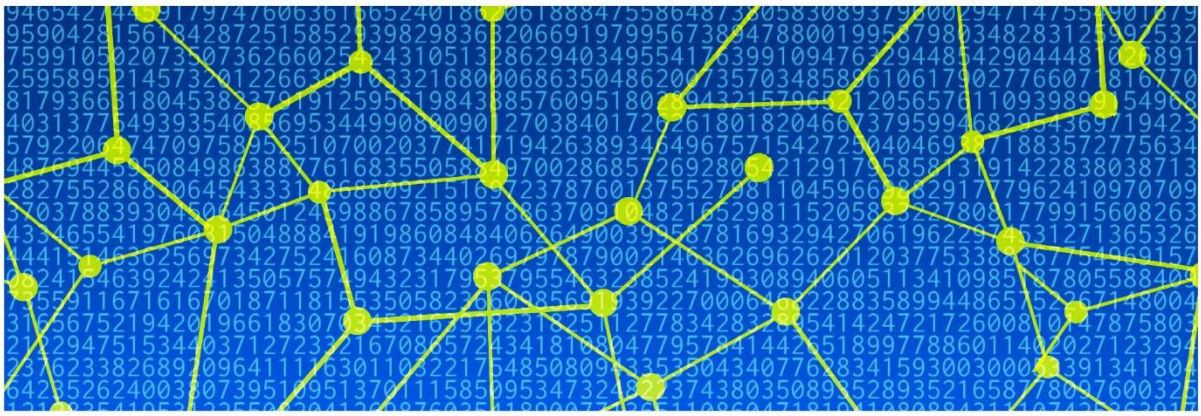

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 4/2020

Stellungnahme des EDSB zum Weißbuch der Europäischen Kommission „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“

EDPS

29. Juni 2020

Zusammenfassung

Am 19. Februar 2020 veröffentlichte die Europäische Kommission ein Weißbuch mit dem Titel „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“. Es ist Teil eines umfassenderen Pakets strategischer Dokumente, zu der auch eine Mitteilung mit dem Titel „Eine europäische Datenstrategie“ gehört.

Mit dem Weißbuch werden zwei Ziele verfolgt: Festlegung politischer Optionen zur Förderung der Nutzung künstlicher Intelligenz (KI) und Eingehen auf „die mit dieser neuen Technologie einhergehenden Gefahren“. Um diese Ziele zu erreichen, werden in dem Weißbuch eine Reihe von Maßnahmen zur Förderung der Entwicklung und der Akzeptanz von KI sowie ein neuer Rechtsrahmen vorgeschlagen, mit dem spezifischen Anliegen im Bereich der KI Rechnung getragen werden soll, die im derzeitigen Rahmen möglicherweise nicht berücksichtigt werden.

In dieser Stellungnahme legt der EDSB seine Ansichten zum Weißbuch insgesamt sowie zu bestimmten spezifischen Aspekten dar, wie dem vorgeschlagenen risikobasierten Ansatz, der Durchsetzung von KI-Vorschriften oder den spezifischen Anforderungen an die biometrische Fernidentifikation (einschließlich Gesichtserkennung).

Der EDSB erkennt die zunehmende Bedeutung und Wirkung der KI an. KI birgt jedoch eigene Risiken und ist keine „Wunderwaffe“, die alle Probleme lösen wird. Vorteile, Kosten und Risiken sollten von jedem, der eine Technologie einsetzt, berücksichtigt werden, insbesondere von öffentlichen Verwaltungen, die große Mengen personenbezogener Daten verarbeiten.

Der EDSB begrüßt nachdrücklich die zahlreichen Verweise des Weißbuchs auf einen **europäischen Ansatz für KI**, der auf den **Werten und Grundrechten der EU** beruht, und die Erwägung, dass die **europäischen Datenschutzvorschriften eingehalten** werden müssen.

Die in dieser Stellungnahme formulierten Empfehlungen zielen daher darauf ab, die Garantien und Kontrollen zum Schutz personenbezogener Daten klarzustellen und, soweit erforderlich, unter Berücksichtigung des besonderen Kontexts von KI weiterzuentwickeln.

