STIFTUNG DATENSCHUTZ

Die KI-Empfehlungen der Datenethikkommission aus Sicht der Datenschutzaufsicht

Marit Hansen

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

DatenTag, 13.12.2021

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

Bild: Dariusz Staniszewski via Pixabay

1. Die Datenethikkommission
2. Die (KI-)Empfehlungen der Datenethikkommission
3. Die Sicht der Datenschutzaufsicht
4. Was noch?
5. Fazit

Auftrag

Koalitionsvertrag 2018

„Wir werden zeitnah eine Daten-Ethikkommission einsetzen, die Regierung und Parlament innerhalb eines Jahres einen Entwicklungsrahmen für Datenpolitik, den Umgang mit Algorithmen, künstlicher Intelligenz und digitalen Innovationen vorschlägt. Die Klärung datenethischer Fragen kann Geschwindigkeit in die digitale Entwicklung bringen und auch einen Weg definieren, der gesellschaftliche Konflikte im Bereich der Datenpolitik auflöst."

Leitfragen zu:

I. „algorithmic decision making" = ADM

II. KI

III. Daten

Gefragt: ethische Leitlinien, rechtliche Vorschläge

Definition „Datenethik"?

Mitglieder der Datenethikkommission

Philosophie

Theologie

vzbv
(VWL)

BfDI
(**Jura**, Informatik)

BDI
(BWL / **Jura**)

Medizinethik

Jura

Informatik
+ Statistik

„Gateway-Personen"

Bild: BMI

Aufgabe und Ergebnis – was und was nicht?

JA

- Auftrag und mehr, Leitlinien
- Anhörung von Expert*innen, öffentl. Veranstaltungen
- Nachvollziehbarkeit der Meinungen
- Formulierungen, bis alles für alle ausreichend okay, Zustimmung

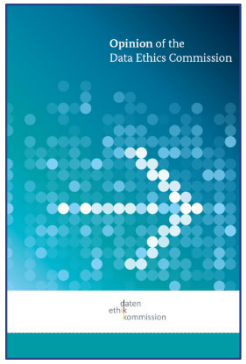
NEIN

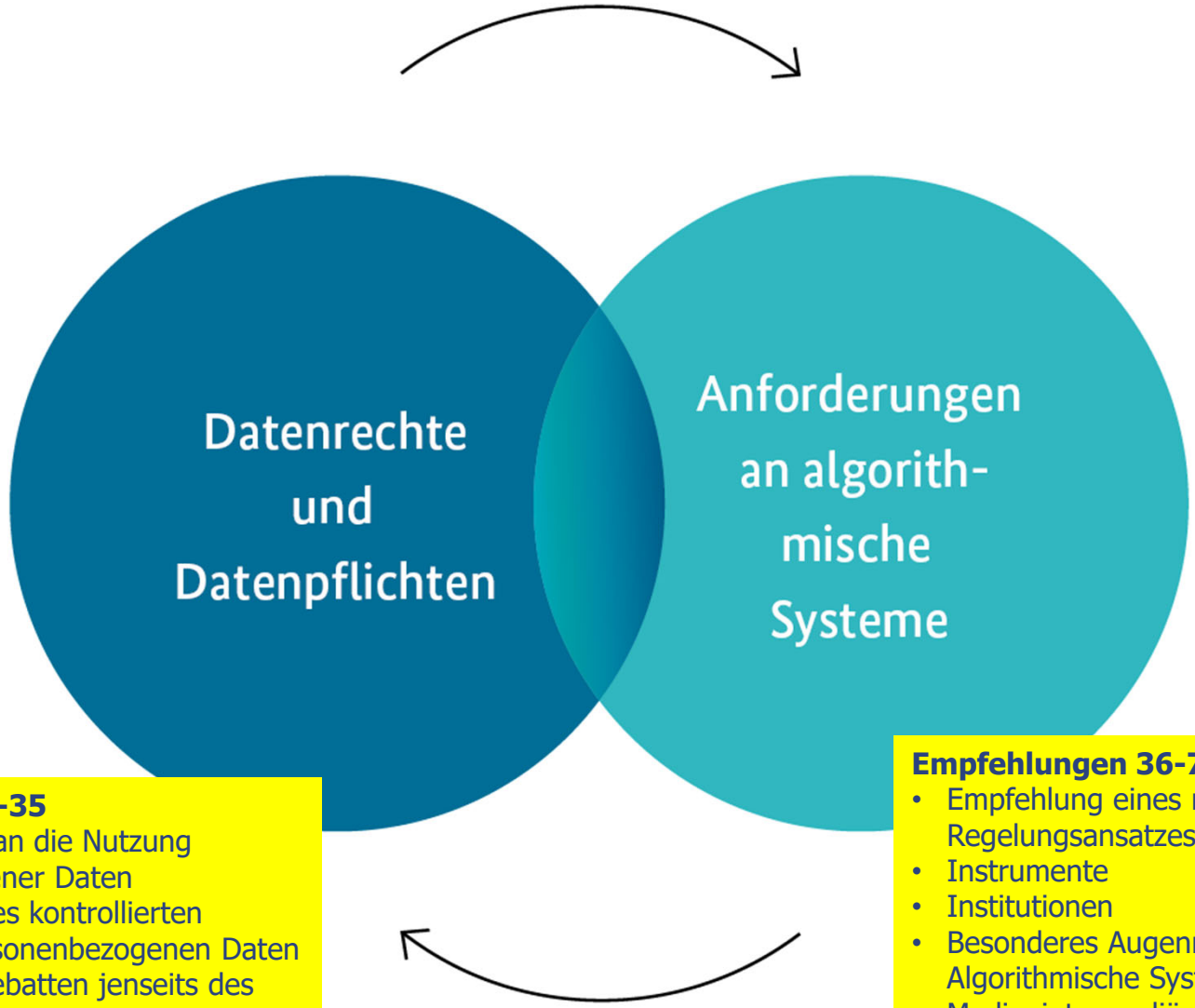
- Gesetzentwurf, techn. Spec, Lehrbuch, Monographie, …
- Konkrete Einmischung von außen in die Arbeit
- Alles von allen bis zum Ende durchdringen
- Ablehnung von Teilen des Gutachtens („dissenting votes“)

Überblick

Bild: Dariusz Staniszewski via Pixabay

1. Die Datenethikkommission
2. Die (KI-)Empfehlungen der Datenethikkommission
3. Die Sicht der Datenschutzaufsicht
4. Was noch?
5. Fazit



