor neue Regulierung für gleiche Situationen bzw. Gegebenheiten geschaffen wird. Es sollten außerdem Technologien für den Jugendschutz entwickelt und eingesetzt werden. Gerade Jugendschutzprogramme stellen einen wichtigen Teil des Jugendschutzportfolios dar, den Eltern einsetzen können. Mit der Verwendung dieser Programme sollte dann aber auch eine rechtssichere Privilegierung einhergehen (die im Fall des Jugendschutzprogramms JusProg nachträglich angegriffen wurde durch die Entscheidung der KJM). Ein verpflichtender Einsatz von Technologien kann dazu führen, dass der Anreiz auf Seiten der Unternehmen, jene zu entwickeln, ausbleibt – dieser müsste aber im Gegenteil verstärkt werden. Die Anforderungen an diese Technologien dürfen nicht zu hoch gesteckt sein sondern müssen zur Entwicklung von praktikablen Lösungen beitragen - die aktuelle Medienrealität, insbesondere die Vielfalt der Plattformen, Geräte und Betriebssysteme muss hier berücksichtigt werden.

[4] Siehe hierzu auch die aktuelle Bitkom Stellungnahme zum Jugendschutzgesetz: https://www.bitkom.org/Bitkom/Publikationen/Stellungnahme-zweites-Gesetz-zur-Aenderung-des-Jugendschutzgesetzes

Empfehlung 13:
Die DEK empfiehlt, eine Reihe verbindlicher Vorgaben für datenschutzfreundliches Design von Produkten und Dienstleistungen einzuführen und damit die an Verantwortliche im Sinne der DSGVO gerichteten Vorgaben von Datenschutz „by design" und „by default" bereits auf der Ebene der Hersteller wie auch der Diensteanbieter wirksam werden zu lassen. Dies betrifft insbesondere Vorgaben für Verbraucherendgeräte. In diesem Zusammenhang sind auch einheitliche Bildsymbole (Piktogramme) einzuführen, die dem Verbraucher eine informierte Kaufentscheidung ermöglichen.

Bitkom Einschätzung:
Über Art. 40ff DS-GVO lässt sich hinsichtlich einer Erweiterung auf Hersteller argumentieren, dass Hersteller sich bisher nicht bestimmten Branchenspezifika gegenüber „labeln" lassen können. Man könnte ggf. daher über ein *quid pro quo* nachdenken: Ist der Hersteller entsprechend eingestuft, ist der Nutzer ist prima facie safe. Auch eine inhaltliche Dopplung wäre möglich: Eine Branche gibt sich entwickelt und erlegt sich einen CoC auf. Die Hersteller lassen sich dann unabhängig und/oder entsprechend des COC prüfen. Für letzteres Modell müsste aber auch eine Änderung des Rechtsrahmens bewirkt werden, da zur Zeit keine Anreize für Verwendung derartiger Software bisher in der DS-GVO niedergelegt sind.

Bezüglich der Einführung der Piktogramme begrüßen wir die explizite Erwähnung im Abschlussgutachten. Die DS-GVO sieht in Art. 12 Abs. 7 vor, dass sich die verantwortliche Stelle zur Erfüllung ihrer Informationspflichten nach Art. 13 und 14 auch bestimmter Bildsymbole bedienen kann, die der betroffenen Person in Kombination mit den erforderlichen (textlichen) Informationen bereitgestellt werden. Dadurch soll der betroffenen Person in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form ein aussagekräftiger Überblick über die beabsichtigte Verarbeitung vermittelt werden.
Die bisher entwickelten Konzepte haben nicht überzeugt. Dennoch erscheint der Ansatz – insbesondere vor dem Hintergrund von Datenverarbeitungen durch Geräte mit sehr kleinen oder gar ohne Displays – sinnvoll und notwendig. Um in der Praxis nicht umsetzbaren oder überschießenden Vorschlägen der Kommission frühzeitig entgegen zu wirken, hat eine Arbeitsgruppe im Bitkom bereits proaktiv eine Umsetzung erarbeitet und bringt sich aktiv in die Weiterentwicklung ein. Bitkom fordert daher, dass die Kommission von der in Art. 12 Abs. 8 DS-GVO angelegten Möglichkeit eines delegierten Rechtsaktes Gebrauch macht. Hierüber kann die Kommission festlegen, welche Informationen durch Bildsymbole darzustellen sind und welche Verfahren dabei Anwendung finden. Wir verstehen Icons dabei stets als sinnvolle Maßnahme zur Transparenzförderung bei Onlinediensten und für Datenverarbeitungsprozesse. Für Verbraucherendgeräte sehen wir eine verpflichtende

Nutzung kritisch, da der Diversität der Geräte kaum durch einheitliche Symbole Rechnung getragen werden kann. Hier wären andere Maßnahmen zu finden, die eine „informierte Kaufentscheidung“ ermöglichen. Für beide Fälle ist in jedem Fall relevant, dass es sich um eine “Kann-Vorschrift” handelt und nicht um eine gesetzliche Pflicht. Daneben ist vor allem der Prozess zur Erarbeitung solcher Icons wichtig.

Empfehlung 15:
Trotz des berechtigten Fokus auf Datenschutz natürlicher Personen darf der Schutzbedarf von Unternehmen und juristischen Personen nicht in den Hintergrund treten. Durch die umfassende Verknüpfbarkeit von Einzeldaten kann ein lückenloses Bild interner Betriebsabläufe entstehen und in die Hände von Konkurrenten, Verhandlungspartnern, Übernahmeinteressenten usw. gelangen. Dies stellt aufgrund umfangreicher Datenflüsse in Drittstaaten u. a. eine Gefährdung der digitalen Souveränität Deutschlands und Europas dar. Viele Handlungsempfehlungen sind daher sinngemäß auch auf die Daten juristischer Personen zu übertragen. Die DEK fordert die Bundesregierung auf, Schritte zu unternehmen, um den datenbezogenen Schutz von Unternehmen zu verbessern.

Bitkom Einschätzung:
Aus unserer Sicht stellt sich hier die Frage, ob tatsächlich, insbesondere angesichts der DS-GVO, Regelungsbedarf besteht. Der bestehende Schutzrahmen ist z.B. durch GeschGehG, geistiges Eigentum, Strafrecht, Fernmeldegeheimnis abgesteckt; wenn allerdings Ansprüche gegen den Datenzugang normiert werden, könnten daraus für Unternehmen die beschriebenen Gefahren erwachsen:

- Wie würde sich die Parallele zum Geschäftsgeheimnisschutz auswirken?
- Wie gestaltet sich das Verhältnis zu Open Data und Datenteilungen unter Unternehmen aus freiwilliger Basis?
- In welchem Verhältnis stünden Regelungen zur ePrivacy Verordnung, die ebenfalls Daten juristischer Personen schützen soll?

Empfehlung 16:
Die DEK sieht in einer Datennutzung für gemeinwohlorientierte Forschungszwecke (z. B. zur Verbesserung der Gesundheitsfürsorge) enormes Potenzial, das es zum Wohle des Einzelnen und der Allgemeinheit zu nutzen gilt. Das geltende Datenschutzrecht erkennt dieses Potenzial durch eine Reihe weitreichender Privilegierungen prinzipiell an. Allerdings bestehen auch Unsicherheiten, insbesondere mit Blick auf die Reichweite des sog. Weiterverarbeitungsprivilegs sowie des Forschungsbegriffs im Zusammenhang mit der Entwicklung von Produkten.

Dem muss aus Sicht der DEK durch entsprechende gesetzliche Klarstellungen begegnet werden.

Bitkom Einschätzung:

Der Datenschutzrahmen stellt durch die entstandenen Rechtsunsicherheiten ein Hemmnis für Datenteilung, Datenzugang und Datenerhebung und damit für die angesprochene Datennutzung auch für gemeinwohlorientierte Forschungszwecke dar.[5] Diese Unsicherheiten müssen schnellstmöglich auf europäischer Ebene reduziert werden. Die Klärung offener Fragen im Bereich Anonymisierung und Pseudonymisierung wird insbesondere für die Datenbereitstellung und die bessere Nutzbarmachung von Gesundheitsdaten maßgeblich sein. Nutzung von pseudonymisierten und anonymisierten Daten wird auch für das Gelingen der KI-Strategie entscheidend sein, sodass die Bundesregierung dies in den Fokus stellen sollte. Auf europäischer Ebene muss die Verbesserung der Datenerhebung und Datennutzung im Gesundheitsbereich und von Gesundheitsdaten gefördert werden. Vor dem Hintergrund, dass der diesjährige DS-GVO Review wohl nicht für tatsächliche Änderungen der Verordnung selbst genutzt werden wird, sollten hier europäische Harmonisierungen durch neue Guidelines oder ggf. sogar neue Regelungen angestoßen werden. Die gesellschaftlichen Mehrwerte, die in Innovationen im Gesundheitswesen erreicht werden könnten, scheitern zur Zeit an der Fragmentierung der europäischen (und teilweise sogar föderalen) Regelungen – gemeinsame Forschungsprojekte, Datenpooling und sogar fördernde Maßnahmen wie anonymisierte Nutzung von Daten sind aktuell nicht oder nur unter so engen Rahmenbedingungen möglich, dass sie nicht erfolgreich skaliert werden können. Die Bundesregierung sollte sich im ersten Schritt hier gemeinsam mit der EU Kommission vor allem dafür einsetzen, dass die bereits in der DS-GVO genannten Auslegungshinweise (insbesondere die ausdrücklich geforderte weite Auslegung des Forschungsbegriffs) auch einheitlich umgesetzt werden.[6]

Empfehlung 17:

Die Zersplitterung der Rechtslage, sowohl innerhalb Deutschlands als auch der EU Mitgliedstaaten untereinander, kann ein Hindernis für datengetriebene Forschung darstellen. Empfohlen wird daher eine Harmonisierung der forschungsspezifischen Regelungen sowohl auf Bundes- und Landesebene als auch der verschiedenen nationalen Regelungen innerhalb der EU. Auch die Einführung eines Notifizierungsverfahrens für mitgliedstaatliche Regelungen

[5] Siehe hierzu auch Bitkom Stellungnahme zu den Eckpunkten der Datenstrategie: https://www.bitkom.org/Bitkom/Publikationen/Stellungnahme-zu-den-Eckpunkten-einer-Datenstrategie-der-Bundesregierung

[6] Zum Thema Forschungsdaten ausführlich Bitkom Position zum DVG: https://www.bitkom.org/Bitkom/Publikationen/Stellungnahme-zum-Entwurf-eines-Gesetzes-fuer-eine-bessere-Versorgung-durch-Digitalisierung-und

zum Forschungsdatenschutz sowie die Einrichtung einer europäischen Clearing-Stelle für grenzüberschreitende Forschungsprojekte könnte eine Erleichterung bringen.

Bitkom Einschätzung:

Wir begrüßen die Initiative zur Harmonisierung des Rechtsrahmens, insbesondere im Bezug zu Gesundheitsdaten und Forschung. Die unterschiedlichen Landesgesetze stellen Anwender und Forschungsstellen vor große Herausforderungen und es sollte dringend größere Harmonisierungsanstrengungen geben. Bei dem Einsatz von neuen Technologien nimmt das Datenschutzrecht gerade in der Verarbeitung von Gesundheits- bzw. Patientendaten eine Schlüsselrolle ein. Die Umsetzung datenschutzrechtlicher Anforderungen, die hochwertige Gesundheitsversorgung und die Sicherung des Wirtschaftsstandorts Deutschland stellen in dem stark regulierten Gesundheitswesen für alle Beteiligten eine Herausforderung dar.

Die Rahmenbedingungen und Strukturen des Datenschutzes im Gesundheitswesen sind teilweise veraltet, unübersichtlich und im heutigen Digitalisierungszeitalter manchmal schwer nachvollziehbar. Dies gilt insbesondere für die Regelungen im stationären Umfeld, da viele datenschutzrechtliche Regelungen in den Landesgesetzen zum Teil seit Jahren nicht an die moderne Gesundheitsversorgung angepasst wurden; so regelt das bayerische Krankenhausgesetz (BayKrG) beispielsweise immer noch explizit „Verarbeitung und Mikroverfilmung von Patientendaten“, obwohl die Mikroverfilmung seit Jahren nicht mehr eingesetzt wird. Bedingt durch die heute eingesetzten digitalen Unterstützungsleistungen und den nicht dazu passenden Landesgesetzen ergeben sich in der Folge sowohl für die in der Gesundheitswirtschaft tätigen Unternehmen, als auch für die Leistungserbringer selbsterhebliche rechtliche Unsicherheiten.