Zu diesem Zweck empfiehlt der EDSB insbesondere, dass jeder neue Rechtsrahmen für KI

- **sowohl** für die EU-Mitgliedstaaten **als auch** für die Organe, Einrichtungen und sonstigen Stellen der EU gilt;

- so konzipiert ist, dass er nicht nur den Einzelnen, sondern auch Gemeinschaften und die Gesellschaft insgesamt **vor negativen Auswirkungen schützt**;

- ein **robusteres und nuancierteres Risikoklassifizierungssystem** vorschlägt, mit dem sichergestellt wird, dass jeder erhebliche potenzielle Schaden, der durch KI-Anwendungen entsteht, durch geeignete Risikominderungsmaßnahmen ausgeglichen wird;

- eine Folgenabschätzung enthält, in der **klar festgelegt ist, welche Regelungslücken** mit dem Rahmen geschlossen werden sollen.

- **Überschneidungen** zwischen verschiedenen Aufsichtsbehörden **vermeidet** und die Einführung eines Mechanismus für die Zusammenarbeit vorsieht.

In Bezug auf die biometrische Fernidentifikation unterstützt der EDSB den Gedanken **eines Moratoriums für die automatische Erkennung menschlicher Merkmale im öffentlichen Raum in der EU**, und zwar nicht nur des Gesichts, sondern auch des Gangs, von Fingerabdrücken, DNA,

Stimme, Tastenanschlägen und anderen biometrischen oder verhaltensgebundenen Signalen, damit eine fundierte und demokratische Debatte stattfinden kann, und zwar bis zu dem Zeitpunkt, zu dem die EU und die Mitgliedstaaten über alle geeigneten Garantien verfügen, einschließlich eines umfassenden Rechtsrahmens, der die Verhältnismäßigkeit der jeweiligen Technologien und Systeme für den konkreten Fall gewährleistet.

Der EDSB steht der Kommission, dem Rat und dem Europäischen Parlament weiterhin für weitere Ratschläge zur Verfügung und erwartet, dass er gemäß Artikel 42 der Verordnung (EU) 2018/1725 zu gegebener Zeit konsultiert wird. Die Bemerkungen in dieser Stellungnahme greifen künftigen zusätzlichen Kommentaren zu bestimmten Fragen und/oder etwaigen weiteren Informationen nicht vor.

INHALTSVERZEICHNIS

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 7 und 8,

gestützt auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, „DSGVO“)[1],

gestützt auf die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates[2] –

gestützt auf die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG[3] („EU-DSVO“), insbesondere von Artikel 57 Absatz 1 Buchstabe h und Artikel 58 Absatz 3 Buchstabe c,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG UND HINTERGRUND

1. Das Weißbuch der Kommission „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“[4] (im Folgenden „Weißbuch“) ist Teil der Initiative Nr. 10 („Ein europäisches Konzept für KI“) und Bestandteil des Kapitels „Ein Europa, das für das digitale Zeitalter gerüstet ist“ des Arbeitsprogramms der Kommission für 2020.

2. Der EDSB stellt fest, dass das Weißbuch eng mit der „Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine europäische Datenstrategie“[5] (im Folgenden „Datenstrategie“) verknüpft ist, zu der der EDSB eine gesonderte Stellungnahme abgegeben hat[6].

3. Der EDSB wurde am 29. Januar 2020 von der Kommission zum Entwurf des Weißbuchs konsultiert und legte vorläufige informelle Bemerkungen vor. Der EDSB begrüßt, dass seine Ansichten in einem frühen Stadium des Verfahrens eingeholt wurden, und fordert die Kommission auf, dieses bewährte Verfahren fortzusetzen.

4. Das Weißbuch ist Gegenstand einer öffentlichen Konsultation. Ziel der Konsultation ist es, Meinungen zum Weißbuch insgesamt sowie zu bestimmten spezifischen Aspekten einzuholen.

[1] ABl. L 119 vom 4.5.2016, S. 1.
[2] ABl. L 119 vom 4.5.2016, S. 89.
[3] Abl. L 295 vom 21.11.2018, S. 39.
[4] COM(2020) 65 final.
[5] COM(2020) 66 final.
[6] Stellungnahme 3/2020 des EDSB zur europäischen Datenstrategie, https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf

Eine ähnliche öffentliche Konsultation ist zu der Mitteilung der Europäischen Kommission „Eine europäische Datenstrategie“ eingeleitet worden.

5. Die vorliegende Stellungnahme geht näher auf einige der informellen Kommentare des EDSB ein und liefert der Europäischen Kommission vor dem Hintergrund der öffentlichen Konsultation etwas gezielteren Input. Darüber ergeht diese Stellungnahme unbeschadet etwaiger weiterer Bemerkungen, die der EDSB möglicherweise auf der Grundlage weiterer verfügbarer Informationen zu einem späteren Zeitpunkt vorlegt, auch im Zusammenhang mit den künftigen legislativen Konsultationen zu den im Weißbuch und im Arbeitsprogramm der Kommission vorgesehenen Rechtsakten.