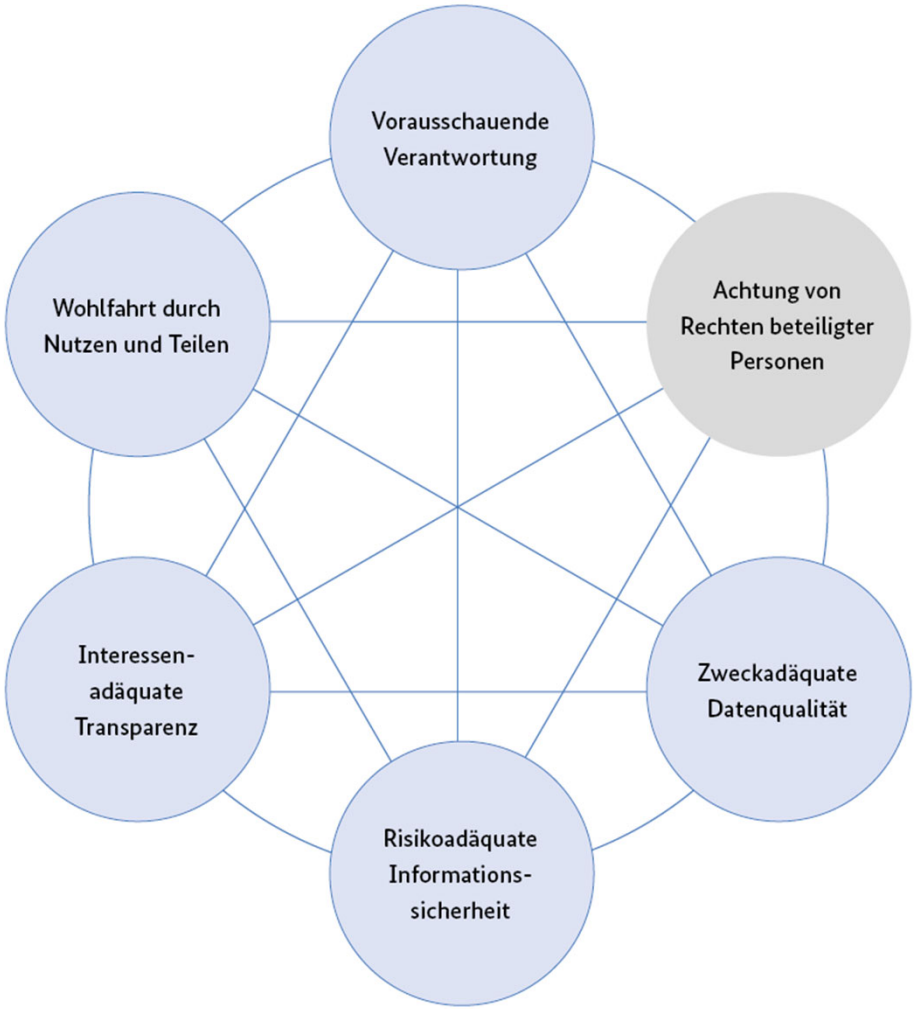


Empfehlungen 1-35
- Anforderungen an die Nutzung personenbezogener Daten
- Verbesserung des kontrollierten Zugangs zu personenbezogenen Daten
- Datenzugangsdebatten jenseits des Personenbezugs

Empfehlungen 36-75
- Empfehlung eines risikoadaptierten Regelungsansatzes
- Instrumente
- Institutionen
- Besonderes Augenmerk: Algorithmische Systeme bei Medienintermediären
- Der Einsatz von algorithmischen Systemen durch staatliche Stellen
- Haftung für algorithmische Systeme

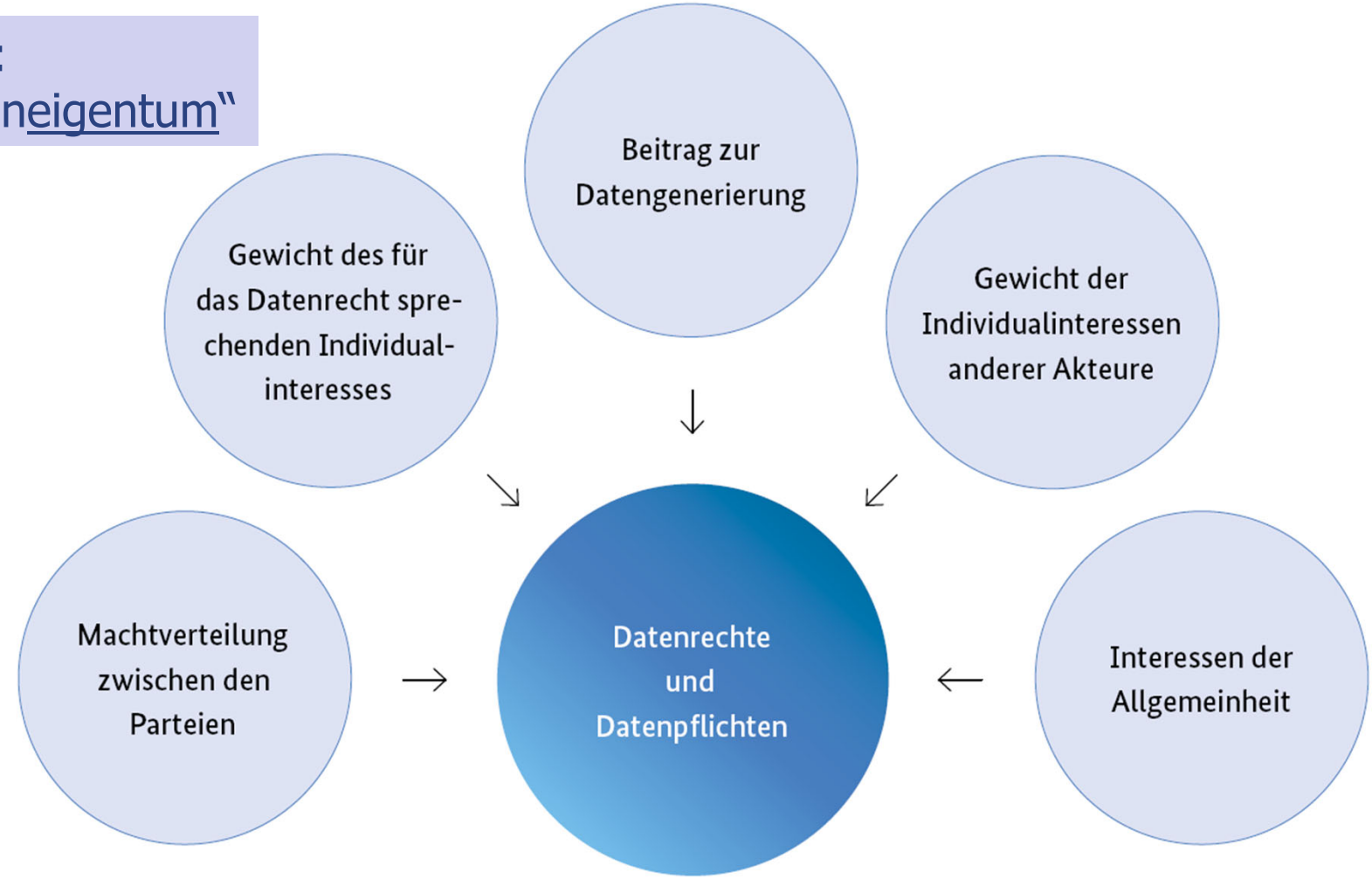
https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_node.html