Zwar wurde auf der EU Ebene mit der Datenschutz-Grundverordnung (DS-GVO) ein EU-weit gültiger Rahmen geschaffen, um die geltenden Datenschutzgesetze zu harmonisieren, aber speziell im Bereich des Gesundheitssektors wurden viele gesetzliche Regelungen noch nicht überarbeitet. Es ist nunmehr an den lokalen Gesetzgebern und den Aufsichtsbehörden in den Mitgliedsstaaten, die Möglichkeiten der in der DS-GVO verankerten Öffnungsklauseln mit Bedacht zu nutzen und hierbei bestehende Unzulänglichkeiten und Widersprüche zu beseitigen. Ein Widerspruch zu Art. 28 DS-GVO wird zum Beispiel in Art. 27 BayKrG gesehen, der vorschreibt, dass sich Krankenhäuser zur Verarbeitung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind, (wie beispielsweise klinische Daten), nur anderer Krankenhäuser bedienen dürfen, obgleich Art. 1 DS-GVO vorgibt, dass aus Datenschutzgründen der „freie Verkehr“ und damit die Verarbeitung personenbezogener Daten in der Union weder einge-

schränkt noch verboten werden darf. Insbesondere sollte auch der Landesgesetzgeber rechtliche Rahmenbedingungen schaffen, welche innovative medizinische Forschung und eine hochwertige Versorgung der Bürgerinnen und Bürger unter Nutzung moderner IT-Verfahren ermöglicht.
Wir sehen in Codes of Conduct einen möglichen Weg um zeitnah zu einheitlichen Verarbeitungsstandards zu gelangen und so die Nutzung von Gesundheitsdaten sowie die Forschungsvorhaben zu fördern.
Übergeordnet halten wir Bestrebungen einen gemeinsamen europäischen Datenraum für Gesundheitsdaten für Forschungszwecke zu etablieren für sinnvoll. Die Rechtszersplitterung zwischen den Mitgliedstaaten der EU führt zur Zeit dazu, dass praktisch keine größeren übergreifenden Projekte aufgesetzt bzw. durchgeführt werden können.

Empfehlung 20:
Im Zentrum aller Bemühungen um eine Verbesserung des kontrollierten Zugangs zu (ursprünglich) personenbezogenen Daten steht die Entwicklung von Verfahren und Standards der Anonymisierung und Pseudonymisierung. Durch rechtliche Vermutungen, dass bei Einhaltung des Standards kein Personenbezug mehr gegeben ist bzw. dass „geeignete Garantien" für die Rechte betroffener Personen vorliegen, könnte die Rechtssicherheit deutlich verbessert werden. Diese Maßnahmen sollten flankiert werden durch strafbewehrte Verbote einer De-Anonymisierung (für den Fall, dass bei bisher anonymen Daten, etwa durch die Entwicklung der Technik, ein Personenbezug hergestellt werden kann) bzw. der Aufhebung der Pseudonymisierung jenseits eng definierter Rechtfertigungsgründe. Auch die Forschung im Bereich synthetischer Daten ist vielversprechend und sollte weiter gefördert werden.

Bitkom Einschätzung:
Die Anonymisierung von Daten ist eine der derzeit wichtigsten Fragen rund um die Anwendung der DS-GVO. Die bisher unklare Rechtslage stellt viele Anwender vor große Herausforderungen. Der Mehrwert von anonymisierten Daten liegt jedoch auf der Hand, da im Bereich der Forschung, KI-Training, für die Entwicklung von Produkten auch ohne personenbezogenen Date Fortschritte gemacht werden könnten, die essentiell sind für die Datenökonomie und damit auch für das Gelingen der deutschen und europäischen Datenstrategie. Auch der mit der KI-Strategie angestoßene Kurs, die gewünschte Förderung von KI-Anwendungen und der Aufbau Deutschlands und Europas als Exzellenzzentrum für KI werden nur gelingen, wenn die Nutzbarmachung von Daten und deren Bereitstellung für das Training von Modellen nachhaltig verbessert wird. Anonymisierung ist eine der vielversprechendsten Lösungen, um Datenschutz und Analyse- und Verarbeitungsinteressen miteinander zu vereinbaren. Die politische Bedeutung der Diskussion rund um die Anonymisierung könnte daher kaum höher sein. Zur Pseudonymisierung gibt es bereits weitge-

diehene Arbeiten, die nun weiter verfolgt werden sollten, um die Rechtssicherheit zu erhöhen.[7][8]

Empfehlung 21:
Großes Potenzial sieht die DEK grundsätzlich auch in innovativen Datenmanagement- und Datentreuhandsystemen, sofern diese praxisgerecht, robust und datenschutzkonform ausgestaltet sind. Solche Modelle rangieren von rein technischen Dashboards (Privacy Management Tools, PMT) bis hin zu umfassenden Dienstleistungen der Daten- und Einwilligungsverwaltung (Personal Information Management Services, PIMS). Ziel ist die Befähigung des Einzelnen zur Kontrolle über seine personenbezogenen Daten sowie die Entlastung des Einzelnen von Entscheidungen, die ihn überfordern. Die DEK empfiehlt, Forschung und Entwicklung im Bereich von Datenmanagement- und Datentreuhandsystemen intensiv zu fördern, mahnt aber auch an, dass eine die Rechte und Interessen aller Beteiligten wahrende Entwicklung ohne eine begleitende europäische Regulierung nicht zu erwarten ist. Diese Regulierung müsste zentrale Funktionen absichern, ohne die Betreiber solcher Systeme nur sehr eingeschränkt tätig werden können. Andererseits geht es um den Schutz des Einzelnen vor vermeintlichen Interessenwaltern, die in Wahrheit vorrangig wirtschaftliche Eigeninteressen oder Interessen Dritter vertreten. Sofern dieser Schutz auch in der Praxis garantiert werden kann, kann Datentreuhandmodellen die Funktion einer wichtigen Schnittstelle zwischen Belangen des Datenschutzes und der Datenwirtschaft zukommen.

Bitkom Einschätzung:
Wir begrüßen den Fokus der DEK auf Datenmanagement- und Datentreuhandymodelle. Hierzu sollten zeitnah gemeinsam mit der Wirtschaft Praxisbeispiele etabliert werden bzw. die gerade im Aufbau befindlichen Datentreuhandmodelle, wo sie in neue praktikable Ansätze bieten, gefördert werden. Hierbei sind auch vorhandene Marktlösungen, die den Verbraucher in der Rechte- und Zugriffszuweisung, dem Handling seiner Daten unterstützen, zu beachten und ggf. auf sie aufzusetzen.

[7] Siehe hierzu die Ausarbeitung im Rahmen des Gipfelprozesses 2019: Entwurf eines CoC für DS-GVO konforme Pseudonymisierung: https://www.bitkom.org/Bitkom/Publikationen/Entwurf-fuer-Code-of-Conduct-Einsatz-DS-GVO-konformer-Pseudonymisierung

[8] Siehe dazu auch die Bitkom Position zur Konsultation des BfDI zu Anonymisierung: https://www.bitkom.org/Bitkom/Publikationen/BfDI-Konsultation-zur-Anonymisierung

Empfehlung 22 und 23

22: In Bezug auf das Recht auf Datenportabilität aus Art. 20 DSGVO empfiehlt die DEK die Erarbeitung branchenbezogener Verhaltensregeln und Standards betreffend Datenformate. Soweit Art. 20 DSGVO nicht nur Anbieterwechsel erleichtern, sondern auch den Datenzugang für andere Anbieter verbessern soll, empfiehlt sich eine sorgfältige Evaluierung, wie sich das bestehende Portabilitätsrecht auf den Markt auswirkt und wie eine zunehmende Stärkung der Marktmacht weniger Anbieter verhindert werden kann. Bevor die Ergebnisse einer solchen Evaluierung vorliegen, sollte von einer vorschnellen Erweiterung des Portabilitätsrechts, etwa auf andere als bereitgestellte Daten oder auf Portierung in Echtzeit, abgesehen werden.
23: Eine Pflicht zur Interoperabilität bzw. Interkonnektivität in bestimmten Sektoren – etwa bei Messenger- Diensten und sozialen Netzwerken – könnte dazu beitragen, Markteintrittsbarrieren für neue Anbieter zu senken. Für eine solche Pflicht würde sich eine asymmetrische, d. h. nach Marktmacht gestaffelte Regulierung empfehlen. Dies wäre auch eine Voraussetzung dafür, bestimmte Basisdienstleistungen der Informationsgesellschaft in Europa neu aufzubauen bzw. zu stärken.

Bitkom Einschätzung:

Wir begrüßen Ansätze zur Förderung von Datenportabilität[9]. Entsprechende Verhaltensregeln und Standards können wir mitentwickeln (einige gibt es bereits) und bieten hier unsere Expertise an. Für wichtig erachten wir dabei auch die Dimension der nichtpersonenbezogenen Daten (Open Data und offene Schnittstellen).[10] Insbesondere im Kontext von Open Data sollten die Dimensionen von Datenportabilität und Interoperabilität stets mitgedacht und konkrete politische Maßnahmen gestartet werden, um die Auffindbarkeit und Nutzbarkeit der vorhandenen Datensätze zu verbessern. Open Data zeichnet sich insbesondere durch eine einfache Auffindbarkeit und eine maschinenlesbare Form aus. Daraus folgt, dass eine nutzerfreundliche Bereitstellung von Open Data nicht in proprietären Formaten (z.B. eher csv als xls) oder in gänzlich ungeeigneter Form (z.B. pdf) erfolgen kann. Open Data müssen über offene, interoperable Formate und über offene Schnittstellen (Open API) bereitgestellt werden, um den maximalen Nutzen aus Open Data zu ziehen.

In der Informationsverarbeitung werden seit jeher Schnittstellen/APIs (Application Programming Interface) verwendet, um die Verzahnung, Dynamik und Komplexität digitaler

[9] Siehe hierzu die Bitkom Position: https://www.bitkom.org/Bitkom/Publikationen/Interoperabilitaet-Datenportabilitaet-Bitkom-Antworten-auf-die-Fragen-des-BMJV sowie die Einschätzungen im Kontext des Kartellrechts: https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Stellungnahme-zur-10-GWB-Novelle
[10] Siehe hierzu auch das Bitkom 10-Punkte Papier zu Open Government Data: https://www.bitkom.org/Bitkom/Publikationen/10-Punkte-fuer-Open-Government-Data

Technologien handhabbar zu machen, sowie die organisatorische und technische Komplexität zu abstrahieren. Durch offene Schnittstellen (Open API) können z. B. bisher unsichtbare Backend-Systeme für Third-Party Developer sicht- und nutzbar gemacht werden. Dadurch entsteht in externen App- und Web-Märkten mehr Kundenreichweite, die Umsätze mit über APIs bereitgestellten Daten können gesteigert werden und Innovationen werden stimuliert. Die Entwicklung von Fähigkeiten zur Planung, Einrichtung und den Betrieb entsprechender API ist von hoher strategischer Bedeutung. Um offene Schnittstellen für Open Data in Deutschland erfolgreich zu etablieren, bedarf es einer gemeinsamen Anstrengung und eines Diskurses von Verwaltung, Wirtschaft, Wissenschaft und Zivilgesellschaft.

Empfehlung 24:
Für die Entwicklung der europäischen Datenwirtschaft sieht die DEK einen zentralen Faktor im Zugang europäischer Unternehmen zu geeigneten nicht-personenbezogenen Daten in geeigneter Qualität. Datenzugang nutzt allerdings nur Akteuren, die ein entsprechendes Bewusstsein für die Bedeutung von Daten haben und über entsprechende Datenkompetenz verfügen, und in ganz überproportionalem Ausmaß denjenigen, bei denen bereits der größte Ausgangsbestand an Daten und die besten Dateninfrastrukturen vorhanden sind. Die DEK empfiehlt daher, bei der Diskussion um eine Verbesserung des Datenzugangs stets die genannten Faktoren gemäß dem ASISA-Prinzip (Awareness – Skills – Infrastructures – Stocks – Access) mit zu berücksichtigen.

Bitkom Einschätzung:
Wichtig wäre aus unserer Sicht zunächst die Klärung der Frage wer die geeigneten nicht-personenbezogenen Daten in geeigneter Qualität bereitstellt. Datenpooling und Datenteilung müssen immer im freiwilligen Kontext vollzogen werden. Viele Unternehmen stellen bereits weitreichende Daten-, Forschungsergebnisteilung sowie offene Standards, Tools und Protokolle zur Verfügung. Verpflichtendes Datenpooling oder eine allgemeine Datenteilungspflicht (sowohl im B2B als auch im B2G-Kontext) lehnen wir ab.

Empfehlung 25:
Daher unterstützt die DEK die bereits auf europäischer Ebene begonnenen Maßnahmen zur Förderung von Dateninfrastrukturen im weitesten Sinne (z. B. Plattformen, Standards für Programmierschnittstellen und weitere Elemente, Modellverträge, EU-Unterstützungszentrum) und empfiehlt der Bundesregierung, diese weiterhin durch entsprechende Bemühungen auf nationaler Ebene zu flankieren. In diesem Zusammenhang bietet sich die Einrichtung einer Ombudsstelle auf Bundesebene an, welche bei Aushandlung von Datenzugangsvereinbarungen und bei Streitigkeiten hilft und vermittelt.

Bitkom Einschätzung:

Wir begrüßen den hier von der DEK vorgezeichneten Ansatz. Es sollten mehr gezielte Anreize für die Zusammenarbeit öffentlicher und privater Stellen, sowie Kooperationserleichterungen im Allgemeinen, z.B. zur Schaffung von Datenplattformen, geboten werden.[11] Freiwillige Maßnahmen sollten politisch gefördert und incentiviert werden.