6. Obwohl die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union der EU-Datenschutzverordnung (EU-DSVO) und nicht der DSGVO unterliegen, verfolgen beide Verordnungen dieselben Ziele und sind ihre Grundsätze identisch.[7] Um dieser Einheitlichkeit Rechnung zu tragen, wird bei jeder Bezugnahme auf eine Bestimmung der DSGVO in dieser Stellungnahme auch in Klammern die entsprechende Bestimmung der EU-DSVO angegeben.

7. Im Interesse eines **kohärenten Ansatzes in der gesamten Union** empfiehlt der EDSB, dass jeder neue Rechtsrahmen für KI sowohl für die EU-Mitgliedstaaten als auch für die Organe, Einrichtungen und sonstigen Stellen der EU gilt. **Wenn Organe, Einrichtungen und sonstige Stellen der Union künstliche Intelligenz („KI“) nutzen, sollten für sie dieselben Vorschriften gelten wie die in den EU-Mitgliedstaaten.**

2. ALLGEMEINE ZIELE UND VISION

8. Der EDSB begrüßt nachdrücklich die zahlreichen Verweise des Weißbuchs auf einen europäischen Ansatz für KI, der auf den **Werten und Grundrechten der EU** beruht, und die Erwägung, dass die europäischen Datenschutzvorschriften eingehalten werden müssen. Gleichzeitig erwartet der EDSB, dass **diesem klaren Bekenntnis in jedem neuen europäischen Rechtsrahmen für KI umfassend Rechnung getragen wird**, um eine wirksame Achtung der Grundrechte und -werte, darunter Menschenwürde, Pluralismus, Gleichheit, Nichtdiskriminierung, Rechtsstaatlichkeit, ordnungsgemäßes Verfahren und Schutz der Privatsphäre und personenbezogener Daten, zu erreichen.

9. Der EDSB erinnert daran, dass gemäß Artikel 5 DSGVO und Artikel 4 EU-DSVO bei der Verarbeitung personenbezogener Daten stets die **allgemeinen Grundsätze** der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht des Verantwortlichen zu beachten sind.

10. In dem Weißbuch heißt es, dass damit zwei Ziele verfolgt werden, nämlich Festlegung politischer Optionen zur Förderung der Nutzung von KI und Eingehen auf „die mit dieser neuen Technologie einhergehenden Gefahren“. Angesichts dieser Ziele stimmt der EDSB mit der Kommission darin überein, dass der Begriff „KI“ „für die Zwecke dieses Weißbuchs sowie

[7] Soweit die Bestimmungen der Verordnung (EU) 2018/1725 auf denselben Grundsätzen beruhen wie die der Verordnung (EU) 2016/679, sollten diese Bestimmungen der beiden Verordnungen unter Beachtung der Rechtsprechung des Gerichtshofs der Europäischen Union einheitlich ausgelegt werden, insbesondere da der Rahmen der EU-DSVO als dem Rahmen der DSGVO gleichwertig verstanden werden sollte; siehe Erwägungsgrund 5 der EU-DSVO, in dem auf das Urteil des EuGH vom 9. März 2010, *Europäische Kommission gegen Bundesrepublik Deutschland*, Rechtssache C-518/04, ECLI:EU:C:2010:125, Rn. 28, verwiesen wird.

für alle weiteren künftigen politischen Initiativen klar definiert werden“ sollte. Der EDSB bedauert allerdings, dass in dem Dokument mehr als eine Definition zu finden ist und keine von ihnen eindeutig *die eine* Definition ist: Zunächst wird im Weißbuch KI definiert als „Kombination von Daten, Algorithmen und Rechenleistung“; hier ist der EDSB jedoch der Meinung, dass eine solche Begriffsbestimmung zu umfassend ist, da sie auch auf andere Technologien (z. B. „Big Data“) zutrifft. Später bezieht sich das Weißbuch auf die Definitionen in der Mitteilung der Europäischen Kommission „Künstliche Intelligenz für Europa“ und in den Arbeiten der hochrangigen Expertengruppe für KI. Schließlich überlässt das Weißbuch die Aufgabe, KI zu definieren, dem „neuen Rechtsinstrument“. Nach Auffassung des EDSB **hat die Europäische Kommission mit dem Weißbuch eine Gelegenheit verstreichen lassen, eine klare Definition von KI vorzuschlagen**, die als Rahmen für den Umfang der Maßnahmen und mögliche künftige Legislativvorschläge dienen würde. Daher dürfte nur schwer verständlich sein, welchen Anwendungsbereich eventuelle Rechtsvorschriften auf der Grundlage dieses Weißbuchs haben werden. Nach Meinung des EDSB sollten bei einer Bestimmung des Begriffs KI für ein künftiges Rechtsinstrument zumindest folgende Elemente berücksichtigt werden: ein Entscheidungsmodell, ein Algorithmus, der dieses Modell in einen rechnerisch zu erfassenden Code umsetzt, die Daten, die dieser Code als Eingabe verwendet, und die Umgebung, in der es verwendet wird.[8]