I. Perspektive „Daten“: Anforderungen an den Umgang mit Daten

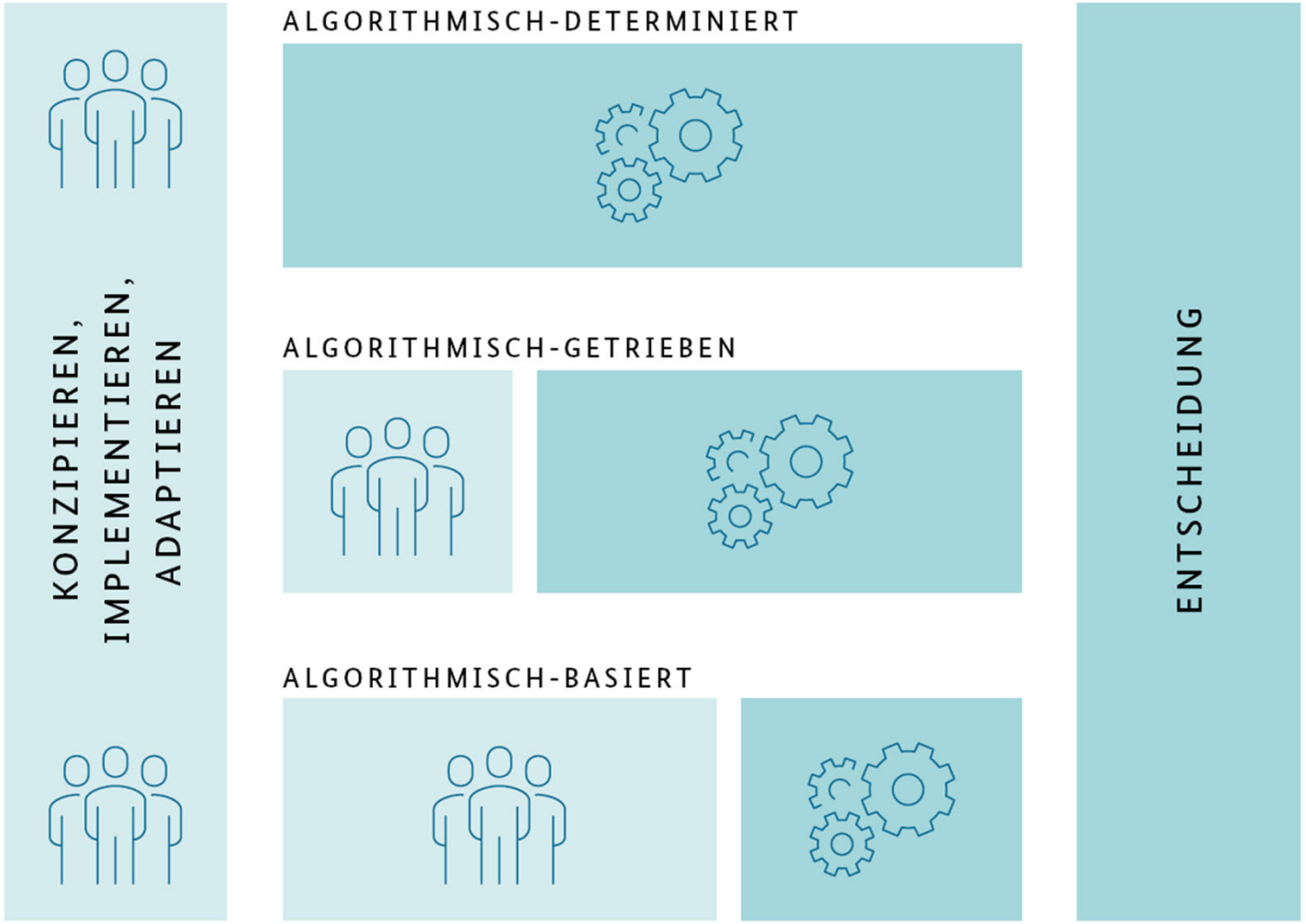


I. Perspektive „Daten“: Faktoren zu Datenrechten und -pflichten

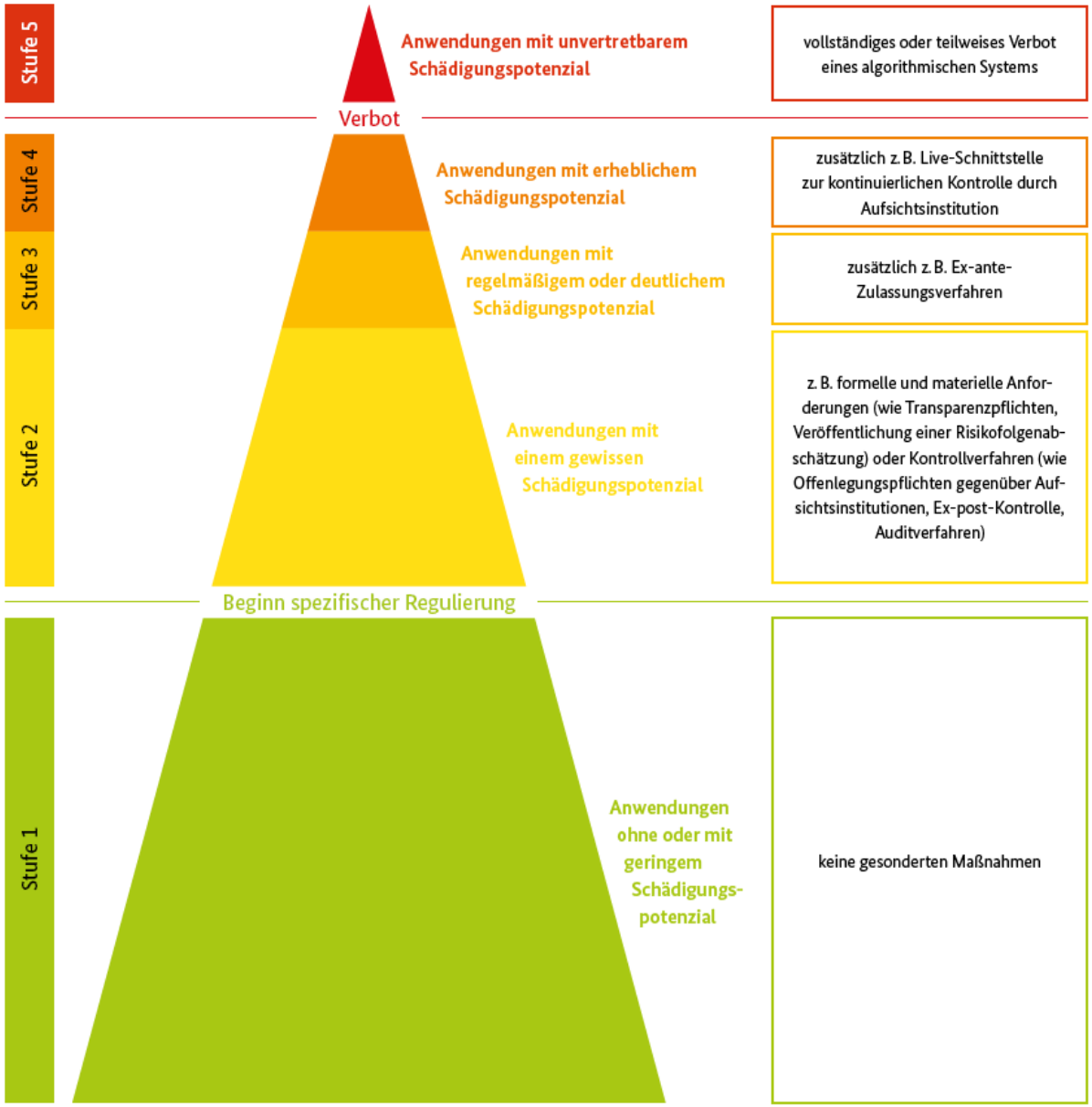
Nicht: „Dateneigentum“



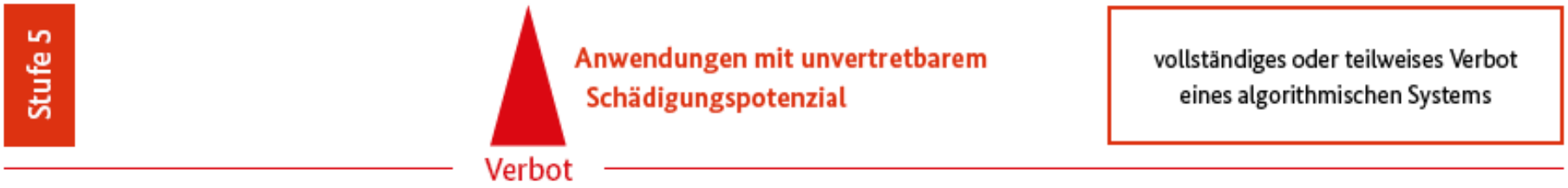
II. Perspektive „algorithmische Systeme": Terminologie