Empfehlung 26:

Die DEK sieht einen Schlüsselfaktor in einer holistisch gedachten, nachhaltigen und strategischen Wirtschaftspolitik, welche der Abwanderung innovativer europäischer Unternehmen bzw. deren Aufkauf durch Akteure aus Drittstaaten ebenso effektiv entgegenwirkt wie der übermäßigen Abhängigkeit von Infrastrukturen (z. B. Serverkapazitäten) in Drittstaaten. Dabei ist die richtige Balance zu finden zwischen gewollter internationaler Kooperation und Vernetzung einerseits und andererseits der entschlossenen Übernahme von Verantwortung für nachhaltige Sicherheit und Wohlfahrt in Europa vor dem Hintergrund sich wandelnder globaler Machtverhältnisse.

Bitkom Einschätzung:

Wir verstehen die hier angesprochenen Aspekte insbesondere im Kontext der Digitalen Souveränität.[12] Die Debatten hierum sind zum Teil missverständlich. Wir wollen deshalb den Begriff der Digitalen Souveränität aufarbeiten und einen fundierten Beitrag zu den jüngsten politischen Debatten z. B. zu Gaia-X oder um den Ausbau des 5G-Netzes leisten. Wir haben kürzlich dargelegt, welche Handlungsfelder Digitale Souveränität aus Sicht der Digitalwirtschaft adressiert und welche unterschiedlichen Interessen dabei bestehen. Im Kern ist die Digitale Souveränität die Möglichkeit zur unabhängigen digitalen Selbstbestimmung. Im internationalen Zusammenhang bedeutet das vor allem, eigene Gestaltungs- und Innovationsspielräume zu erhalten und einseitige Abhängigkeiten zu vermeiden. Welche Punkte aus Sicht der Digitalwirtschaft grundlegend für die Wahrung dieser Handlungs- und Gestaltungsfreiheit sind, haben wir in unserem Positionspapier „Digitale Souveränität: Anforderungen an Technologien- und Kompetenzfelder mit Schlüsselfunktion“ zusammengefasst.
Wir halten konkrete Maßnahmen und Empfehlungen für notwendig, um insbesondere die Abwanderung zeitnah zu adressieren und die angesprochene nachhaltige und strategische Wirtschaftspolitik zu fördern.

[11] Siehe hierzu auch die Ausführungen zu Kooperationserleichterungen in der 10. GWB Novelle: https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Stellungnahme-zur-10-GWB-Novelle

[12] Siehe hierzu auch die Ausführungen in der Bitkom Stellungnahme zur Digitalen Souveränität: https://www.bitkom.org/Bitkom/Publikationen/Digitale-Souveraenitaet-Anforderungen-an-Technologien-und-Kompetenzfelder-mit-Schluesselfunktion

Empfehlung 27:

Die DEK sieht auch unter dem Blickwinkel einer Förderung der Datenwirtschaft keinen Bedarf nach der Einführung neuer Ausschließlichkeitsrechte („Dateneigentum", „Datenerzeugerrecht"), sondern empfiehlt stattdessen eine beschränkte Drittwirkung vertraglicher Vereinbarungen (z. B. betreffend Beschränkungen der Nutzung und Weitergabe von Daten) nach dem Vorbild des neuen europäischen Regimes zum Schutz von Geschäftsgeheimnissen. Ferner wäre es wünschenswert, wenn gesetzlich Wege aufgezeigt würden, wie europäische Unternehmen – etwa unter Einschaltung von Treuhändern – unter voller Wahrung kartellrechtlicher Belange bei der Datennutzung kooperieren können („Datenpartnerschaften").

Bitkom Einschätzung:

Auch wir halten neue Ausschließlichkeitsrechte für nicht zielführend. Ebenso wie die DEK lehnen wir die Schaffung eines „Dateneigentums" ab.[13] Die im Rahmen der 10. GWB Novelle adressierte Kooperationsförderung unterstützen wir. Sie ist notwendige Voraussetzungen für Wettbewerbsfähigkeit und für den Aufbau von Plattformen und Datenpools.

Empfehlung 28:

In bestehenden Wertschöpfungssystemen (z. B. Produktions- und Vertriebsketten) fallen vielfach Daten an, die innerhalb wie außerhalb des Wertschöpfungssystems von enormer wirtschaftlicher Bedeutung sind. Die zwischen den einzelnen Teilnehmern eines Wertschöpfungssystems bestehenden Verträge enthalten aber häufig entweder keine bzw. eine unfaire und/oder ineffiziente Regelung des Datenzugangs, oder es fehlt ganz an einer vertraglichen Vereinbarung. Weit über die klassische „Datenwirtschaft" hinaus ist daher Bewusstseinsbildung bei Wirtschaftstreibenden erforderlich, die durch praktische Hilfestellungen (z. B. Modellverträge) ergänzt werden sollte.

Bitkom Einschätzung:

Mit der zunehmenden Bewusstseinsbildung über die Bedeutung von Daten werden auch entsprechende Regelungen in Verträge[14] zwischen Unternehmen aufgenommen. Dass diese Verträge häufig ineffiziente oder gar unfaire Regelungen zum Datenzugang enthalten teilen wir nicht, halten aber die Weiterentwicklungen von Datenteilungsregeln vertraglicher Art für sinnvoll, wo dies branchenspezifisch umsetzbar ist. Die Erfahrung zeigt, dass die Erstellung von Modellverträgen (abgesehen von den Anforderungen des Kartell-

[13] Bitkom Positionen zum Thema: https://www.bitkom.org/sites/default/files/2019-09/bitkom-stellungnahme-zu-datenrechten_kurzfassung_final.pdf und https://www.bitkom.org/Bitkom/Publikationen/Wettbewerbskommission-40-Fragen-und-Antworten
Und Stellungnahme zur 10. GWB-Novelle: https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Stellungnahme-zur-10-GWB-Novelle

[14] Siehe auch hierzu: https://www.bitkom.org/Bitkom/Publikationen/Rechtsfragen-der-digitalisierten-Wirtschaft-Rechte-an-Daten

rechts und des AGB-Rechts) angesichts der Vielzahl ganz unterschiedlicher Geschäftsbeziehungen, Regelungsszenarien und Anforderungen im Einzelfall sowie der rasanten Entwicklung neuer Geschäftsmodelle und –beziehungen nur einen begrenzten Wert haben und praktisch kaum durchführbar ist. So hat z.B. auch die EU-Kommission mit diesem Ziel Untersuchungen begonnen. Das Ergebnis waren aber keine Modellvertragsklauseln, sondern „nur" allgemeine Empfehlungen für die Vertragsgestaltung.[15]

Empfehlung 29:
Darüber hinaus regt die DEK eine behutsame Ergänzung des geltenden Rechtsrahmens an. Dabei sollte ein erster Schritt darin liegen, die Sonderbeziehung zwischen einer Partei, welche zur Generierung von Daten in einem Wertschöpfungssystem beigetragen hat, und der Partei, welche die Daten faktisch kontrolliert, in § 311 BGB explizit anzuführen. Unter anderem sollte die Aufnahme von Vertragsverhandlungen über ein faires und effizientes Datenzugangsregime Bestandteil einer solchen allgemeinen Treuepflicht sein. Im Übrigen sollte geprüft werden, ob darüber hinaus Maßnahmen erforderlich sind, welche von punktuellen Klauselverboten in B2B-Geschäften über ein dispositives Datenschuldrecht bis zu sektorspezifischen Datenzugangsrechten rangieren könnten.

Bitkom Einschätzung:
Jeder Eingriff in das geltende Vertragsrecht sollte sehr behutsam durchgeführt werden. Dabei darf es nicht zu einer allgemeinen Datenteilungspflicht kommen. Sektorspezifische Datenzugangsrechte dürfen nicht im allgemeinen Vertragsrecht geregelt werden. Vielmehr sollte der Gesetzgeber den insoweit schon eingeschlagenen Weg der begrenzten spezialgesetzlichen Regulierung (z.B. im Messstellenbetriebsgesetz oder im Zahlungsdiensteaufsichtsgesetz) weiter verfolgen.

Empfehlung 30:
Die DEK sieht großes Potenzial in Konzepten offener Daten des öffentlichen Sektors (Open Government Data, OGD) und empfiehlt, solche Konzepte auszubauen und zu fördern. Sie empfiehlt eine Reihe von Maßnahmen, die einen teilweise noch nicht ganz vollzogenen Bewusstseinswandel öffentlicher Stellen befördern und das Teilen von Daten im Rahmen von OGD-Konzepten praktisch erleichtern könnten. Dazu gehört neben der Etablierung entsprechender Infrastrukturen (z. B. Plattformen) auch eine Harmonisierung und punktuelle Ergänzung des derzeit zersplitterten und nicht in jeder Hinsicht konsistenten Rechtsrahmens.

[15] Vgl hier: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018SC0125&from=EN

Bitkom Einschätzung:

Wir begrüßen die Aussagen der DEK zu Open Government Data und unterstützen ausdrücklich, dass die darin liegenden Potenziale durch konkrete Maßnahmenpakete gefördert werden müssen.[16] Wir unterstützen Public-Private Kollaboration sowie Partnerschaften und die Zielsetzung, darüber eine Vereinfachung/Unterstützung der Veröffentlichung und Nutzbarmachung von öffentlichen Daten zu erreichen. Aufnahme von Open Government Data und Förderung befürworten wir. Insbesondere die Verzahnung der Novellierung des Open Data Gesetzes und der PSI Richtlinie ist dabei wichtig.

Empfehlung 31:

Allerdings sieht die DEK auch ein schwer zu lösendes Spannungsverhältnis zwischen der Diskussion um OGD (mit Prinzipien wie „offen by default" und „offen für alle Zwecke") einerseits und um besseren Schutz von Geschäftsgeheimnissen und personenbezogenen Daten (mit gesetzlichen Vorgaben wie „Datenschutz by default") andererseits. Sie plädiert dafür, in Zweifelsfällen zugunsten des staatlichen Schutzauftrags zu entscheiden, der in Bezug auf Daten, welche Einzelne oder Unternehmen dem Staat – oft nicht freiwillig – anvertraut haben (z. B. Steuerdaten), besteht. Diesem staatlichen Schutzauftrag ist durch eine Reihe von Maßnahmen nachzukommen, die auch technische und rechtliche Schutzvorkehrungen gegen Missbrauch umfassen.

Bitkom Einschätzung:

Aus unserer Sicht ist fraglich, wie weit der staatliche Schutzauftrag gefasst werden würde und ob somit die Ausnahmetatbestände vergrößert werden / (zu) wenig veröffentlicht werden.

Empfehlung 32:

In diesem Zusammenhang wird insbesondere empfohlen, für das Teilen von Daten durch den öffentlichen Sektor Standardlizenzen und Modellkonditionen zu entwickeln und – mindestens sektorspezifisch – deren Verwendung bindend vorzuschreiben. Diese sollten klar definierte Garantien für die Rechte betroffener Dritter enthalten. Ferner sollten sie Mechanismen vorsehen, die geeignet sind, eine gemeinwohlschädigende Nutzung der Daten ebenso zu verhindern wie eine wettbewerbsrechtlich unerwünschte Verstärkung bestehender Marktmacht oder eine Doppelbelastung des Steuerzahlers.

[16] Siehe hierzu auch die Bitkom Stellungnahme zu den Eckpunkten der Datenstrategie: https://www.bitkom.org/Bitkom/Publikationen/Stellungnahme-zu-den-Eckpunkten-einer-Datenstrategie-der-Bundesregierung sowie den 10-Punkte Plan für Open Government Data: https://www.bitkom.org/Bitkom/Publikationen/10-Punkte-fuer-Open-Government-Data

Bitkom Einschätzung:
Wir stimmen der DEK hinsichtlich der Nutzung von Standardlizenzen zu, halten grundsätzlich aber europäische Standards für zielführender. Hinsichtlich der angesprochenen Garantien für die Rechte betroffener Dritter weisen wir darauf hin, dass Open Data gerade darauf basiert, dass eben nicht nachverfolgt wird, bzw. keine Rechtfertigung gegeben werden muss, was mit den Daten geschieht. Zudem ist aus unserer Sicht unklar, wer definieren würde was eine „gemeinwohlschädigende Nutzung der Daten ist" und nach welchen Kriterien diese Bewertung erfolgen würde.

Empfehlung 33:
Betreffend Konzepte offener Daten im privaten Sektor sollte in erster Linie auf die Ermutigung und Förderung eines freiwilligen Teilens von Daten gesetzt werden. Dabei ist nicht nur an Infrastrukturen (z. B. Plattformen) zu denken, sondern auch an eine breite Palette möglicher Anreizstrukturen, etwa bei der Besteuerung, bei öffentlichen Ausschreibungen, bei Förderprogrammen oder bei Genehmigungsverfahren. Gesetzliche Datenzugangsrechte und korrespondierende Zugangsgewährungspflichten sollten dagegen erst in zweiter Linie in Betracht gezogen werden.