11. Für das Erreichen seiner Ziele erklärt das Weißbuch als einen seiner wichtigsten Bausteine die Schaffung eines politischen Rahmens, um „die richtigen Anreize, um die Akzeptanz von KI-Lösungen zu beschleunigen“. Ferner hält es das Weißbuch für „*äußerst wichtig*, dass öffentliche Verwaltungen, Krankenhäuser, Versorgungsbetriebe und Verkehrsdienste, Finanzaufsichtsbehörden und andere Bereiche von öffentlichem Interesse rasch mit der Einführung KI-gestützter Produkte und Dienstleistungen beginnen“.[9] Mit seiner Einstufung von KI als „äußerst wichtiger“ Technologie scheint das Weißbuch davon auszugehen, dass es sich auf jeden Fall um die geeigneteste Technologie handelt, ganz unabhängig von den Geschäftsabläufen einer Behörde und den durch ihre Nutzung entstehenden Gefahren. Nach Ansicht des EDSB **gibt es keine technologische „Wunderwaffe“**. KI ist wie jede andere Technologie ein reines Instrument und sollte so konzipiert werden, dass sie der Menschheit dient. KI bietet wie jede andere Technologie Vor- und Nachteile, und sowohl Behörden und als auch private Einrichtungen sollten von Fall zu Fall prüfen, ob eine KI-Anwendung die beste Option ist, um wichtige Ergebnisse im öffentlichen Interesse zu erzielen.

12. In diesem Sinne heißt es im Weißbuch: „Ein besonderer Schwerpunkt wird auf den Bereichen Gesundheitsfürsorge und Verkehr liegen, **in denen die Technologien so weit ausgereift sind, dass sie in großem Maßstab eingesetzt werden können**.“ (Hervorhebung hinzugefügt). Das Weißbuch enthält keinen Verweis auf wissenschaftliche Nachweise, die eine solche Behauptung stützen, und birgt die Gefahr, dass eine **blinde Akzeptanz** von KI gefördert wird. In dem Weißbuch werden keine Kriterien für die Bewertung der Ausgereiftheit von KI in

[8] Anregungen für diese Elemente sind in folgenden Dokumenten zu finden: HLEG on AI „A definition of Artificial Intelligence: Main capabilities and disciplines“, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341 and AlgorithmWatch, „Automating Society Taking Stock of Automated Decision-Making in the EU (2019)“, https://algorithmwatch.org/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf.
[9] Weißbuch zur KI, Abschnitt 4.F.

bestimmten Anwendungsbereichen definiert.[10] Der EDSB ist daher der Auffassung, dass eine eingehendere und stärker mit Zahlen belegte Analyse auf der Grundlage identifizierter Quellen, als sie derzeit im Weißbuch enthalten ist, die Position der Kommission stärken und der öffentlichen Debatte über das Weißbuch zugute kommen würde, weil die Argumente besser gestützt wären.

13. Der EDSB ist ferner der Auffassung, dass einige KI-Anwendungen (z. B. Live-Gesichtserkennung) die Grundrechte und Grundfreiheiten in einem solchen Ausmaß beeinträchtigen, dass sie den Wesensgehalt dieser Rechte und Freiheiten in Frage stellen können. Aufgrund der noch frühen Phasen der Entwicklung oder Einführung von KI und des Mangels an einem umfassenden Überblick über ihre Auswirkungen auf unsere Gesellschaft sollte sich die Europäische Kommission für eine strikte Anwendung des Vorsorgeprinzips einsetzen. Diese Überlegungen werden in den folgenden Abschnitten weiter ausgeführt.