Kritikalitäts-pyramide

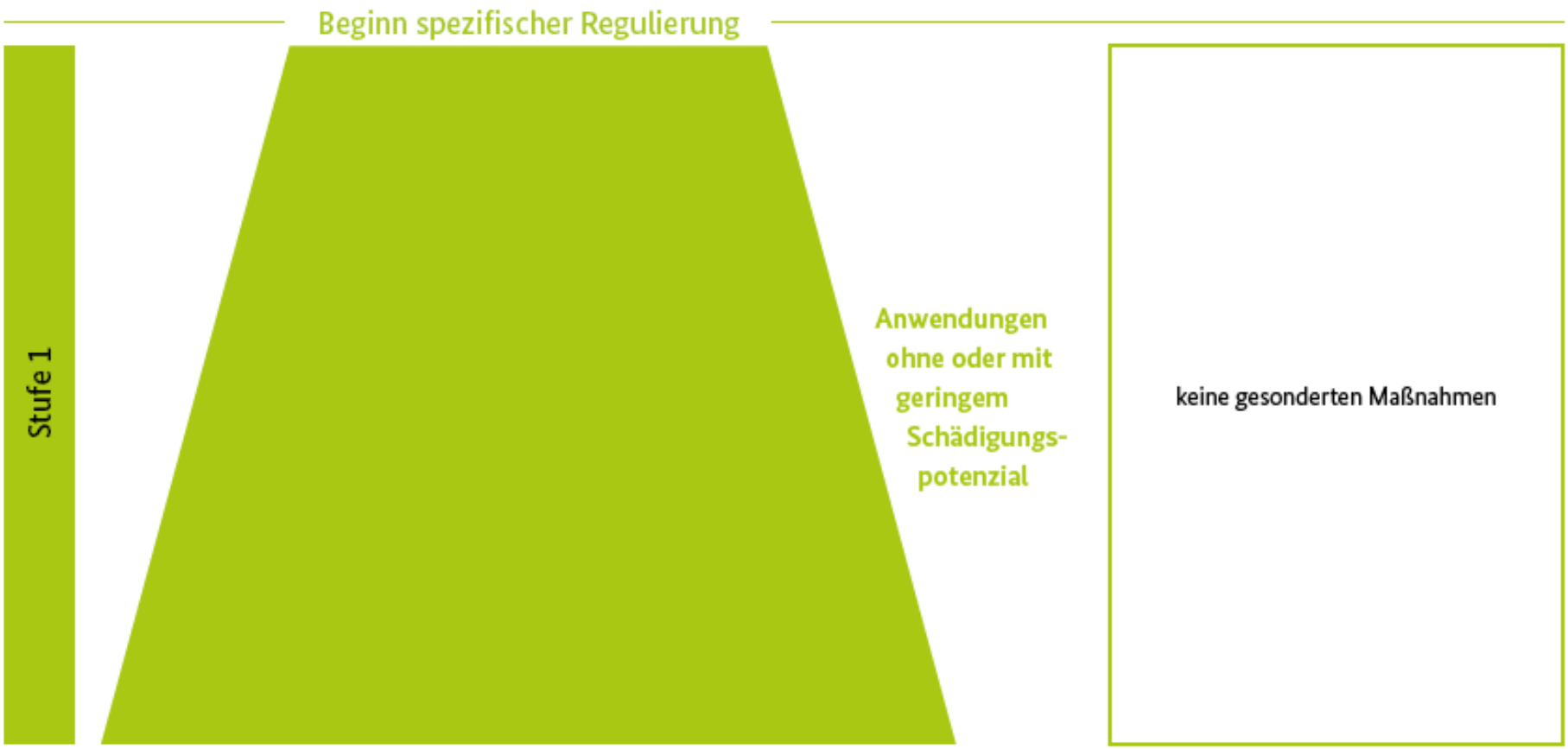


II. Perspektive „algorithmische Systeme": Kritikalität Stufe 5



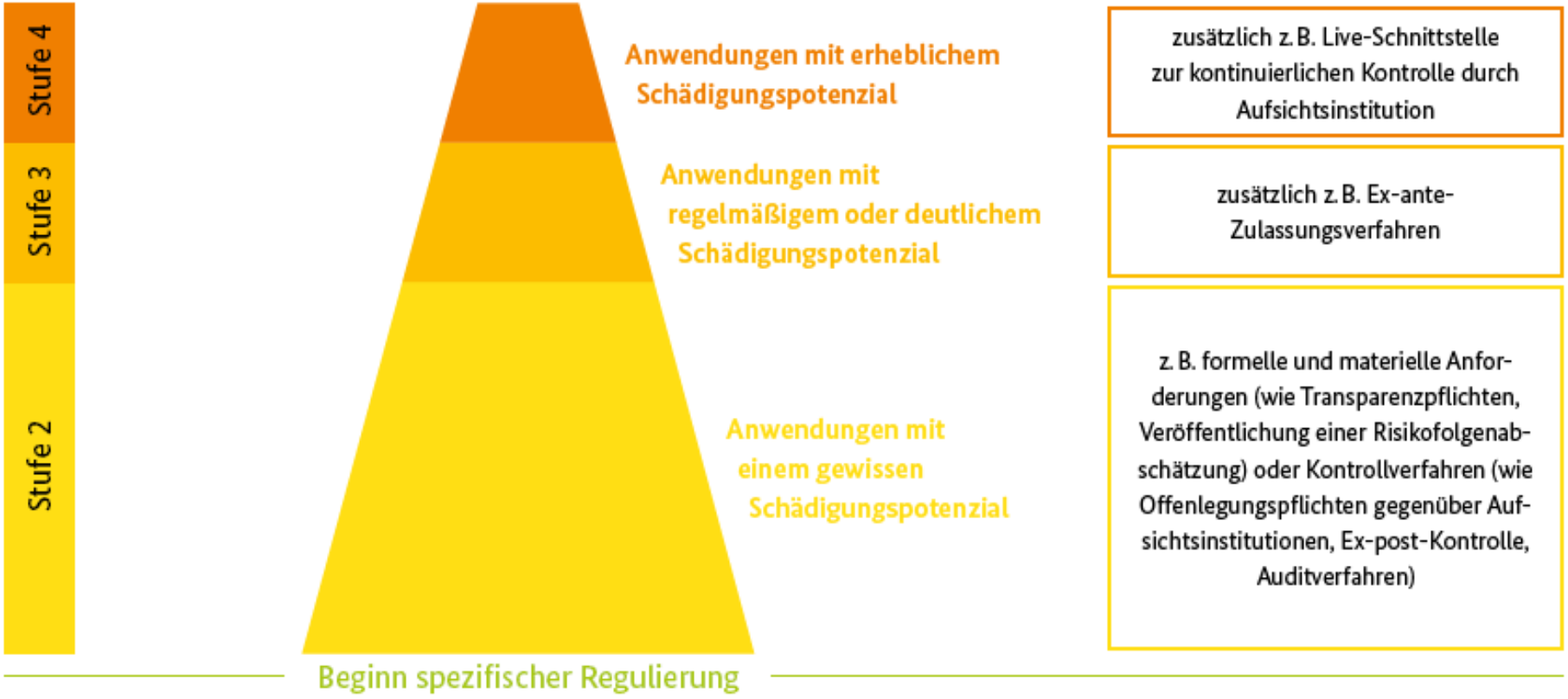
Bsp. Stufe 5: autonome Waffensysteme

II. Perspektive „algorithmische Systeme": Kritikalität Stufe 1



Bsp. Stufe 1: kontrollierte Spam-Filter; Getränkeautomat (Ware/Geld)

II. Perspektive „algorithmische Systeme": Kritikalität Stufen 2-4



Bsp. Stufe 2-4: dynamische Preissetzung – personalisiert – Marktmacht

DEK-Empfehlungen

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.

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.

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.

DEK-Empfehlungen

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.

42

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

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.