Bitkom Einschätzung:
Die Auffassung der DEK in dieser Empfehlung teilt Bitkom. Auch hier könnte auf CoCs abgestellt werden, was insbesondere auch eine sektorspezifische Adressierung umfassen würde: Eine Branche könnte festlegen, wie Daten geteilt werden und erhält die hier aufbereiteten Anreize. Bei den durchaus sinnvollen und weitreichenden Anreizen sollte aber sichergestellt sein, dass wer diese bekommt, auch die Pflichten dafür erfüllt. Sonst wird gerade bei Erleichterungen gesetzlicher Pflichten die Gefahr groß, dass das Instrument der freiwilligen Verpflichtung durch Täuschung missbraucht und nach Jahren der Imageverbesserung wieder mit Misskredit kommt.

Empfehlung 34:
Insgesamt rät die DEK bei allgemeinen gesetzlichen Datenzugangsrechten zu einem behutsamen Vorgehen, idealerweise zunächst in ausgewählten Sektoren. Beispielsweise könnte ein Bedarf im Nachrichten-, Mobilitäts- oder Energiesektor geprüft werden. Dabei sind jeweils alle möglichen Konsequenzen einer Zugangsgewährungs- oder gar Offenlegungspflicht sorgsam zu bedenken und gegeneinander abzuwägen, angefangen von möglichen Implikationen für den Datenschutz und Schutz von Geschäftsgeheimnissen, über Folgen für Investitionsentscheidungen und die Verteilung von Marktmacht bis hin zu den strategischen Interessen deutscher und europäischer Unternehmen im Verhältnis zu Unternehmen in Drittstaaten.

Bitkom Einschätzung:

Bitkom lehnt allgemeine gesetzliche Zugangsrechte ab. Solche Rechte sind auf spezifische Bereiche zu beschränken und erst nach sorgsamer Analyse des bestehenden Bedarfs, der betroffenen Interessen und des notwendigen Interessenausgleichs einzuführen.

Empfehlung 35:

Die DEK empfiehlt, Zugangsgewährungspflichten privater Unternehmen zugunsten gemeinwohlorientierter Zwecke und des öffentlichen Sektors (Business-to- Government, B2G) in Erwägung zu ziehen. Auch diesbezüglich dürfte indessen ein behutsames und sektorspezifisches Vorgehen anzuraten sein.

Bitkom Einschätzung:

Grundsätzlich begrüßen wir neue Zugangsmöglichkeiten. Im Detail sind diese jedoch zu prüfen und vor allem aber ist darauf achten, dass nicht umgekehrt ein Zugangsanspruch staatlicher Stellen auf privatwirtschaftliche Daten geschaffen wird.[17] Zugangsgewährungspflichten privater Unternehmen zugunsten gemeinwohlorientierter Zwecke sind aus unserer Sicht deutlich zu unbestimmt. Es darf keine Generalklausel für den Staat geben, unter der er in das Eigentumsrecht von Unternehmen eingreift, zumal hier auch kollidierende Güter in Frage stehen, zB Datenschutz oder Geschäftsgeheimnisse. Es ist auch nicht ersichtlich, wieso ein Unternehmen (unabhängig von der Branche) dem Staat seine Daten offenlegen sollte.

2. Einleitung und Bitkom Einschätzung zu den DEK Empfehlungen für algorithmische Systeme:

Ab Empfehlung 35 des Abschlussgutachtens setzt sich die DEK mit „algorithmischen Systemen“ auseinander und macht verschiedene Vorschläge zu deren Regulierung, Governance und Einsatz. Aus unserer Sicht wäre es notwendig gewesen, die Begrifflichkeit einleitend zu definieren und festzulegen, was darunter gefasst werden soll. Indem das Gutachten diesen wichtigen ersten Schritt überspringt lässt es wichtige Fragen ungeklärt und die Empfehlungen einerseits konturlos, andererseits deutlich zu weit gefasst stehen. Die definitorische Arbeit ist zweifelsohne mühsam und hätte ggf. den zeitlichen Rahmen der Beauftragung der Datenethikkommission gesprengt – dies darf ein staatlich eingesetztes Expertengremium jedoch nicht von dieser Aufgabe entbinden. Die hier fehlenden Ausführungen sollten im Rahmen der weiteren Bearbeitungen und insbesondere auch einer konkreten Umsetzung der Empfehlungen dringend nachgeholt werden.

[17] Siehe hierzu auch die Ausführungen in der Kommentierung der Eckpunkte der Datenstrategie: https://www.bitkom.org/Bitkom/Publikationen/Stellungnahme-zu-den-Eckpunkten-einer-Datenstrategie-der-Bundesregierung

Die im Abschlussbericht vorgeschlagene Kritikalitätspyramide zur Bewertung und Einstufung von „algorithmischen Systemen“ ist grundsätzlich ein interessanter Ansatz. Auch in anderen Ländern werden Möglichkeiten der Bewertung und Einstufung von algorithmischen Systemen entwickelt.[18] Jedoch gehen diese anderen Ansätze differenzierter vor und ermöglichen eine Betrachtungsweise, die etwas mehr der Vielzahl an möglichen Algorithmen, deren Kombination und Weiterentwicklungsmöglichkeit entspricht. Eine Einstufung in 5 Kategorien geht aus unserer Sicht an der Lebenswirklichkeit vorbei: Viele Algorithmen werden für ein bestimmtes Einsatzgebiet entwickelt, für einen weiteren Einsatzzweck fortentwickelt und schließlich in Kombination mit weiteren Anwendungen in einem völlig neuem Kontext eingesetzt.

Der Bericht hätte in den Ausführungen zu algorithmischen Systemen daher herausstellen müssen, dass Algorithmen Werkzeuge sind, sich verändernde, in verschiedenem Kontext eingesetzte Software und Entscheidungshilfen. Es kommt daher immer auf die Anwendungen und Umgebungen an, in denen sie eingesetzt werden, ohne dass eine pauschale Einstufung vorab möglich und sinnvoll ist. Genauso zentral und wichtig wie die gesellschaftliche Debatte um den ethischen und vertrauenswürdigen Einsatz von Daten und Algorithmen ist eine gesellschaftliche Debatte und eine breite gesellschaftliche Bildung über das Verständnis und die Funktionsweise von Algorithmen. Diese basieren auf Regeln, Handlungsvorschriften und der Betrachtung historischer Daten und Prozesse. Wenn also über die Chancen und Risiken, sowie das Schädigungspotenzial von Algorithmen diskutiert wird, dann muss als Referenzszenario auch immer eines mitberücksichtigt werden, in dem kein Algorithmus genutzt wird. Wie werden Entscheidungen dann getroffen? Wie werden Probleme dann gelöst? Welche Fehlerquoten und Schädigungspotenziale existieren in dem jeweiligen kontextspezifischen Referenzszenario? In vielen Fällen sorgen Algorithmen zum Beispiel dafür, dass bestehende Diskriminierungen und Schädigungen aufgedeckt und transparent gemacht werden und dann im nächsten Schritt reduziert und abgeschaltet werden können. Eine Betrachtung der Chancen und Potenziale in diesem Zusammenhang fehlt in dem Bericht und sorgt dafür, dass ein generelles Bild der Bedrohungen und Risiken beim Einsatz von Algorithmen entsteht.

Einige Passagen des Gutachtens zeigen deutlich, wie essentiell detaillierte Ausführungen und Beispiele sind, beschäftigt sich die DEK doch mit wichtigen Fragen wie der Kritikalität

[18] So zB in Canada: https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/responsible-use-ai/algorithmic-impact-assessment.html; oder auch durch die EU Guidelines zu Ethics in AI: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf. Siehe hierzu auch: https://www.bitkom.org/Presse/Presseinformation/Bitkom-zur-europaeischen-Daten-und-KI-Strategie

und alltäglichen Anwendungen wie dynamischer Preissetzung. So ist es aus unserer Sicht zwar positiv, dass der Bericht im Rahmen der Stufenpyramide einen großen Anwendungsbereich algorithmischer Systeme ohne oder mit geringem Schädigungspotential sieht (S.177). Wenn aber das gewählte Beispiel für diese untere Stufe ohne besonderen Regelungsbedarf der Algorithmus in einem Getränkeautomaten ist (Beispiel 13, S. 178) und damit die Benchmark für das Einsatzgebiet „im grünen Bereich" anlegt, liegt die Frage nahe, ob alle Anwendungen, die „gefährlicher" als ein Getränkeautomat sind, zukünftig kontrollbedürftig sind. Das verstellt den Blick auf die Potentiale und Chancen algorithmischer Systeme enorm und führt aus unserer Sicht nicht dazu, das Vertrauen in technologische Entwicklung zu erhöhen. Hier hätte es weiterer Ausführungen und vor allem differenzierter Beispiele bedurft, um die grafisch dargestellte Kernaussage (großer grüner Bereich) zu untermauern und Verständnis für die Anwendungen zu schaffen.
Ein „kritischer" Algorithmus findet sich ebenso in der dynamischen Preissetzung: "Dynamische Preissetzung (etwa nach den Kriterien von Angebot und Nachfrage) im Online-Handel, die aber keine Personalisierung von Preisen beinhaltet, hat laut Gutachten ein meist geringes, aber doch die Relevanzschwelle überschreitendes Schädigungspotenzial, etwa betreffend einer versteckten Diskriminierung." (Beispiel 14, S.179). Preissetzung nach den Kriterien Angebot und Nachfrage mit einer versteckten Diskriminierung zu verbinden und hieraus Regulierungsbedürftigkeit und Kontrollmechanismen abzuleiten, schießt über das Ziel hinaus.

Mit weiteren wichtigen Fragen hat sich die DEK ebenfalls nicht ausreichend beschäftigen können (wobei uns selbstverständlich der enge zeitliche Erarbeitungskorridor bekannt ist): Nicht ausreichend beantwortet ist z.B. die Frage, wie wir mit Algorithmen umgehen, die auf der Welt für den Weltmarkt entwickelt werden und hier dann bei uns aufgrund der Anforderungen nicht eingesetzt werden können, obwohl der EU Rechtsrahmen dies zuließe – das wird für den weit überwiegenden Großteil der Algorithmen gelten. Auch hier zeigt sich, dass wir in der Diskussion um Algorithmen eine andere Perspektive einnehmen müssen: Wir sollten unsere begrenzten Kapazitäten auf die Entwicklung von Algorithmen konzentrieren, nicht auf ihre Kontrolle. Wir müssen Entwicklungschancen betonen und Forschung fördern. Das Risiko einiger weniger Anwendungen rechtfertigt nicht das Risiko, unsere technologische Entwicklung nachhaltig zu hemmen, Wettbewerbsfähigkeit vollständig einzubüßen und die riesigen Potentiale von Datenökonomie und algorithmischen Anwendungen für die Gesellschaft zu verhindern.
Hinsichtlich eines möglichen Referenzmodells könnte über einen dreigeteilten risikobasierten Ansatz in Kombination mit einem CoC nachgedacht werden:

- (Stufe 1) Generell unkritische Szenarien identifizieren, und gesetzlich unmittelbar privilegieren / erlauben.
- (Stufe 3) Generell kritische Szenarien identifizieren, und gesetzlich unmittelbar untersagen – am besten mit Evaluierungsfrist.
- (Stufe 2) Grauzone erlauben, wenn hinreichende TOMs etabliert. Wenn sektorspezifisch mit CoC unterlegt, wie Stufe 1 behandeln.

Empfehlung 36 und 37:
36: Die DEK empfiehlt einen risikoadaptierten Regulierungsansatz für algorithmische Systeme. Er sollte auf dem Grundsatz aufbauen, dass ein steigendes Schädigungspotenzial mit wachsenden Anforderungen und Eingriffstiefen der regulatorischen Instrumente einhergeht. Für die Beurteilung kommt es jeweils auf das gesamte sozio-technische System an, also alle Komponenten einer algorithmischen Anwendung einschließlich aller menschlichen Akteure, von der Entwicklungsphase (z. B. hinsichtlich der verwendeten Trainingsdaten) bis hin zur Implementierung in einer Anwendungsumgebung und zur Phase von Bewertung und Korrektur.
37: Die DEK empfiehlt, die Bestimmung des Schädigungspotenzials algorithmischer Systeme für Einzelne und/oder die Gesellschaft anhand eines übergreifenden Modells einheitlich vorzunehmen. Dafür sollte der Gesetzgeber mit Hilfe von Kriterien ein Prüfschema definieren, nach welchem die Kritikalität algorithmischer Systeme auf der Grundlage der von der DEK vorgestellten allgemeinen ethischen und rechtlichen Grundsätze und Prinzipien zu bestimmen ist.

Bitkom Einschätzung:
Wir unterstützen, dass die DEK hier von Risikoadaption ausgeht, raten jedoch zu Vorsicht wenn bereits in dieser frühen Phase der Entwicklung reguliert wird. Regulierungsansätze müssen zwingend vertikal, nicht horizontal die Risikobewertung vornehmen. Das hier aufgezeigte Risikomodell ist in sich widersprüchlich und die einzelnen Klassen zT schwer voneinander abzugrenzen (insb. Klasse 3 und 4). Die Schwellen sind darüber hinaus zu ungenau/unvollständig definiert, sodass selbst einfachste algorithmische Anwendungen (Waschmaschine, Warenautomat) nicht mehr „risikofrei“ und damit nach Auffassung der DEK regulierungsbedürftig wären. Die technologische Entwicklung darf weder horizontal noch zu früh eingeschränkt werden – es müssen Freiräume für Weiterentwicklung und Experimentierräume bleiben. Die risikobasierte Betrachtung als Basis für Überlegungen zur Notwendigkeit einer (sektorspezifischen) Regulierung kann sinnvoll sein, aber die hier beschriebene Umsetzung in eine generelle Regulierung mit den zusätzlich aufgeführten Prinzipien würde fast unweigerlich zu Überregulierung und Bürokratie auch in unkriti-

schen Bereichen führen. Das vorgeschlagene Modell ist daher auch in sich widersprüchlich.