3. NOTWENDIGKEIT EINES GEÄNDERTEN RECHTSRAHMENS

14. Der EDSB begrüßt die Forderung nach einer **vollständigen und wirksamen Anwendung und Durchsetzung der bestehenden Rechtsvorschriften der EU** sowie nach einer sorgfältigen und objektiven Bewertung der Notwendigkeit etwaiger künftiger legislativer Anpassungen.

15. Der EDSB stimmt auch dem im Weißbuch dargelegten Ansatz zu, wonach es für in der EU betriebene KI-Systeme *„von entscheidender Bedeutung [ist], dass die EU-Vorschriften für alle Akteure gelten, unabhängig davon, ob sie in der EU niedergelassen sind oder nicht“*, da dies mit dem Ansatz der EU-Gesetzgeber für den Schutz personenbezogener Daten, insbesondere mit der DSGVO, im Einklang steht.

16. **Der europäische Rechtsrahmen für den Datenschutz ist technologieneutral und stellt kein Hindernis für die erfolgreiche Einführung neuer Technologien, insbesondere KI, dar.** Er soll vielmehr **die Anwendung jeglicher Technologie** bei der Verarbeitung personenbezogener Daten unter uneingeschränkter Achtung der europäischen Werte und Grundrechte **fördern**.

17. Dem Weißbuch zufolge ist es das Ziel, die Risiken in Verbindung mit der Nutzung von KI zu minimieren, und als größte Risiken werden dort genannt „die Anwendung von Vorschriften zum Schutz von Grundrechten“ und „Fragen der Sicherheit und Haftung“. Bezüglich der ersten Art von Risiken werden später aufgeführt das „Recht auf freie Meinungsäußerung, des Schutzes personenbezogener Daten, der Privatsphäre und politischer Freiheiten“. In Abschnitt 5.B des Weißbuchs werden die Risiken und Situationen beschrieben, bei denen der EU-Rechtsrahmen möglicherweise verbessert werden muss, um eine ordnungsgemäße Durchsetzung zu gewährleisten:

    - Das Risiko in Bezug auf die „ordnungsgemäße Anwendung und Durchsetzung der Rechtsvorschriften der EU und der Mitgliedstaaten“ wird im Zusammenhang mit der

[10] Zieht man die Zahl der seit 2013 durchgeführten Forschungsarbeiten zur Verwendung von KI in der Gesundheitsversorgung als Näherungswert für die Ausgereiftheit heran, findet man recht unterschiedliche Reifegrade (z. B. 531 Studien zur Bildverarbeitung und -analyse, 45 Studien zur pathologischen Analyse oder 10 Studien zum Krankheitsmanagement); siehe Journal of Biomedical Informatics, Band 100, Dezember 2019, „Transforming healthcare with big data analytics and artificial intelligence: A systematic mapping study“, https://www.sciencedirect.com/science/article/abs/pii/S1532046419302308

Opazität von KI beschrieben, auf die weiter unten in Abschnitt 4.3 „Rechenschaftspflicht und Durchsetzung“ eingegangen wird.

- Das Risiko „Einschränkungen des Geltungsbereichs bestehender EU-Rechtsvorschriften“ hebt im Wesentlichen auf den EU-Rechtsrahmen für die Produktsicherheit ab.

- Das im Weißbuch[11] beschriebene Risiko der „Änderung der Funktionalität von KI-Systemen“ ist nicht neu oder gilt nicht nur für KI-Anwendungen. Der EDSB bedauert, dass im Weißbuch nicht näher erläutert wird, warum Software-Upgrades durch Hinzufügung neuer Funktionen andere Konformitätsprobleme aufwerfen als solche mit einer Änderung der Funktionen in Nicht-KI-Systemen.

- Das Risiko der „Unsicherheit hinsichtlich der Aufteilung der Zuständigkeiten...“ dürfte mit den EU-Rechtsvorschriften zur Produktsicherheit in Zusammenhang stehen. Da die Anforderungen der DSGVO von Verantwortlichen und Auftragsverarbeitern im Zusammenhang mit KI-Anwendungen bei der Verarbeitung personenbezogener Daten erfüllt werden müssen, müssen diese Aufgaben eindeutig zugewiesen werden, damit die Zuständigkeiten angemessen zugewiesen werden können. Eine Datenschutz-Folgenabschätzung (DSFA) ist ein nützliches Instrument bei der Zuweisung von Zuständigkeiten.