DEK-Empfehlungen

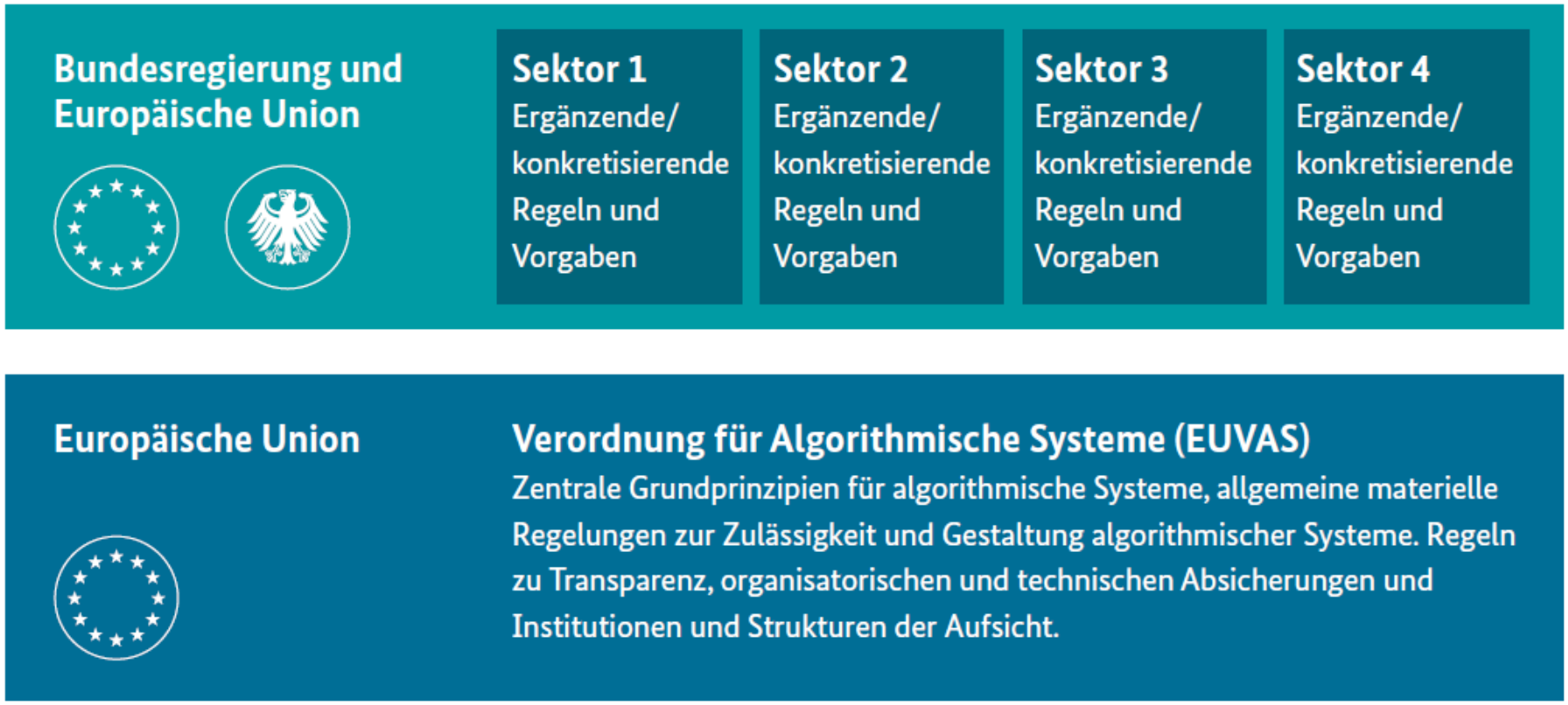


Abbildung 9:
Regulierung algorithmischer Systeme durch horizontale Vorgaben im Recht der Europäischen Union und sektorale Konkretisierung

DEK-Empfehlungen

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.

DEK-Empfehlungen

Haftung für algorithmische Systeme

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.

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.

Grundlegend: nur ethisch Vertretbares

Anforderungen an die Nutzung personenbezogener Daten

1

Die DEK empfiehlt **Maßnahmen gegen ethisch nicht-vertretbare 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.

- Totalüberwachung
- Addictive Design
- Dark Patterns
- Politische Manipulation
- Lock-in

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.

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.

Kompetenz-zentrum + Initiativen

„Mehr-Ebenen-Governance komplexer Ökosysteme"

D Mehr-Ebenen-Governance komplexer Datenökosysteme 67

Kompetenz

By Design

Standardisierung

Lebenslanges Lernen

Selbstverpflichtungen

Forschung

Komponenten, die mit einer aus ethischer oder datenschutzrechtlicher Sicht besseren Gestaltung aufwarten, allenfalls ein Nischendasein. In diesen Bereichen sind Änderungen nötig, damit der Einbau ethischer Prinzipien im Allgemeinen und Datenschutzprinzipien im Speziellen die Regel wird, statt weiterhin eine Ausnahmeeigenschaft darzustellen. Ethics by Design erfordert einen Brückenschlag zwischen verschiedenen Gemeinschaften („Communities“) und hat Auswirkungen auf die betroffenen Berufsbilder. Hilfreich für die Umsetzung wären neben Informationen zu Methoden und Katalogen **Best-Practice-Konzepte, unterstützende Werkzeuge, Entwicklungs-Frameworks** und **(Open-Source-) Code-Komponenten**. Über Plattformen mit Repositorien für solche Komponenten sowie verwendbare Datenbestände, die gegebenenfalls Überprüfungen erst möglich machen, könnten die besonderen Eigenschaften herausgestellt, nötige Dokumentationen gleich mitgeliefert und Möglichkeiten zum Austausch von Erfahrungswissen bereitgestellt werden.

... by Design

Repositories:

Best Practice

Tools

Frameworks

Code

Überblick

1. Die Datenethikkommission
2. Die (KI-)Empfehlungen der Datenethikkommission
3. Die Sicht der Datenschutzaufsicht
4. Was noch?
5. Fazit

Bild: Dariusz Staniszewski via Pixabay

Sicht der Datenschutzaufsicht

- Vor dem Erscheinen des Gutachtens: Zweifel Einzelner aus den Reihen der Datenschutz-aufsicht an einem ethikbasierten Ansatz

- Klarstellung durch die DEK selbst (1/2): Kap. B-2: „Verhältnis von Ethik und Recht“

> **Ethik geht nicht im Recht auf.** Nicht jedes Detail, das ethisch relevant ist, kann und sollte rechtlich reguliert werden. Umgekehrt gibt es Aspekte rechtlicher Regulierung, die pragmatischer Art und ethisch nicht zwingend sind. Rechtssetzung muss aber immer mögliche ethische Implikationen reflektieren und ethischen Ansprüchen genügen – den verfassungsrechtlichen Vorgaben ohnehin.

Sicht der Datenschutzaufsicht

- Klarstellung durch die DEK selbst (1/2):
  Kap. B-2: „Verhältnis von Ethik und Recht“

> Andererseits können und müssen regulative Rahmenbedingungen wesentliche Rechte und Freiheiten schützen und Rechtssicherheit schaffen. Dies ist die Grundlage dafür, dass Bürgerinnen und Bürger, Unternehmen und Institutionen auf eine ethisch ausgerichtete gesellschaftliche Transformation vertrauen können. Zudem bietet das Rechtssystem mit der Möglichkeit von Regulierung auf unterschiedlichen Ebenen – vom Gesetz über Verordnungen bishin zu Kodizes, Selbstverwaltung und Selbstverpflichtung – einen Instrumentenkasten, um anpassungsfähige und dem technologischen Fortschritt gerecht werdende Rahmenbedingungen zu gestalten.

Sicht der Datenschutzaufsicht

- Klarstellung durch die DEK selbst (2/2):
  Kap. B-3: „Allgemeine ethische und rechtliche Grundsätze und Prinzipien“
  - Menschenwürde
  - Selbstbestimmung
  - Privatheit
  - Sicherheit
  - Demokratie
  - Gerechtigkeit und Solidarität
  - Nachhaltigkeit

Sicht der Datenschutzaufsicht

- Gutachten als Material für die eigene Arbeit

- Achtung: allgemeiner Ansatz der DEK
  - Für alle Arten von Daten mit oder ohne Personenbezug
  - Individuelle, kollektive und gesellschaftliche Sicht


DSK

Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
Hambacher Schloss
3. April 2019

Hambacher Erklärung zur Künstlichen Intelligenz

Sieben datenschutzrechtliche Anforderungen

https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf

- Kein Handbuch für Bestehendes, aber perspektivisch

- Äußerung des Europäischen Datenschutzausschusses zum AI Act (18.06.2021)

EDSA zum AI Act

Der EDSA und der EDSB **begrüßen den risikobasierten Ansatz**, der dem Vorschlag zugrunde liegt. Allerdings sollte dieser Ansatz präzisiert und der Begriff „Risiko für die Grundrechte" mit der DSGVO und der Verordnung (EU) 2018/1725 (EU-DSVO) in Einklang gebracht werden, da Aspekte eine Rolle spielen, die den Schutz personenbezogener Daten betreffen.