Aus unserer Sicht bleiben derzeit vor allem die wichtigsten grundlegenden Fragen unbeantwortet:

- Wer nimmt die Risikobewertung vor? Und für welche Einsatzfelder?
- Wird die Weiterentwicklung, Zusammenführung, Dynamik der Entwicklung ausreichend berücksichtigt?
- Welche Kriterien werden für die Kritikalität herangezogen? Um welche betroffenen Rechte kann und sollte es dabei (nur) gehen?

Empfehlung 38:

Regulatorische Instrumente und Anforderungen an algorithmische Systeme sollten u. a. Korrektur- und Kontrollinstrumente, Vorgaben für die Transparenz, die Erklärbarkeit und die Nachvollziehbarkeit der Ergebnisse sowie Regelungen zur Zuordnung von Verantwortlichkeit und Haftung für den Einsatz umfassen.

Bitkom Einschätzung:

Anforderungen an die Erklärbarkeit algorithmischer Systeme sind bereits in der DS-GVO angelegt. Hierbei gilt es jedoch, die technischen Möglichkeiten, die Verständlichkeit und Nachvollziehbarkeit für den Betroffenen und die Interessen der Algorithmeninhaber an Geschäftsgeheimnisschutz zu beachten. Eine parallele Algorithmenverordnung mit gesonderten Vorgaben könnte sowohl zu Dopplungen als auch zu Widersprüchen mit den Datenschutzvorgaben führen. Der Abschlussbericht ist diesbezüglich aus unserer Sicht auch noch zu unklar formuliert, da nicht deutlich wird, wie weitreichend die Erklärbarkeit zu verstehen ist – hier können Ansätze von (verständlichem) generellem Produktverständnis bis hin zu (zu weitreichender) exakter Kriterienwidergabe oder Open Code Anforderungen reichen.

Zur Herstellung von Transparenz gibt es zudem bereits Prozesse und Methoden, die weiterentwickelt werden sollten.[19]

[19] Bitkom Positionen zum Thema:
Nachvollziehbarkeit von Algorithmen: https://www.bitkom.org/Bitkom/Publikationen/Blick-Blackbox-Nachvollziehbarkeit-KI-Algorithmen-Praxis
Und Transparenzanforderungen bei Machine Learning:
https://www.bitkom.org/Bitkom/Publikationen/Machine-Learning-und-die-Transparenzanforderungen-der-DS-GVO.html

Empfehlung 39:
Die DEK erachtet es als sinnvoll, mit Blick auf das Schädigungspotenzial algorithmischer Systeme in einem ersten Schritt fünf Kritikalitäts-Stufen zu unterscheiden. Auf der untersten Stufe (Stufe 1) von Anwendungen ohne oder mit geringem Schädigungspotenzial besteht keine Notwendigkeit einer besonderen Kontrolle oder von Anforderungen, die über die allgemeinen Qualitätsanforderungen, welche auch für Produkte ohne algorithmische Elemente gelten, hinausgehen.

Bitkom Einschätzung:
Die pauschale Einordnung in 5 Stufen bewerten wir kritisch. Für problematisch halten wir, dass die Beschreibung der Stufen so nicht operationalisierbar ist, insbesondere vor dem Hintergrund der Frage, wie die einzelnen Kritikalitätsstufen von „gewissem", „regelmäßigen oder deutlichen" und „erheblichen" Schädigungspotential voneinander abzugrenzen sind. Es sollte auch das durchaus geminderte Risiko der durch KI ersetzten (menschlichen) Tätigkeit berücksichtigt werden. Auch ist stets der begleitende Prozess des Einsatzes wichtig (Anfechtbarkeit, Revidierbarkeit). Es könnte helfen, entlang vordefinierter Schutzziele und Use Cases algorithmische Systeme zu entwickeln. Unter anderem könnten auch Entwickler anhand der intendierten Nutzung des Algorithmus den Schutzbedarf abstecken.

Wir halten es nicht für zielführend, wenn nur vom abstrakten Schädigungspotential gesprochen wird und eine Berücksichtigung der Wahrscheinlichkeit des Eintritts nicht vorgesehen scheint. Üblicherweise wird bei Risikoabschätzungen immer die Schwere des möglichen Schadens sowie dessen Eintrittswahrscheinlichkeit berücksichtigt. Auch bleibt unklar, was der Mehrwert bzw. die Abgrenzung zur Risikobewertung und Datenschutzfolgenabschätzung nach der DS-GVO sein wird (jedenfalls, wenn personenbezogene Daten involviert sind). Das im Abschlussbericht genannte Beispiel im „grünen" Bereich wird durch das genannte Beispiel völlig entwertet – Regulierung sollte hier noch gar nicht ansetzen.
Aus unserer Sicht ist eine Risiko-Matrix sinnvoller, die die Risikoeinschätzung auch nach Einsatzgebieten und Weiterentwicklungsmöglichkeiten differenzieren, Einsatzgebiete unterscheiden kann (s.o.).

Empfehlung 40:
Bei Anwendungen mit einem gewissen Schädigungspotenzial (Stufe 2) kann und soll bedarfsgerechte Regulierung einsetzen, wie etwa Ex-post- Kontrollen, die Pflicht zur Erstellung und Veröffentlichung einer angemessenen Risikofolgenabschätzung, Offenlegungspflichten

gegenüber Aufsichtsinstitutionen oder auch gesteigerte Transparenzpflichten sowie Auskunftsrechte für Betroffene.

Bitkom Einschätzung:
Aus unserer Sicht bleibt hier die wichtige Frage ungeklärt, was ein „gewisses" Schädigungspotential ausmachen soll. Rechtfertigt dies allein auch schon zusätzliche Maßnahmen beim Unternehmen? Risikofolgeabschätzungen sind aufwändig und kein kleiner Eingriff, wenn sie ernst genommen werden: Wie wir bei der Datenschutzfolgenabschätzung gelernt haben, sind solche Abschätzungen bei etablierten Verfahren auch irgendwann redundant – sie machen nur beim Einsatz neuer Verfahren zu neuen Zwecken Sinn und sollten nicht generell für jede Anwendung in jedem Kontext (egal wie bekannt und erprobt) gelten. Wir sehen es daher kritisch, dass auf so früher Stufe Regulierung greifen soll. Auch sind die entsprechenden Kosten zu beachten, die bei KMU und Startups im Rahmen eines solchen Prüfprozesses relativ zu größeren Unternehmen deutlich höher anfallen. Das behindert Innovation und Chancen des Einsatzes von Algorithmen. Insgesamt wird so eine starke Imbalance zwischen Innovation & Chancen auf der einen Seite und Sicherheit & Kontrolle auf der anderen Seite erzeugt.

Empfehlung 41:
Bei Anwendungen mit regelmäßigem oder deutlichem Schädigungspotenzial (Stufe 3) können zusätzlich Zulassungsverfahren gerechtfertigt sein. Bei Anwendungen mit erheblichem Schädigungspotenzial (Stufe 4) fordert die DEK darüber hinaus verschärfte Kontroll- und Transparenzpflichten bis hin zu einer Veröffentlichung der in die algorithmische Berechnung einfließenden Faktoren und deren Gewichtung, der Datengrundlage und des algorithmischen Entscheidungsmodells sowie die Möglichkeit einer kontinuierlichen behördlichen Kontrolle über eine Live-Schnittstelle zum System.

Bitkom Einschätzung:
Auch hier stellen sich die vorgenannten Fragen: Wie wird ein Stufe 3 bzw. Stufe 4 Zulassungsverfahren konkret aussehen? Bezüglich Stufe 4 wäre dringend zu erörtern wem gegenüber diese weitreichenden Offenlegungen erfolgen müssten und wie hier eine angemessene Balance zwischen Wahrung von Geschäftsgeheimnissen/IP und Sicherheit & Kontrolle erfolgen soll.

Empfehlung 42:
Bei Anwendungen mit unvertretbarem Schädigungspotenzial (Stufe 5) ist schließlich ein vollständiges oder teilweises Verbot auszusprechen.

Bitkom Einschätzung:
Ohne eine Definition dazu, wie eine Klassifizierung nach Stufe 5 vorzunehmen wäre sehen wir die Einordnung kritisch. Nach welchen Kriterien soll entschieden werden, ob ein vollständiges oder teilweises Verbot erfolgt?

Empfehlung 43:
Zur Umsetzung der durch die DEK vorgeschlagenen Maßnahmen empfiehlt die DEK eine Regulierung algorithmischer Systeme durch allgemeine horizontale Vorgaben im Recht der Europäischen Union (Verordnung für Algorithmische Systeme, EUVAS). Dieser horizontale Rechtsakt sollte die zentralen Grundprinzipien für algorithmische Systeme enthalten, wie sie die DEK als Anforderungen an algorithmische Systeme entwickelt hat. Insbesondere sollte er im Lichte der Systemkritikalität allgemeine materielle Regelungen zur Zulässigkeit und Gestaltung algorithmischer Systeme, zur Transparenz, zu Betroffenenrechten, zu organisatorischen und technischen Absicherungen und zu den Institutionen und Strukturen der Aufsicht bündeln. Der horizontale Rechtsakt sollte auf der Ebene der EU und der Mitgliedstaaten eine sektorale Konkretisierung erfahren, die wiederum am Gedanken der Systemkritikalität orientiert ist.

Bitkom Einschätzung:
Auch hier lässt der Abschlussbericht wichtige Fragen ungeklärt. Sind Algorithmen etwas derart neues, das in diesem frühen Stadium neue horizontale Vorgaben notwendig sind? An welchen Stellen reicht der existierende Rechtsrahmen konkret nicht aus? Wenn eine solche Kombination aus neuer europäischer horizontaler Regulierung und sektoraler Konkretisierung eben dieser geplant ist, entsteht ein vollständig neues rechtliches Framework. Wie können neue Rechtsunsicherheiten und ungewünschte Wechselwirkungen mit bestehendem Recht vermieden werden?
Es ist außerdem fraglich, welcher Mehrwert generiert wird, wenn die von der DEK genannten Grundprinzipien in einer europäischen Verordnung flächendeckend für die Entwicklung und den Einsatz von Softwaresystemen vorgeschrieben werden – in der Allgemeinheit sind sie schwer umzusetzen (das sehen wir auch bei Prinzipien der DS-GVO) und teilweise ohnehin in geltenden Regelungen enthalten. Es wäre sinnvoller konkrete Handreichungen zu entwickeln, wie diese Prinzipien verwirklicht werden können (aber nicht auf gesetzlicher Ebene, sondern eher als Verwaltungsvorschriften im öffentlichen Bereich und als Handreichungen für Unternehmen).

Empfehlung 44:
Im Zuge der hier empfohlenen Entwicklung einer EUVAS sollte die Aufgabenverteilung zwischen dieser Regulierung und der DSGVO überdacht werden. Dabei ist zum einen zu berücksichtigen, dass sich spezifische Risiken algorithmischer Systeme für den Einzelnen und für Gruppen auch dann manifestieren können, wenn keine personenbezogenen Daten verarbeitet werden, und dass die Risiken nicht unbedingt solche des Datenschutzes sind, wenn sie etwa das Vermögen, Eigentum, körperliche Integrität oder Diskriminierung betreffen. Zum anderen ist zu bedenken, dass für eine künftige horizontale Regulierung algorithmischer Systeme ein flexibleres, stärker risikoadaptiertes Regulierungsregime als für den Datenschutz in Betracht gezogen werden sollte.

Bitkom Einschätzung:
Grundsätzlich ist es richtig, dass es im Anwendungsbereich der DS-GVO schon Regelungen gibt, die einen Teil der Vorschläge der DEK abdecken, so dass es zu Überschneidungen kämen, würde ergänzende Regulierung in Bezug auf Algorithmen geschaffen. Die DS-GVO betrachtet auch nicht nur „Datenschutz-Schäden", sondern alle Beeinträchtigungen für Rechte und Freiheiten der Betroffenen. Es bedürfte erst einmal der Evidenz, dass darüber hinaus auch bei Verarbeitung nicht-personenbeziehbarer Daten ein Schädigungspotential besteht, das eine zusätzliche Regulierung rechtfertigt. Diese findet sich im Gutachten nicht ausreichend.
Wir sehen es kritisch, dass hier Ausweitung des Rahmens angedacht wird (dass aus den „Fehlern" der Grundverordnung gelernt werden soll und ein risikobasiertes Regulierungsregime angestrebt wird, ist aber natürlich begrüßenswert).