- Die „Änderungen des Sicherheitskonzepts“ beziehen sich auf „Risiken, die derzeit in den EU-Rechtsvorschriften nicht explizit erfasst sind“ und steht im Zusammenhang mit dem EU-Rechtsrahmen für die Produktsicherheit.

Der Zusammenhang zwischen diesen Risiken und spezifischen Gesetzeslücken, die die Notwendigkeit der neuen Verordnung nach sich ziehen, ist nach wie vor unklar. In der Folgenabschätzung von Vorschlägen für einen KI-Rechtsrahmen sollten solche Verbindungen klar dargestellt werden.

18. Im zweiten Halbjahr 2019 gaben über 350 Organisationen Rückmeldungen[12] zu den Leitlinien der hochrangigen Expertengruppe für vertrauenswürdige KI ab[13]. Im Zusammenhang mit diesem Feedback wird im Weißbuch darauf hingewiesen, dass wesentliche Anforderungen in Bezug auf Transparenz[14], Rückverfolgbarkeit[15] und Kontrolle durch den Menschen[16] in den Leitlinien der hochrangigen Expertengruppe[17] „in vielen Wirtschaftssektoren durch die geltenden Rechtsvorschriften noch nicht ausdrücklich abgedeckt sind“. Nach Auffassung des

[11] „Wenn Software, *einschließlich KI*, in Produkte eingebunden wird, kann dies die Funktionsweise dieser Produkte und Systeme im weiteren Verlauf ihres Lebenszyklus verändern“. (Hervorhebung hinzugefügt).
[12] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57590
[13] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
[14] „Diese Anforderung steht in engem Zusammenhang mit dem Grundsatz der Erklärbarkeit und umfasst die Transparenz von Elementen, die für ein KI-System relevant sind: Daten, System und Geschäftsmodelle.“ HLEGAI Leitlinien (S. 18).
[15] „Die Datensätze und Verfahren, die der Entscheidung des KI-Systems zugrunde liegen, einschließlich der Datensammlung und -kennzeichnung sowie der verwendeten Algorithmen, sollten nach bestmöglichen Standards dokumentiert werden, um die Rückverfolgbarkeit und eine größere Transparenz zu ermöglichen. Dies gilt auch für die Entscheidungen des KI-Systems. Damit können die Gründe ermittelt werden, aus denen eine KI-Entscheidung fehlerhaft war, was wiederum dazu beitragen könnte, künftige Fehler zu vermeiden. Rückverfolgbarkeit erleichtert sowohl die Überprüfbarkeit als auch die Erklärbarkeit.“ HLEG Leitlinien (S. 18).
[16] „KI-Systeme sollten die Autonomie der Menschen und die Entscheidungsfindung unterstützen, wie es der Grundsatz der Achtung der Autonomie der Menschen vorsieht.“ HLEG-Leitlinien (S. 15).
[17] Rückmeldungen aus der öffentlichen Konsultation zu den von der HLEG veröffentlichten Leitlinien zur KI.

EDSB spiegelt die DSGVO die genannten Kernanforderungen in vollem Umfang wider und gilt bei der Verarbeitung personenbezogener Daten sowohl für den privaten als auch für den öffentlichen Sektor. Transparenz ist vorgeschrieben in Artikel 5 Absatz 1 Buchstabe a DSGVO (Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz) [*Artikel 4 Absatz 1 Buchstabe a EU-DSVO*] und in den Artikeln 12 bis 14 DSGVO (Pflicht zur transparenten Information) [*Artikel 14 bis 16 EU-DSVO*], während die Kontrolle durch den Menschen konkret in Artikel 22 DSGVO [*Artikel 24 EU-DSVO*] und ausführlicher in Artikel 5 Absatz 2 DSGVO (Rechenschaftspflicht) [*Artikel 4 Absatz 2 EU-DSVO*] geregelt ist. Hier dürfte also kaum ein Problem für die Datenschutzvorschriften der EU bestehen.