Dem Vorschlag entsprechend **bedeutet die Einstufung eines KI-Systems als hochriskant nicht, dass dieses zwangsläufig mit geltendem Recht vereinbar ist** und vom Nutzer entsprechend verwendet werden kann; diese Auffassung wird vom EDSA und EDSB geteilt. Die verantwortliche Stelle wird **unter Umständen weitere sich aus dem Datenschutzrecht der Union ergebende Anforderungen einhalten müssen**. Überdies sollte die Einhaltung der sich aus dem Unionsrecht ergebenden Anforderungen (einschließlich derjenigen über den Schutz personenbezogener Daten) Voraussetzung für die Zulassung als mit CE-Kennzeichnung versehenes Produkt für den europäischen Markt sein. Der EDSA und der EDSB sind deshalb der Ansicht, dass das **Erfordernis, die Einhaltung der DSGVO und der EU-DSVO sicherzustellen, in Titel III Kapitel 2 aufgenommen werden sollte**. Außerdem halten es der EDSA und der EDSB für erforderlich, das im Vorschlag vorgesehene Konformitätsbewertungsverfahren dahingehend anzupassen, dass die Ex-ante-Konformitätsbewertungen für Hochrisiko-KI-Systeme stets von Dritten durchgeführt werden.

EDSA-EDSB Gemeinsame Stellungnahme 5/2021 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, 18. Juni 2021, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_de

EDSA zum AI Act

Wegen des hohen Diskriminierungsrisikos enthält der Vorschlag ein Verbot der Bewertung des sozialen Verhaltens („Social Scoring"), wenn diese „über einen bestimmten Zeitraum" oder „durch Behörden oder in deren Auftrag" erfolgt. Allerdings sind auch Privatunternehmen (wie Anbieter von sozialen Medien und Cloud-Diensten) in der Lage, enorme Mengen personenbezogener Daten zu verarbeiten und Social Scoring anzuwenden. Folglich **sollte die künftige KI-Verordnung das Verbot jeder Art von Bewertung des sozialen Verhaltens vorsehen**.

Die biometrische Fernidentifizierung natürlicher Personen in öffentlich zugänglichen Räumen birgt ein hohes Risiko, dass die Privatsphäre natürlicher Personen verletzt wird, und läuft der Erwartung der Bevölkerung, im öffentlichen Raum anonym zu bleiben, fundamental zuwider. Aus diesen Gründen erheben der EDSA und der EDSB die **Forderung nach einem allgemeinen Verbot der Verwendung von KI zur automatischen Erkennung von personenbezogenen Merkmalen in öffentlich zugänglichen Räumen**, und zwar im jeglichem Zusammenhang; solche Merkmale sind z. B. Gesichtszüge, aber auch Gangart, Fingerabdrücke, DNA, Stimme, Tastenanschlagsmuster und andere biometrische Merkmale oder Verhaltenssignale. Ein **Verbot** wird auch für **KI-Systeme empfohlen, die natürliche Personen nach biometrischen Merkmalen in Cluster eingruppieren**, etwa nach ethnischer Zugehörigkeit, Geschlecht bzw. politischer oder sexueller Orientierung oder sonstigen Merkmalen, die zu den gemäß Artikel 21 der Charta verbotenen Diskriminierungsgründen zählen. Des Weiteren sind der EDSA und der EDSB der Ansicht, dass die Verwendung von KI **zur Erkennung von Emotionen natürlicher Personen unter keinen Umständen wünschenswert ist und verboten werden sollte**.

Sicht der Datenschutzaufsicht: Grundsätze in der DSGVO

Oberthema: Fairness

Art. 5 DSGVO
– immer zu erfüllen bei personenbezogenen Daten

Abs. 1:

a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
b) Zweckbindung
c) Datenminimierung
d) Richtigkeit
e) Speicherbegrenzung
f) Integrität und Vertraulichkeit (Datensicherheit)

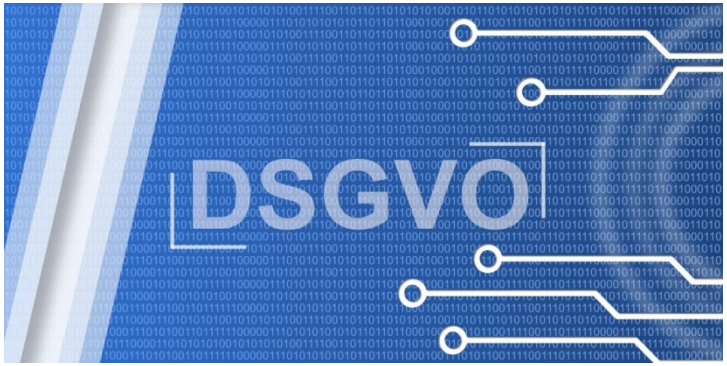
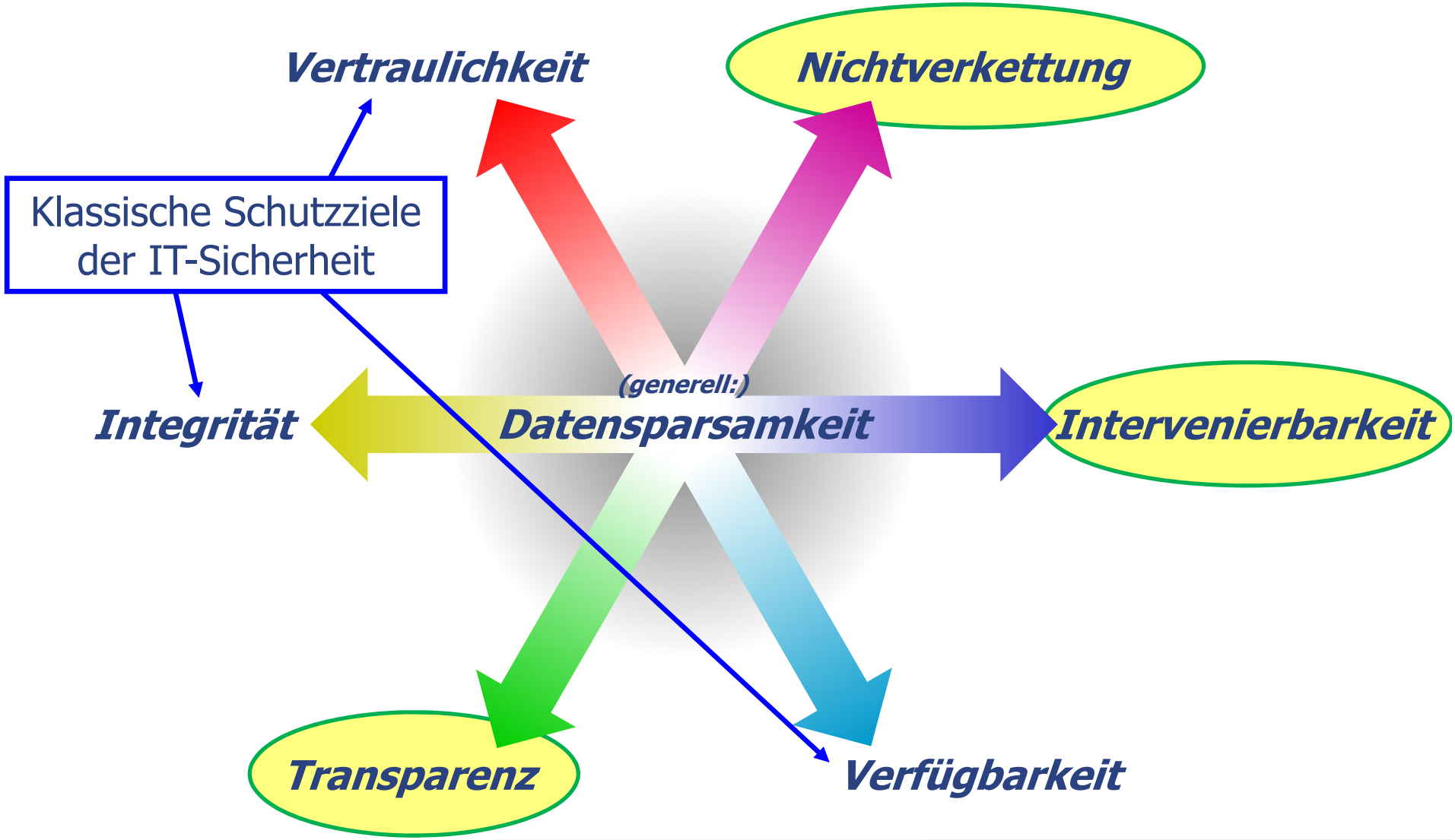