Empfehlung 45:
Die DEK empfiehlt bei algorithmischen Systemen erhöhter Systemkritikalität (ab Stufe 2) eine Kennzeichnungspflicht: Eine solche Pflicht trägt Betreibern auf, deutlich zu machen, wann und in welchem Umfang algorithmische Systeme zum Einsatz kommen (Information über das „Ob"). Eine Kennzeichnungspflicht sollte unabhängig von der Systemkritikalität stets im Falle einer ethisch relevanten Verwechselungsgefahr zwischen Mensch und algorithmischem System bestehen.

Bitkom Einschätzung:
Eine allgemeine Kennzeichnungspflicht halten wir für wenig praktikabel und nicht zielführend. Es wäre ohnehin vorab zu klären, wie eine solche Kennzeichnungspflicht in der Praxis

aussehen könnte.[20] Im Rahmen des BDSG-neu wurde auch eine Regelung zu Versicherungen eingeführt. Neben der eigentlichen Kennzeichnung könnte man die Frage stellen, ob es nicht im Kern darum gehen muss zu wissen, ob eine belastende (!) Entscheidung auf einer jedenfalls automatisierten Verarbeitung beruht? In diesen Fällen könnte man darüber nachdenken, Betroffenen eine Art Recht auf manuelle Prüfung einzuräumen. Welcher Mehrwert entstünde sonst aus dem bloßen Wissen über manuelle oder automatisierte Entscheidung, wenn das Anliegen vollumfänglich erfüllt wurde.
Mindestens genauso wichtig ist eine Aufklärung darüber was ein Algorithmus ist und wie Algorithmen funktionieren (Entmystifizierung). Eine Kennzeichnungspflicht suggeriert, dass es sich um etwas grundsätzlich Gefährliches handelt. Dieser Eindruck, der leider teilweise in der Bevölkerung existiert, darf nicht noch durch die DEK und politisches Handeln verstärkt werden.

Empfehlung 46:
Das Recht einer betroffenen Person auf aussagekräftige Informationen über die „involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen" eines algorithmischen Systems (vgl. DSGVO) sollte nicht nur für vollständig automatisierte Systeme, sondern bereits für Profilbildungen als solche und unabhängig von einer nachgelagerten Entscheidungssituation bestehen. Es sollte – abgestuft nach der Systemkritikalität – künftig auch bereits für algorithmenbasierte Entscheidungen greifen. Dazu sollte teilweise eine gesetzliche Klarstellung und teilweise eine Erweiterung der Regelung auf europäischer Ebene erfolgen.

Bitkom Einschätzung:
Diese Thematik wurde umfassen im Prozess der Schaffung der DS-GVO diskutiert und ist aus guten Gründen dort nicht verankert worden. Wie solle dies auch praktisch operationalisiert und die Balance zwischen den entgegenstehenden Rechten ausgewogen in ein Regulierungssystem überführt werden?

Empfehlung 47:
In bestimmten Bereichen kann es sachgerecht sein, dem Betreiber algorithmischer Systeme zusätzlich zur allgemeinen Erläuterung der Logik (Vorgehensweise) und Tragweite des Systems eine individuelle Erklärung der getroffenen Entscheidung abzuverlangen. Wesentlich ist dabei, dass betroffene Personen verständlich, relevant und konkret informiert werden. Die DEK begrüßt daher die technischen Bemühungen, die Erklärbarkeit algorithmischer (insbe-

[20] Zur Kennzeichnung sich dynamisch entwickelnder Produkte siehe hier: https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Stellungnahme-zum-IT-Sicherheitskennzeichen

sondere selbstlernender) Systeme zu stärken („Explainable AI"), und empfiehlt der Bundesregierung, die weitere Forschung und Entwicklung in diesem Bereich zu fördern.

Bitkom Einschätzung:
Wir halten Forschungs- und Entwicklungsförderung in diesem Bereich für sinnvoll, neue Regulierung sollte aber nur in wenigen, kritischen Bereichen erfolgen (zur Frage der Risikobewertung s.o.). Individuelle Erklärungen und Erläuterungen können nur soweit gewährleistet werden, wie das technisch und operationell und unter Abwägung der entgegenstehenden Rechte und Interessen möglich sowie sachgerecht ist.[21]

Empfehlung 48:
In bestimmten Sektoren, in denen nicht nur individuelle, sondern in besonderem Maße auch gesellschaftliche Interessen berührt sind, sollten auch nicht unmittelbar betroffene Personen ein Recht auf Zugang zu bestimmten Informationen über die algorithmischen Systeme erhalten. Entsprechende Rechte werden in erster Linie für journalistische und Forschungszwecke infrage kommen und sind zudem mit Blick auf die betroffenen Interessen der Betreiber durch hinreichende Schutzmaßnahmen zu flankieren. Unter Umständen, insbesondere beim staatlichen Einsatz von algorithmischen Systemen mit einem erheblichen Schädigungspotenzial (Stufe 4), kommen nach Ansicht der DEK darüber hinaus auch voraussetzungslose Informationszugangsansprüche in Frage.

Bitkom Einschätzung:
Bezüglich dieser Empfehlung der DEK wäre aus unserer Sicht zunächst zu beantworten, inwiefern die aktuelle Rechtslage nicht ausreicht um die „Stufe 4 Algorithmen" zu regulieren. In jedem Fall ist die Abwägung und Ausbalancierung zwischen Geschäftsgeheimnissen und Offenlegungspflichten zu wahren.

Empfehlung 49:
Bei algorithmischen Systemen ab einem gewissen Schädigungspotenzial (ab Stufe 2) ist es sachgerecht und zumutbar, dem Betreiber gesetzlich die Erstellung und Veröffentlichung einer angemessenen Risikofolgenabschätzung abzuverlangen, die auch bei der Verarbeitung nicht-personenbezogener Daten greift und Risiken außerhalb des Datenschutzes berücksichtigt. Sie sollte insbesondere auch eine Abschätzung der Risiken für Selbstbestimmung, Privatheit, körperliche Unversehrtheit, persönliche Integrität sowie Vermögen, Eigentum und Diskriminierung umfassen. Außerdem sollte sie neben den zugrundeliegenden Daten und der

[21] Bitkom Leitfaden zum Thema:
https://www.bitkom.org/Bitkom/Publikationen/Blick-Blackbox-Nachvollziehbarkeit-KI-Algorithmen-Praxis

Logik des Modells auch Qualitätsmaße und Fairnessmaße zu den Daten und zur Modellgüte berücksichtigen, etwa zu Bias oder (statistischen) Fehlerquoten (insgesamt oder für bestimmte Teilgruppen), die ein System bei der Vorhersage/ Kategorienbildung aufweist.

Bitkom Einschätzung:

Auch hier stellen sich die bereits oben angesprochenen offenen Fragen: Wer prüft eine „angemessene" Risikofolgenabschätzung in der Praxis? Wer definiert und prüft Qualitäts- und Fairnessmaße? Wer definiert Kriterien der Modellgüte und wer prüft diese? Wir halten eine Fortsetzung der Diskussion rund um diese Fragen für essentiell.

Empfehlung 50:

Die Anforderungen an Dokumentation und Protokollierung in Bezug auf die verwendeten Datensätze und Modelle, die Granularität, die Aufbewahrungszeiten und die Verwendungszwecke sollten konkretisiert werden, damit die Verantwortlichen und Auftragsverarbeiter Rechtsklarheit erhalten. Zum anderen sollte für sensible Anwendungen künftig eine Pflicht etabliert werden, die Programmabläufe einer Software, die nachhaltige Schäden verursachen können, zu dokumentieren und zu protokollieren. Die verwendeten Datensätze und Modelle sind so zu beschreiben, dass diese für Aufsichtsinstitutionen im Falle einer Kontrolle nachvollziehbar sind (etwa hinsichtlich der Herkunft und Aufbereitung von Datensätzen oder der Optimierungsziele der Modelle).

Bitkom Einschätzung:

Wir sehen diese Empfehlung kritisch, da die Umsetzung in der Praxis extrem zeitaufwendig und ressourcenintensiv sein wird und Nachvollziehbarkeit auch auf anderen Wegen hergestellt werden könnte. Die Aufwände müssen hier in Relation zum erstrebten Zweck gesetzt werden.

Empfehlung 51:

Der Normgeber sollte Betreibern ein Mindestmaß an technischen und mathematisch-prozeduralen Qualitätsgarantien abverlangen, welche die Korrektheit und Rechtmäßigkeit der algorithmisch ermittelten Ergebnisse durch Verfahrensvorgaben absichern. Dazu können insbesondere Vorgaben für Korrektur- und Kontrollmechanismen oder für die Datenqualität sowie die Sicherheit des Systems gehören. So wäre es beispielsweise sachgerecht, qualitative Anforderungen an das Verhältnis zwischen der Datengrundlage und dem Ergebnis des algorithmischen Datenverarbeitungsprozesses vorzugeben.

Bitkom Einschätzung:
Die Richtigkeit der algorithmischen Entscheidung nachvollziehbar zu machen kann das Vertrauen in die Systeme maßgeblich erhöhen. Allerdings stellt sich die Frage, wie ein solches „Mindestmaß" an technischen und mathematisch prozeduralen Qualitätsgarantien konkret ausgestaltet werden kann? Wer definiert das Mindestmaß und wer kontrolliert es?

Empfehlung 52:
Beim Einsatz algorithmischer Systeme im Kontext menschlicher Entscheidungen sieht die DEK zunächst Klarstellungs- und Konkretisierungsbedarf betreffend die Anwendungsvoraussetzungen und Rechtsfolgen von Art. 22 DSGVO. Darüber hinaus empfiehlt die DEK, Schutzmechanismen auch für algorithmenbasierte und -getriebene Entscheidungssysteme vorzusehen, da sich der Einfluss dieser Systeme in der Praxis nahezu ebenso stark auswirken kann wie bei algorithmendeterminierten Anwendungen. Diesbezüglich empfiehlt sich anstelle des von Art. 22 DSGVO bislang verfolgten Verbotsprinzips ein flexibleres, risikoadaptiertes Regulierungsregime, das dem Einzelnen angemessene Schutzgarantien (insbesondere im Falle von Profiling) und Verteidigungsmöglichkeiten gegen Fehler und Bedrohungen seiner Rechte vermittelt.

Bitkom Einschätzung:
Das risikobasierte Prinzip ist aus unserer Sicht eher zu begrüßen als ein generelles Verbotsprinzip; daraus sollte aber nicht reflexartig neue Regulierung entstehen (konkreter Regelungsbedarf ist stets vorab zu prüfen).

Empfehlung 53:
Es ist erwägenswert, den Anwendungsbereich des Antidiskriminierungsrechts in situativer Hinsicht auf Diskriminierungen auszudehnen, die auf einer automatisierten Datenauswertung oder einem automatisierten Entscheidungsverfahren beruhen. Der Gesetzgeber sollte darüber hinaus Maßnahmen eines wirksamen Schutzes gegen Diskriminierungen aufgrund von Gruppenmerkmalen etablieren, die an sich nicht zu den gesetzlich geschützten Diskriminierungsmerkmalen zählen, und bei denen Diskriminierungen derzeit vielfach auch nicht als mittelbare Diskriminierung aufgrund eines geschützten Merkmals qualifiziert werden können.

Bitkom Einschätzung:

Im Medienstaatsvertrag der Länder befindet sich eine Vorgabe zur Diskriminierungsfreiheit, sowohl für Medienplattformen als auch für Medienintermediäre.[22]
Natürlich darf es nicht zu unzulässigen Diskriminierungen kommen. Zwischen den jeweiligen Regulierungsobjekten ist in jedem Fall aber eine differenzierte Betrachtung und Einzelfallbewertung erforderlich, denn es bestehen erhebliche funktionale Unterschiede.
Generell ist festzustellen, dass es absolute Neutralität und objektiv korrekte Darstellung nicht geben kann: Die schiere Masse der Inhalte macht eine gewisse Ungleichbehandlung im Interesse des Nutzers zwingend erforderlich. Insoweit bemühen sich die Anbieter jedoch bereits im eigenen wirtschaftlichen Interesse darum, das subjektiv beste Ergebnis zu liefern, um den Nutzer nicht an die Konkurrenz zu verlieren. Den Medienintermediären sollte bei der Gestaltung ihrer Algorithmen ein weiter Entscheidungsspielraum zugestanden werden.
Eine Alternative zu einem zu tiefen regulatorischen Eingriff könnte es sein, dass Anbieter Lösungen anbieten, sodass Suchergebnisse und Newsfeeds auch ohne nutzerbasierte Priorisierung angezeigt werden können.

Empfehlung 54:

Zusätzlich zu bereits bestehender Regulierung ist es für algorithmische Systeme mit deutlichem oder regelmäßigem (Stufe 3) oder sogar erheblichem Schädigungspotenzial (Stufe 4) sinnvoll, Zulassungsverfahren oder Vorabprüfungen von algorithmischen Systemen durch Aufsichtsinstitutionen zu etablieren, um Schäden für einzelne Betroffene, Bevölkerungsgruppen oder die Gesellschaft als Ganzes abzuwenden.