19. Bestimmte Anwendungen der künstlichen Intelligenz, wie z. B. vorausschauende Polizeiarbeit[18] (predictive policing), können negative Auswirkungen haben, wie z. B. eine übertriebene Überwachung von Gruppen und Einzelpersonen. Gleichzeitig sollen Datenschutzvorschriften in erster Linie Einzelpersonen schützen und dürften kaum geeignet sein, Risiken für *Gruppen von Einzelpersonen* zu begegnen. Da keine bestimmte Person diskriminiert wird, wenn beispielsweise ein Stadtviertel allmählich zu einem Gebiet wird, in dem immer häufiger Polizei patrouilliert, könnte auch die Anwendung von Antidiskriminierungsgesetzen schwierig sein. Der EDSB empfiehlt daher, alle KI-bezogenen Vorschriften so konzipieren, dass sie nicht nur Einzelpersonen, sondern auch Gruppen und die Gesellschaft insgesamt **vor *allen* negativen Auswirkungen schützen**. In diesem Zusammenhang fordert der EDSB die Kommission auf, inklusive Governance-Modelle zu entwickeln, die Organisationen, die die Zivilgesellschaft vertreten (z. B. NRO und andere gemeinnützige Vereinigungen), stärken würden, damit sie auch dazu beitragen können, die Auswirkungen von KI-Anwendungen auf bestimmte Gruppen und die Gesellschaft im Allgemeinen zu prüfen.

20. Der EDSB stimmt mit der Kommission darin überein, dass bei jedem künftigen Rechtsrahmen Elemente wie Datenqualität und Rückverfolgbarkeit, Transparenz und Kontrolle durch den Menschen sowie spezifische Kriterien für biometrische Identifikationssysteme berücksichtigt werden müssen. Der EDSB unterstützt diese Anforderungen uneingeschränkt, die einigen der Leitprinzipien entsprechen, die in der von der 40. Internationalen Konferenz der Datenschutzbeauftragten (ICDPPC) in Brüssel[19] angenommenen **Erklärung über Ethik und Datenschutz im Bereich der künstlichen Intelligenz** niedergelegt wurden. Darüber hinaus empfiehlt der EDSB, auch die anderen in der Erklärung des ICDPPC festgelegten Leitprinzipien zu berücksichtigen, wie etwa verantwortungsvolle Gestaltung und Entwicklung durch Anwendung der Grundsätze des Datenschutzes durch Voreinstellungen und des Datenschutzes durch Technik sowie die Ermächtigung des Einzelnen.

21. Der EDSB räumt ein, dass der Einsatz von KI Risiken für ein breites Spektrum von Grundrechten bedeuten kann, zu denen, wenn auch nicht ausschließlich, der Schutz der Privatsphäre und der Schutz personenbezogener Daten gehören.[20] Der EDSB ist jedoch der

[18]AI & Global Governance: Turning the Tide on Crime with Predictive Policing https://cpr.unu.edu/ai-global-governance-turning-the-tide-on-crime-with-predictive-policing.html

[19]Https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_ai-declaration_adopted_en_0.pdfDie Internationale Konferenz der Datenschutzbeauftragten, inzwischen umbenannt in Global Privacy Assembly, ist seit mehr als vier Jahrzehnten das wichtigste globale Forum für Datenschutzbehörden.

[20] Siehe ferner das Papier der Agentur für Grundrechte „Facial recognition technology: fundamental rights considerations in the context of law enforcement“, 27. November 2019, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

Ansicht, dass darüber hinaus eine verstärkte Überwachung und missbräuchliche Formen der Governance (z. B. durch die Klassifizierung des maschinellen Lernens und die Vorhersage des Verhaltens von Einzelpersonen mit oder ohne Gesichtserkennung) ebenfalls als wichtige Risikofaktoren für KI betrachtet werden sollten, z. B. wegen ihrer potenziellen abschreckenden Wirkung auf verschiedene andere Grundrechte. Ferner werden im Weißbuch zwar zwei Risikoquellen für den Einzelnen genannt – voreingenommene Datensätze und fehlerhafte Gestaltung des KI-Systems –, doch ist der EDSB der Auffassung, dass auch andere Risikoquellen berücksichtigt werden sollten, einschließlich fehlerhafter Datenqualität oder der Risiken, die sich aus der Nutzung der KI ergeben (wie die Neigung des Menschen, blind auf automatisierte Entscheidungssysteme zu vertrauen[21]).

22. Der EDSB teilt zwar die Auffassung, dass Voreingenommenheiten auch KI-Systeme, die „lernen", während sie angewendet werden, beeinträchtigen könnten, doch geht das Weißbuch noch weiter und besagt, dass, wenn das KI-System „lernt", während es angewendet wird, „die Risiken, wenn dies *in der Entwurfsphase nicht hätte verhindert oder vorhergesehen werden können*, nicht aus Fehlern in der ursprünglichen Auslegung des Systems, sondern aus den praktischen Folgen der Korrelationen oder Muster, die das System in großen Datensätzen identifiziert, resultieren". (eigene Hervorhebung) Der EDSB stimmt dieser Einschätzung nicht zu. **Bei der Gestaltung von KI-Anwendungen sollten potenzielle Voreingenommenheiten bei den Schulungsdaten und gegebenenfalls bei den Betriebsdaten berücksichtigt werden.** Voreingenommenheiten können und müssen *während des Betriebs* von KI-Anwendungen ebenso gemessen und korrigiert werden, wie sie während ihrer Entwicklung gemessen und korrigiert werden können[22].