Bild: skylarvision via Pixabay

Abs. 2: Rechenschaftspflicht

Sicht der Datenschutzaufsicht: Gewährleistungsziele



7 Gewähr-leistungsziele

Veröffentlichungen der DSK

DATENSCHUTZKONFERENZ

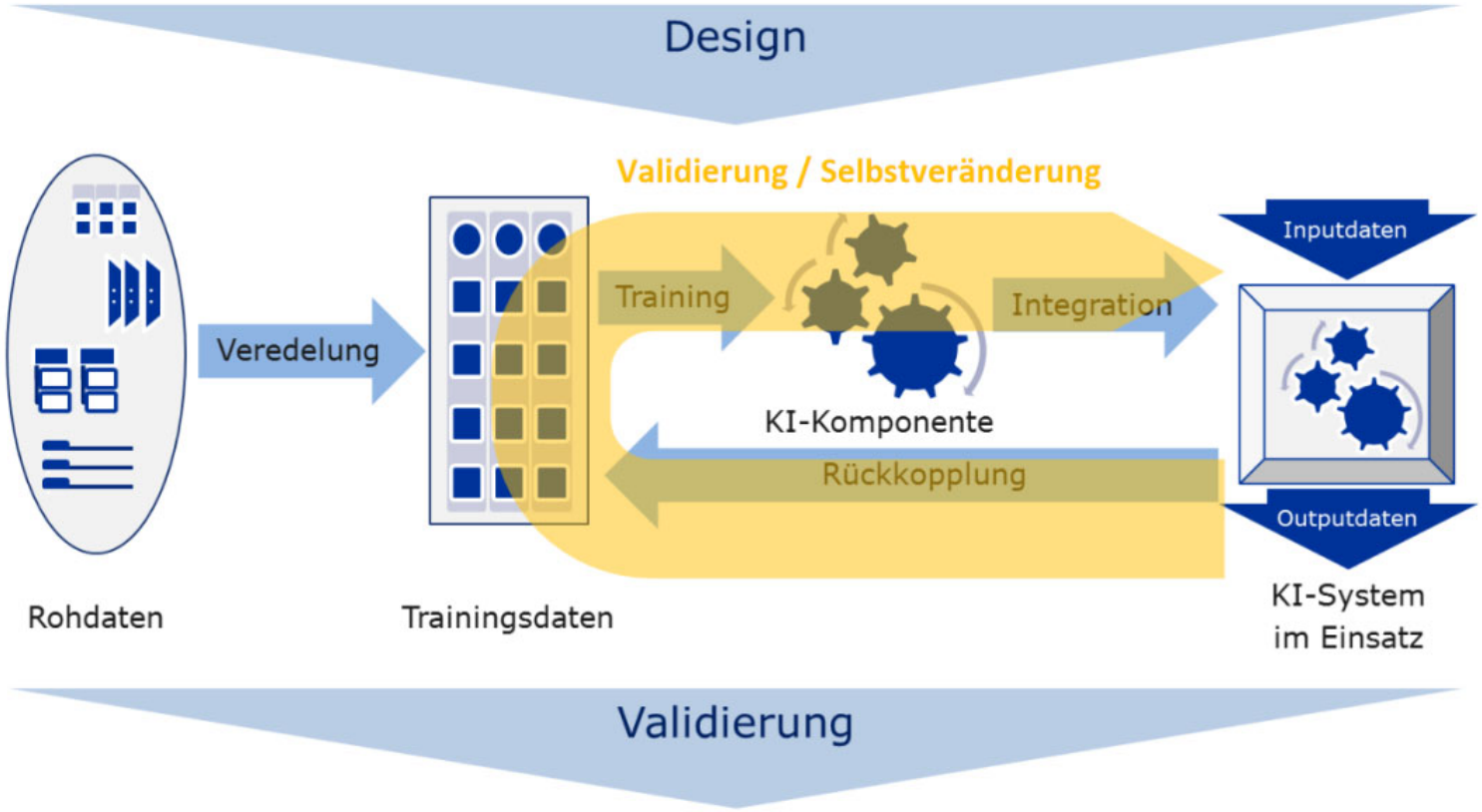


Abbildung 1 - Allgemeiner Lebenszyklus von KI-Systemen

https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf

7 Gewährleistungsziele

Veröffentlichungen der DSK

DATENSCHUTZKONFERENZ

Technische und organisatorische Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen

Festlegung von Primär-Trainings-, Verifikations- und Testdatensätzen	Training	Integrität
Dokumentation des Verfahrens zur Einteilung der Primär-Trainings-, Verifikations-, Sekundär-Trainings- und Testdatensätze	Training	Transparenz
Regelung zur Verwendung von Trainings-, Verifikations- und Testdatensätzen	Training	Integrität
Festlegung des Verfahrens zur Ermittlung der Güte der KI-Komponente	Training	Integrität
Dokumentation des Verfahrens zur Ermittlung der Güte der KI-Komponente	Training	Transparenz
Gegebenenfalls Prozess zur Erweiterung der Trainingsdaten, um gesteckte Güte zu erreichen	Training	Datenminimierung
Verhinderung von unbefugten Manipulationen an KI-Komponenten	Training	Integrität
Test mit (synthetischen) Testdaten auf Basis der Hypothese und Erwartungen	Validierung	Integrität
Test mit störsignalbehafteten(, synthetischen) Daten auf Basis des unerwünschten Verhaltens	Validierung	Integrität
Prüfung der Hypothese und der Erwartungen auf Basis des Testdatensatzes	Validierung	Integrität
Dokumentation der Güte der KI-Komponente inklusive der ermittelten Fehlerrate und Systemstabilität	Validierung	Transparenz
Untersuchung der KI-Komponente auf Erklärbarkeit und Nachvollziehbarkeit	Validierung	Transparenz
Evaluation des ausgewählten KI-Verfahrens bezüglich alternativer, erklärbarerer KI-Verfahren	Validierung	Transparenz
Prüfung auf Neben- bzw. Zwischenergebnisse und Bewertung dieser	Validierung	Nichtverkettung
Möglichkeit des Eingreifens einer Person in den Entscheidungsprozess	Einsatz	Intervenierbarkeit
Entscheidungen, die hohe Risiken für Betroffene bergen, dürfen von KI-Systemen nur vorbereitet werden.	Einsatz	Intervenierbarkeit
Möglichkeit des Stoppens einer KI-Komponente, von der potentiell Risiken für die Rechte und Freiheiten natürlicher Personen ausgehen, oder des Ersetzens der KI-Komponente durch eine Fall-Back-Lösung	Einsatz	Intervenierbarkeit
Auskunftsmöglichkeit für Betroffene zum Zustandekommen von Entscheidungen und Prognosen	Einsatz	Transparenz
Überwachung des Verhaltens der KI-Komponente	Einsatz	Transparenz
Protokollierung von finalen Entscheidungen, deren Freigabe/Bestätigung/Ablehnung, Zeitpunkt und ggf. entscheidende Person	Einsatz	Transparenz