Bitkom Einschätzung:

Hierzu muss vorab eine Klassifizierung erfolgen ob ein Algorithmus Stufe 3 oder 4 zuzuordnen ist. Soll diese zB in Form einer Selbstauskunft oder einer Vorabprüfung erfolgen? Auch stellt sich weiterhin die Frage, wann ein „Schädigungspotenzial" vorliegt? Was ist das Referenzszenario? Ein Algorithmus basiert auf historischen Trainingsdaten. Wenn diese „biased" sind bildet ein Algorithmus die historischen Anwendungen ab. Falls diese z.B. diskriminieren kann es ja sein, dass auch ohne Algorithmen ein (wie auch immer geartetes) Schädigungspotenzial bzw. eine konkrete Schädigung vorliegt?
Diese Überlegung ist wichtig um zu verstehen mit was man den Algorithmus vergleicht/welche Maßstäbe man ansetzt.
Auch sollte erörtert werden, wie die fortlaufende Weiterentwicklung und weiteres Lernen gehandhabt werden kann. Sonst dürften ja theoretisch nur „locked-algorithms" in den

[22] Siehe hierzu auch die Bitkom Stellungnahme zum Medienstaatsvertrag: https://www.bitkom.org/Stellungnahme-Medienstaatsvertrag

Verkehr gebracht werden. Eine entsprechende Aufsichtsbehörde müsste daher dauerhaft und fortlaufend prüfen.

Empfehlung 55:
Die DEK empfiehlt der Bundesregierung, die bestehenden Aufsichtsinstitutionen und -strukturen im Rahmen ihrer Zuständigkeit zu stärken, neu auszurichten und, wo erforderlich, auch neue Institutionen und Strukturen zu schaffen. Dabei sollten die behördlichen Aufsichtsaufgaben und Kontrollbefugnisse primär jeweils denjenigen sektoralen Aufsichtsbehörden zugewiesen werden, die bereits sektorspezifische Sachkompetenzen ausgebildet haben. Von großer Bedeutung ist es dabei, dass die zuständigen Behörden mit den erforderlichen finanziellen, personellen und technischen Ressourcen ausgestattet werden.

Bitkom Einschätzung:
Die erforderlichen finanziellen, personellen und technischen Ressourcen sind dann sinnvoll, wenn es einem angemessenen und hochwertigen Verständnis der zu regulierenden Materie dient. So kann eine sachgerechte Regulierung (oder eben ggf. keine Regulierung) mit Augenmaß erreicht werden. Das Anknüpfen an sektoral ausgebildeten Kompetenzen und bestehenden Strukturen von Aufsichtsinstitutionen ebenfalls sinnvoll. Insgesamt halten wir die Stärkung vorhandener Instrumentarien für sinnvoll und zielführender zur Durchsetzung existierender Regulierung.
Es ist aber zu berücksichtigen, dass bei der Breite der angedachten Regulierung auf jeden Fall auch Sachverhalte erfasst würden, die momentan keiner speziellen Aufsicht unterliegen. Damit würde erheblicher Mehrbedarf an behördlicher Kontrolle geschaffen. Es könnte außerdem zu unterschiedlichen Beurteilungen der eingesetzten Tools im Rahmen von kontextbezogenen, sektorspezifischen Prüfungen kommen, die sich nicht nur auf den sektorspezifischen Einsatz, sondern auch auf generelle Transparenz und Designvorgaben beziehen. Das würde u.U. für die Hersteller widersprüchliche Anforderungen an die Grundkonzeption bedeuten.

Empfehlung 56:
Darüber hinaus empfiehlt die DEK der Bundesregierung die Schaffung eines bundesweiten Kompetenzzentrums Algorithmische Systeme, welches die sektoralen Aufsichtsbehörden durch technischen und regulatorischen Sachverstand in ihrer Aufgabe unterstützt, algorithmische Systeme im Hinblick auf die Einhaltung von Recht und Gesetz zu kontrollieren.

Bitkom Einschätzung:
Dies erscheint sinnvoll, wenn es um den Aufbau von Kompetenzen des Verständnisses der Funktionsweise von Algorithmischen Systemen geht. So kann eine praxisnahe und sachgerechte Regulierung bzw. an einigen Stellen keine Regulierung erreicht werden.

Empfehlung 57:
Aus Sicht der DEK sollten Initiativen unterstützt werden, die – ggf. differenziert nach kritischen Anwendungsbereichen – technisch-statistische Standards für die Qualität von Testverfahren und Audits festlegen. Für die Überprüfbarkeit algorithmischer Systeme können derartige Testverfahren künftig eine zentrale Rolle spielen, wenn sie hinreichend aussagekräftig, verlässlich und sicher ausgestaltet sind.

Bitkom Einschätzung:
Wenn diese technisch-statistischen Standards neutral, praxisnah und hochwertig sind, kann dies ein tatsächlicher Mehrwert sein, um Verständnis, Vertrauen und Akzeptanz in die Funktionsweise algorithmischer Systeme zu erhöhen.

Empfehlung 58:
Innovative Formen der Ko- und Selbstregulierung verdienen aus Sicht der DEK neben und in Ergänzung zu staatlichen Formen der Regulierung besondere Aufmerksamkeit. Die DEK empfiehlt der Bundesregierung die Prüfung verschiedener Modelle der Ko- und Selbstregulierung, die für bestimmte Konstellationen adäquate Antworten liefern können.

Bitkom Einschätzung:
Wir teilen die Empfehlung der DEK grundsätzlich. Ko- und Selbstregulierung sollten stärker gefördert und als alternative Regulierungsinstrumente häufiger eingesetzt werden. Sie haben den Vorteil, dass sie deutlich schnellere Entwicklung möglich machen und praxisnähere Ausgestaltung gewährleisten können.

Empfehlung 59:
Die DEK hält es für erwägenswert, den Betreibern – nach dem Regulierungsmodell „Comply or Explain" – die gesetzliche Pflicht aufzuerlegen, sich zu den Regeln eines Algorithmic Accountability Codex zu bekennen. Die Erarbeitung eines solchen bindenden Codex für die Betreiber von algorithmischen Systemen könnte dabei durch eine unabhängige, paritätisch besetzte Kommission erfolgen, die nicht unter staatlichem Einfluss stehen dürfte. Vertreter der Zivilgesellschaft sollten bei der Erarbeitung eines solches Codex in angemessener Weise beteiligt werden.

Bitkom Einschätzung:

Die Entwicklung eines Algorithmic Accountability Codex kann eine vertrauensstiftende Maßnahme sein. Allerdings sollte die Mitzeichnung auf freiwilliger Basis erfolgen, wie dies zB auch bei anderen Corporate Digital Responsibility Maßnahmen[23] der Fall ist. Wir halten es darüber hinaus für fraglich, ob ein horizontaler Codex tatsächlich möglich ist – dies sollte zunächst in Anlehnung an bekannte Code of Conduct Strukturen sorgfältig geprüft werden. Auf freiwilliger Basis kann ein Codex attraktiv/interessant sein, um auf Basis eines etablierten Codex-Regelwerkes Vertrauen und Akzeptanz in die Wirkungsweise und Anwendung meiner Systeme zu erzeugen. Rechtlich verpflichtend sollte für Unternehmen die Algorithmen einsetzen nur die geltende bestehende Rechtslage sein. Der bestehende Rechtsrahmen reicht aus um Diskriminierungen und weitere mögliche Schädigungen zu verhindern.

Empfehlung 60:

Auch ein spezifisches Gütesiegel als freiwilliges oder verpflichtendes Schutzzeichen kann Verbrauchern Orientierung über vertrauenswürdige algorithmische Systeme geben und gleichzeitig marktwirtschaftliche Anreize für Entwickler und Betreiber setzen, vertrauenswürdige Systeme zu entwickeln und zu verwenden.

Bitkom Einschätzung:

Die Digitalwirtschaft steht freiwilligen Kennzeichnungen zur Erhöhung der Transparenz und als vertrauensstiftende Maßnahme grundsätzlich positiv und offen gegenüber. Transparenz ist für den Verbraucher ein notwendiger Baustein der Vertrauensbildung - dies unterstützen wir. Kennzeichnungspflichten, sofern sie für einzelne Anwendungen/produktgruppen tatsächlich notwendig sind, können darüber hinaus nur europäisch adressiert werden (nationale Kennzeichnungspflicht wäre Marktzugangsbeschränkung, die eine verpflichtende Kennzeichnung auf nationaler Ebene wohl ausschließen dürfte).[24]

Empfehlung 61:

Ähnlich wie schon heute Unternehmen ab einer bestimmten Größe einen Datenschutzbeauftragten benennen müssen, sollten nach Auffassung der DEK künftig auch solche Unternehmen und Behörden, die kritische algorithmische Systeme betreiben, einen Ansprechpartner

[23] Siehe zb die Bitkom Empfehlungen zu CDR und Automatic Decision Making: https://www.bitkom.org/Bitkom/Publikationen/Empfehlungen-fuer-den-verantwortlichen-Einsatz-von-KI-und-automatisierten-Entscheidungen-Corporate-Digital-Responsibility-and-Decision-Making.html.

[24] Bitkom Position zum Thema (bezüglich Sicherheitskennzeichen): https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Stellungnahme-zum-IT-Sicherheitskennzeichen

benennen müssen. Er soll für die Kommunikation mit Behörden zur Verfügung stehen und zu einer Mitwirkung verpflichtet sein.

Bitkom Einschätzung:
Beauftragte mit besonderer Expertise im Unternehmen zu benennen kann ein probates Mittel darstellen. Allerdings stellt sich die Frage, was die konkreten Rechten und Pflichten eines solchen Beauftragten in der Praxis wären? Es sollte außerdem geprüft werden, ob die Einführung einer zusätzlichen Stelle hierfür wirklich sinnvoll und praxistauglich ist und ob nicht eine Funktionsbündelung mit bereits etablierten Rollen oder Abteilungen im Unternehmen (zB dem DSB) möglich ist. Anstelle eines Beauftragten mit eigenen Kompetenzen könnte so ein interner Ansprechpartner (oder auch Abteilung) aufgebaut und mit bisherigen Aufgaben verknüpft werden. Dies erleichtert die Sachkompetenz und schafft Vertrauen und Standardisierung, ohne dabei mehr überbordende Bürokratie zu schaffen. Außerdem muss in jedem Fall der entstehende Bürokratieaufwand, insbesondere für KMU und Startups im Blick behalten werden.

Empfehlung 62:
Um sicherzustellen, dass bei der behördlichen Überprüfung algorithmischer Systeme auch die Interessen der Zivilgesellschaft und betroffener Unternehmen angemessen berücksichtigt werden, sollten geeignete Beiräte bei den sektoralen Aufsichtsbehörden gebildet werden.

Bitkom Einschätzung:
Interdisziplinär besetzte Gremien zur Ausbalancierung der betroffenen Interessen zu schaffen halten wir für sinnvoll und notwendig. Allerdings ist der Terminus „berechtigte Interessen der Zivilgesellschaft“ sehr unscharf und juristisch nicht abgrenzbar – die damit einhergehende Rechtsunsicherheit würde die Planungssicherheit der Unternehmen damit deutlich beeinträchtigen. Außerdem dürften die dort formulierten Anforderungen nicht über den geltenden Rechtsrahmen hinausgehen. In Anlehnung an Art. 40/41 DS-GVO könnte für alle neu entwickelten freiwilligen Anforderungen, bzw. Rahmenwerke eine Art Anerkennung erfolgen, die dann auch die durchaus sehr positiv Erwähnung findenden Rechtsfolgen (Anreize) auslöst.

Empfehlung 63:
Die DEK stuft technische Standards akkreditierter Normungsorganisationen als ein grundsätzlich sinnvolles Instrument zwischen staatlicher Regulierung und rein privater Selbstregulierung an. Sie empfiehlt daher der Bundesregierung, in geeigneter Weise auf die Entwicklung und Verabschiedung technischer Standards hinzuwirken.

Bitkom Einschätzung:
Grundsätzlich begrüßen wir den hier gesetzten Fokus auf technische Standardisierung. Es sollte nun erarbeitet werden, welche Standards notwendig und wie diese zu priorisieren sind.

Empfehlung 65 und 66:
65: Vor dem Hintergrund der besonderen Gefahren von Medienintermediären mit Torwächterfunktion für die Demokratie empfiehlt die DEK, auch mit Blick auf eine Einwirkung auf den EU- Gesetzgeber (→ siehe oben Empfehlung Nr. 43) zu prüfen, wie den mit einer solchen Torwächterfunktion verbundenen Gefahren begegnet werden kann. Dabei sollte ein ganzes Spektrum gefahrenabwehrender Maßnahmen erwogen werden, das bis hin zu einer Ex-ante-Kontrolle (z. B. in Form eines Lizenzierungsverfahrens) reichen kann.
66: Den nationalen Gesetzgeber trifft die verfassungsrechtliche Pflicht, die Demokratie vor den Gefahren für die freie demokratische und plurale Meinungsbildung, die von Anbietern mit Torwächterfunktion ausgehen, durch Etablierung einer positiven Medienordnung zu schützen. Die DEK empfiehlt, die Anbieter in diesem engen Bereich zum Einsatz solcher algorithmischer Systeme zu verpflichten, die den Nutzern zumindest als zusätzliches Angebot auch einen Zugriff auf eine tendenzfreie, ausgewogene und die plurale Meinungsvielfalt abbildende Zusammenstellung von Beiträgen und Informationen verschaffen.

Bitkom Einschätzung:
Hinsichtlich der Dienste von Intermediären erfordern gravierende regulatorische Eingriffe zunächst den empirischen Beleg für den Regelungsbedarf im Hinblick auf ihre Meinungsbildungsrelevanz. Die verschiedenen Medienintermediäre sind untereinander nur bedingt vergleichbar, erfüllen sie doch für Nutzerinnen und Nutzer ganz unterschiedliche Zwecke. Bitkom sieht grundsätzlich keine von Medienintermediären ausgehende größere Gefährdungssituation der Meinungsvielfalt als bspw. von Rundfunkanbietern auch.
Wer würde potentiell die Inhalte bzw. Kriterien dieses Angebots der tendenzfreien, ausgewogenen, die plurale Medienvielfalt abbildenden Zusammenstellung von Beiträgen festlegen?

Empfehlung 67:
Für alle Medienintermediäre und auch bei Anbietern ohne Torwächterfunktion oder bei geringerem Schädigungspotenzial für die demokratische Meinungsbildung sollte die Bundesregierung Maßnahmen prüfen, die den charakteristischen Gefahren des Mediensektors Rechnung tragen. Dies könnte Mechanismen zur Transparenzsteigerung (z. B. Einblick in

technische Verfahren der Nachrichtenauswahl und -priorisierung, Kennzeichnungspflichten für Social Bots) und ein Recht auf Gegendarstellung in Timelines umfassen.

Bitkom Einschätzung:
Transparenzverpflichtungen und Kennzeichnungspflichten für Social Bots befinden sich bereits im Medienstaatsvertrag. Ersteres ebenfalls in der Platform to Business Verordnung. Hier sollte dringend von einer doppelten Regulierung abgesehen werden. Transparenzvorgaben sollten grundsätzlich nie zu einer Verpflichtung der Offenlegung von Algorithmen oder Offenbarung von Geschäftsgeheimnissen führen.

Empfehlung 68:
Der Staat ist im Interesse seiner Bürger zur Nutzung der besten verfügbaren Technik – einschließlich algorithmischer Systeme – verpflichtet, muss dabei jedoch im Lichte seiner Grundrechtsbindung sowie der Vorbildfunktion allen staatlichen Handelns besondere Sorgfalt walten lassen. Der Einsatz algorithmischer Systeme durch Hoheitsträger ist daher im Allgemeinen als besonders sensibel im Sinne des Kritikalitätsmodells einzustufen und erfordert mindestens eine umfassende Risikofolgenabschätzung.

Bitkom Einschätzung:
Auch im öffentlichen Raum gibt es weniger kritische Daten und kritischere Daten (z.B. im Geheimschutzbereich). Es sollte eine Differenzierung entlang des Modells geben und nicht direkt für eine „umfassende Risikofolgenabschätzung“ eingeführt werden.

Empfehlung 69:
Aufgaben in der Rechtsetzung und der Rechtsprechung dürfen algorithmischen Systemen allenfalls in Randbereichen übertragen werden. Insbesondere dürfen algorithmische Systeme nicht genutzt werden, um die freie Willensbildung im demokratischen Prozess und die sachliche Unabhängigkeit der Gerichte zu unterminieren. Große Potenziale für den Einsatz algorithmischer Systeme bestehen hingegen in der Verwaltung, vor allem in der Leistungsverwaltung. Um dem Rechnung zu tragen, sollte der Gesetzgeber verstärkt teil- und vollautomatisierte Verwaltungsverfahren zulassen. Dazu bedarf es auch einer vorsichtigen Fortentwicklung des zu engen § 35a VwVfG sowie der entsprechenden einfachrechtlichen Normen. Bei alledem gilt es, hinreichende Schutzmaßnahmen für die Bürger vorzusehen.

Bitkom Einschätzung:
Algorithmische Systeme sollten bei einer richterlichen Urteilsfindung unterstützen (z.B. durch Analyse bereits ergangener Urteile in vergleichbaren Fallkonstellationen), sie sollten aber richterliche und gesetzgeberische Entscheidungen nicht ersetzen dürfen. Dies wäre

auch mit den geltenden Prinzipien des Grundgesetzes (z.B. Demokratieprinzip, gesetzlicher Richter) nicht vereinbar.
Beispielsweise könnte aber im Verwaltungsverfahren eine Baugenehmigung durchaus vollautomatisiert erfolgen. Die Unterlagen könnten komplett digital eingereicht werden. Wenn ein Verwaltungsakte ausschließlich begünstigt, entsteht kein Nachteil für den Antragsteller. Wenn der Verwaltungsakt teilbelastend ist, kann ein ergänzender Rechtsweg geschaffen werden, etwa ein „Vorwiderspruch" der erstmal nur auf manuelle Entscheidung gerichtet ist und im Weiteren noch nicht materiell oder formell angreift.

Empfehlung 70:
Staatliche Entscheidungen, die unter Nutzung algorithmischer Systeme zustande kommen, müssen transparent und begründbar bleiben. Dazu bedarf es ggf. Klarstellungen bzw. Erweiterungen der bestehenden Informationsfreiheits- und Transparenzgesetze. Ferner entbindet der Einsatz algorithmischer Systeme nicht vom Grundsatz, dass hoheitliche Entscheidungen regelmäßig im Einzelfall begründet werden müssen; im Gegenteil kann dieser Grundsatz dem Einsatz allzu komplexer algorithmischer Systeme Grenzen setzen. Schließlich trägt die Nutzung von Open-Source-Lösungen wesentlich zur Transparenz staatlichen Handelns bei und sollte daher verstärkt angestrebt werden.

Bitkom Einschätzung:
Auch hier sollte differenziert werden – wenn Verwaltungsentscheidungen nach klaren „A" oder „B" Kriterien entschieden werden, steht einer Automatisierung von Entscheidungen bei gleichbleibender Nachvollziehbarkeit im Einzelfall nichts entgegen. Die (positiven oder negativen) Folgen vom Einsatz von Open Source Lösungen hängen davon ab, wie die Kommunikation und Transparenz rund um den Einsatz solcher Systeme gehandhabt wird. Ein zielführender Ansatz aus unserer Sicht ist es, die Digitalisierungstauglichkeit von Gesetzen stets gesondert vorab zu prüfen– so dass algorithmengestützte Entscheidungen überhaupt getroffen werden können. Hier sind auch die Ergebnisse der Enquete KI – PG Staat und KI zu berücksichtigen. Dort wird u.a. geprüft, welche rechtlichen Hürden bestehen, um KI in Verwaltungsentscheidungen einzusetzen.

Empfehlung 72:
Neben strafrechtlicher Verantwortlichkeit und Verwaltungssanktionen ist auch die Haftung auf Schadensersatz unverzichtbarer Bestandteil eines ethisch vertretbaren Ordnungsrahmens. Es ist bereits jetzt erkennbar, dass algorithmische Systeme – u. a. aufgrund der Komplexität und Dynamik der Systeme sowie aufgrund ihrer wachsenden „Autonomie" – das bestehende haftungsrecht vor Herausforderungen stellen. Die DEK empfiehlt daher eine umfassende Prüfung und, soweit erforderlich, Anpassung des geltenden Haftungsrechts. Der

Blick sollte sich dabei nicht allein auf bestimmte technologische Merkmale – wie etwa auf das Merkmal maschinellen Lernens oder Künstlicher Intelligenz – verengen.

Bitkom Einschätzung:
Neue Technologien fordern das Recht immer heraus und geben Anlass, über die noch bestehende Angemessenheit und Zielgenauigkeit geltender Rechtsvorschriften nachzudenken. Das bedeutet aber nicht, dass bewährtes Recht komplett revidiert werden müsste. Es muss aber so zugeschnitten werden, dass Vorschriften auch auf neue Technologie entsprechend ihrem Normzweck Anwendung finden können. Normzweck von Haftungsvorschriften ist aber nicht, die Entwicklung neuer Technologien zu verhindern, sondern deren spezifische Risiken und Gefährdungspotenziale zu begrenzen. In diesem Sinn darf keine Haftungsfolge an den Einsatz von algorithmischen Systemen an sich geknüpft werden, sondern nur an eine Rechtsgutsverletzung durch solche Systeme. Das derzeitige Haftungsregime des Zivilrechts ist bereits in der Lage, die aktuell denkbaren Haftungsszenarien vollumfänglich abzubilden.

Empfehlung 73:
Der Gedanke, algorithmischen Systemen hoher Autonomie künftig Rechtspersönlichkeit zuzuerkennen und sie selbst für Schäden haften zu lassen („elektronische Person"), sollte nicht weiterverfolgt werden. Soweit dieser Gedanke auf eine Analogie zwischen Mensch und Maschine gestützt wird, ist er schon ethisch nicht vertretbar, und soweit es schlicht um die Anerkennung einer neuen Gesellschaftsform im Sinne des Gesellschaftsrechts geht, löst er keine Probleme.

Bitkom Einschätzung:
Bitkom steht Überlegungen zur Einführung einer neuen Rechtsfigur „elektronische Person" ebenfalls ablehnend gegenüber. Es kann nicht im Sinne von Gesetzgeber und Gesellschaft sein, der Delegation von Verantwortung auf KI-Systeme Vorschub zu leisten. Solange (natürliche oder juristische) Personen für die Folgen des Einsatzes von KI haftbar bleiben, besteht ein Eigeninteresse des möglicherweise Haftenden, die KI und ihre Ergebnisse zu kontrollieren und Schadensrisiken zu minimieren. Es ist auch nicht erkennbar, wie die Schaffung einer elektronischen Rechtspersönlichkeit einen Schadensausgleich erleichtern oder Haftungsprobleme beseitigen könnte. Haftungsverantwortlichkeiten lassen sich bereits durch Haftungsgrundlagen und Zurechnungsnormen des geltenden Rechts zuweisen. Neue Regelungen für elektronische Personen werden sich kaum bruchlos und widerspruchsfrei in das Geflecht der geltenden Haftungsregelungen einfügen lassen, die im Grundsatz auf Willensfreiheit, Pflichtverletzung und Verschulden beruhen.

Empfehlung 74:
Dagegen ist es geboten, für den Einsatz sog. Autonomer Systeme – abhängig von der Natur der dem System übertragenen Aufgaben – auch eine Zurechnung schädigender Vorgänge entsprechend den Regelungen über die Haftung für Gehilfen (vgl. insbes. § 278 BGB) vorzunehmen. Beispielsweise sollte eine Bank, die sich für die Prüfung der Kreditwürdigkeit eines autonomen Systems bedient, gegenüber ihrem Kunden mindestens in gleichem Maße haften, wie wenn sie sich eines menschlichen Mitarbeiters bedient hätte.

Bitkom Einschätzung:
Wir halten diese Aussage für diskussionswürdig. Es sollte die Frage geklärt werden, was anstelle des Verschuldens bei § 278 BGB treten sollte bzw. ob nicht das Deliktsrecht hierfür bereits einen ausreichenden Rahmen bildet. Das Konzept mutet insgesamt fremdartig an und impliziert, dass die Maschine hier selbstständig und mit einem Menschen vergleichbar handelt. Auch ist es schwierig, Begriffe wie etwa Fahrlässigkeit auf dieses Konzept zu übertragen.

Empfehlung 75:
Daneben erscheint es nach derzeitigem Stand der Diskussion sehr wahrscheinlich, dass zusätzlich zu einer sachgerechten Anpassung der aus den 1980er Jahren stammenden Produkthaftungsrichtlinie und Verknüpfung mit neuen Standards der Produktsicherheit auch punktuelle Modifikationen der Verschuldenshaftung und/oder neue Tatbestände der Gefährdungshaftung erforderlich sein werden. Dabei wird jeweils zu klären sein, für welche Produkte, digitalen Inhalte und digitalen Dienstleistungen welches Haftungsregime sachgerecht und wie dieses konkret auszugestalten ist, wobei es wiederum wesentlich u. a. auf die Kritikalität des betreffenden algorithmischen Systems ankommen wird. Dabei sollten auch innovative Haftungskonzepte, wie sie derzeit auf europäischer Ebene entwickelt werden, in Betracht gezogen werden.

Bitkom Einschätzung:
Änderungen des Produktsicherheits- und des Produkthaftungsrechts werden derzeit auf verschiedenen Ebenen diskutiert (vor allem auf EU-Ebene). Die Ergebnisse dieser Diskussionen sollten abgewartet werden. Grundsätzlich ist das geltende Haftungsrecht für die Belange der Datenökonomie gut aufgestellt und muss nicht grundlegend geändert werden. Insbesondere sind bisher keine gravierenden Haftungslücken entstanden. Die Einführung eines allgemeinen Gefährdungshaftungstatbestandes für algorithmische Systeme ist jedenfalls nicht gerechtfertigt und würde die Entwicklung solcher Systeme in Europa empfindlich zurückwerfen. Die Gefährdungshaftung ist in der Rechtsordnung nur für außer-

gewöhnlich gefährliche Tätigkeiten reserviert. Bei den allermeisten Applikationen wird das nicht zutreffen. Eine pauschale Erhöhung des Haftungsmaßstabes würde für Unternehmen ein riesiges, zusätzliches Wirtschaftsrisiko mit sich bringen. Dies könnte sowohl die Entwicklung als auch die Verwendung nützlicher Applikationen verhindern.