21

Prüfung und Bewertung der Hypothese und der Erwartungen auf Basis des Verhaltens im Betrieb	Einsatz	Transparenz
Einhaltung der Policy überwachen und sicherstellen	Einsatz	Integrität
Regelmäßige Prüfung der KI-Komponente auf Diskriminierungen und anderes unerwünschtes Verhalten	Einsatz	Integrität
Regelmäßige Evaluierung der Hypothese, Erwartungen, unerwünschtem Verhalten bezüglich der Wissensdomäne und den sonstigen Rahmenbedingungen	Einsatz	Integrität
Regelmäßige Evaluierung welche Eingabe- und Ausgabeparameter der KI-Komponenten für das gewünschte Verhalten des KI-Systems relevant und erforderlich sind und wenn möglich Anpassung der KI-Komponenten zur Verarbeitung nur relevanter und erforderlicher Daten	Einsatz	Datenminimierung
Regelmäßige Prüfung der Güte des KI-Systems und seiner KI-Komponenten auf Basis der Betriebsdaten	Einsatz	Integrität
Berechnungen der KI-Komponente möglichst auf Endgerät des Nutzer ohne Übermittlung der Daten	Einsatz	Vertraulichkeit
Wenn Berechnungen der KI-Komponente nicht auf Endgerät des Nutzer durchgeführt werden kann, dann möglichst auf Geräten unter der Kontrolle des Verantwortlichen	Einsatz	Vertraulichkeit
Wenn Übermittlung der Daten an KI-Komponente erforderlich, dann Ende-zu-Ende-Verschlüsselung einsetzen	Einsatz	Vertraulichkeit
Betroffene über das Verfahren zur Ermittlung der Güte des KI-Systems und die festgestellte Güte informieren	Einsatz	Transparenz
Betroffene und eingreifende Personen möglichst über Teilergebnisse und, ob Schwellwert nur knapp (nicht) erreicht wurde, informieren.	Einsatz	Transparenz
Ausschluss der Nutzung von Neben- bzw. Zwischenergebnissen durch Unbefugte	Einsatz	Vertraulichkeit
Ausschluss der Nutzung von Neben- bzw. Zwischenergebnissen zu nicht vorgesehenen Zwecken	Einsatz	Nichtverkettung
Mechanismen zum Anfechten und Korrigieren von Entscheidungen einer KI-Komponente vorsehen	Einsatz	Intervenierbarkeit
Verwendung von angefochtenen und korrigierten Entscheidungen zur Weiterentwicklung der KI-Komponente	Einsatz	Integrität
Hinweis auf die Möglichkeit zur Anfechtung und Korrektur von Entscheidungen geben	Einsatz	Transparenz
Verhinderung von unbefugten Manipulationen an KI-Komponenten	Einsatz	Integrität

22

https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf

Überblick

Bild: Dariusz Staniszewski via Pixabay

1. Die Datenethikkommission
2. Die (KI-)Empfehlungen der Datenethikkommission
3. Die Sicht der Datenschutzaufsicht
4. Was noch?
5. Fazit

Koalitionsvertrag 2021

Zentrale Zukunftsfelder sind unter anderem: Erstens: Moderne Technologien für eine wettbewerbsfähige und klimaneutrale Industrie (wie Stahl- und Grundstoffindustrie) in Deutschland. Sicherstellung sauberer Energiegewinnung- und -versorgung sowie die nachhaltige Mobilität der Zukunft. Zweitens: Klima, Klimafolgen, Biodiversität, Nachhaltigkeit, Erdsystem und entsprechende Anpassungsstrategien, sowie nachhaltiges Landwirtschafts- und Ernährungssystem. Drittens: ein vorsorgendes, krisenfestes und modernes Gesundheitssystem, welches die Chancen biotechnologischer und medizinischer Verfahren nutzt, und das altersabhängige Erkrankungen sowie seltene oder armutsbedingte Krankheiten bekämpft. Viertens: technologische Souveränität und die Potentiale der Digitalisierung, z. B. in Künstlicher Intelligenz und Quantentechnologie, für datenbasierte Lösungen quer durch alle Sektoren. Fünftens: Erforschung von Weltraum und Meeren und Schaffung nachhaltiger Nutzungsmöglichkeiten. Sechstens: gesellschaftliche Resilienz, Geschlechtergerechtigkeit, Zusammenhalt, Demokratie und Frieden.

Koalitionsvertrag 2021

institutionelle Freiräume. Im Sinne eines lernenden, technologiefördernden Staates setzen wir digitale Innovationen in der Verwaltung ein, schaffen notwendige Rechtsgrundlagen und Transparenz. Wir unterstützen den europäischen AI Act. Wir setzen auf einen mehrstufigen risikobasierten Ansatz, wahren digitale Bürgerrechte, insbesondere die Diskriminierungsfreiheit, definieren Haftungsregeln und vermeiden innovationshemmende ex-ante-Regulierung. Biometrische Erkennung im öffentlichen Raum sowie automatisierte staatliche Scoring Systeme durch KI sind europarechtlich auszuschließen.

Überblick

1. Die Datenethikkommission
2. Die (KI-)Empfehlungen der Datenethikkommission
3. Die Sicht der Datenschutzaufsicht
4. Was noch?
5. Fazit

Bild: Dariusz Staniszewski via Pixabay

Fazit

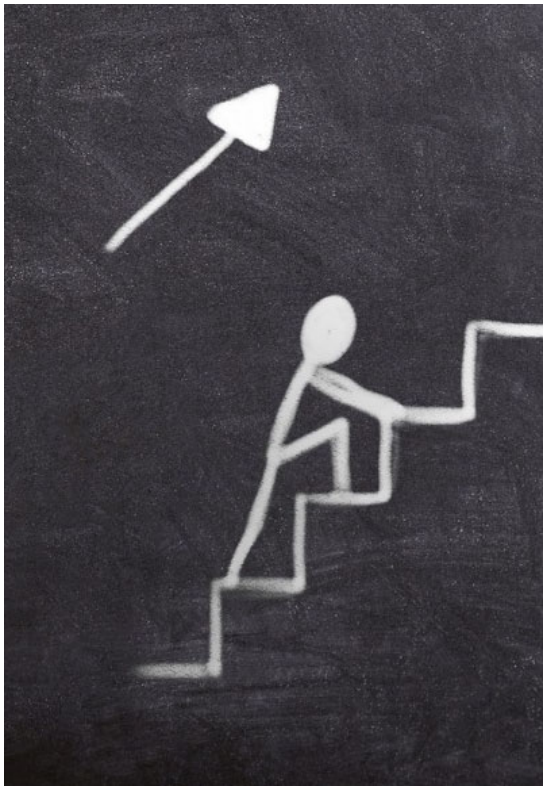


Bild: athree23 via Pixabay

- DEK-Gutachten:
  - Perspektivische Ausarbeitung für übergeordneten Umgang mit Daten und Digitalisierung
  - Keine Infragestellung der DSGVO an sich
  - Nutzbarmachung der Konzepte der DSGVO
  - Gerichtet an Gestalter von Normen und Systemen (insbesondere Politik und Gesetzgebung)
- Datenschutzaufsicht:
  - DSGVO++: heutige (rechtliche) Realität
  - Konkretisierung auf dem Weg
- Ausblick: Europäischer AI Act


Vielen Dank