4. BEWERTUNG DES KÜNFTIGEN RECHTSRAHMENS FÜR KI

4.1. Vorsorgeprinzip und risikobasierter Ansatz

23. Das Weißbuch folgt einem risikobasierten Ansatz, „um die Verhältnismäßigkeit des regulatorischen Eingreifens zu gewährleisten", um also die Anwendbarkeit des vorgeschlagenen Rechtsrahmens einzuschränken. Mit dem Weißbuch sollen zusätzlich zu den bestehenden Anforderungen bestimmte rechtliche Anforderungen für KI-Anwendungen *mit hohem Risiko* hinzugefügt werden.

24. In Bezug auf die Risiken, die von KI-Anwendungen, die personenbezogene Daten verarbeiten, für betroffene Personen ausgehen, erscheint eine solche ergänzende Regulierung unnötig, da der risikobasierte Ansatz, der bereits in den Artikeln 32 (Sicherheit der Verarbeitung) und 35 (Datenschutz-Folgenabschätzung) DSGVO [*Artikel 33 und 39 EU-DSVO*] verankert ist, makellos ist und an die spezifischen Bedürfnisse der einzelnen Anwendungen anzupassen ist.

[21] „Der vermeintlich verlässliche Charakter der auf Mathematik beruhenden KI-Lösungen veranlasst diejenigen, die Entscheidungen auf der Grundlage der Ergebnisse von Algorithmen treffen, das Bild des Einzelnen und der Gesellschaft zu glauben, das die Analysen nahelegen. Darüber hinaus kann diese Haltung durch das Risiko potenzieller Sanktionen für eine Entscheidung verstärkt werden, bei der die Analyseergebnisse außer Acht gelassen werden." AI and data protection: Challenges and envisaged remedies. Im Auftrag des Europarates erstellter Bericht von Professor Alessandro Mantelero. https://rm.coe.int/report-on-artificial-intelligence-artificial-intelligence-and-data-pro/16808b2e39 https://rm.coe.int/report-on-artificial-intelligence-artificial-intelligence-and-data-pro/16808b2e39

[22] Tay, der KI-Chatbot von Microsoft, erhält von Twitter einen Schnellkurs in Rassismus https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter?CMP=twt_a-technology_b-gdntech

Im Februar 2020 kam der EDSA zu dem Schluss[23], dass „es verfrüht ist, den Rechtstext zum gegenwärtigen Zeitpunkt zu überarbeiten".

25. In der risikobasierten Strategie des Weißbuchs heißt es (S. 21): „Die verbindlichen Anforderungen des neuen Rechtsrahmens für KI (s. u. Abschnitt D) würden grundsätzlich *nur* für diejenigen Anwendungen gelten, die nach den beiden *kumulativen* Kriterien des Hochrisiko*sektors* und der *Nutzung und Wirkung* der KI-Anwendung als Anwendungen mit hohem Risiko eingestuft wurden (eigene Hervorhebung).

26. Der EDSB schlägt Folgendes für den Fall vor, dass ein neuer Rechtsrahmen angenommen werden sollte:

27. Bezüglich der *kumulativen* Kriterien für ein hohes Risiko ist der EDSB der Auffassung, dass das Konzept des „hohen Risikos" im Weißbuch zu eng gefasst ist, da es Einzelpersonen davon ausschließt, angemessen vor KI-Anwendungen geschützt zu werden, die ihre Grundrechte verletzen könnten. Im Weißbuch wird eingeräumt, dass die Definition nicht vollständig alles abdeckt, denn dort heißt es: „Es kann auch Ausnahmefälle geben, in denen aufgrund der immanenten Risiken der Einsatz von KI-Anwendungen für bestimmte Zwecke grundsätzlich als hochriskant einzustufen ist."

28. Nach Auffassung des EDSB sollte der Ansatz zur Bestimmung des Risikoniveaus bei der Nutzung von KI-Anwendungen **robuster** und **differenzierter** sein, und die *Leitlinien* des Europäischen Datenschutzausschusses *zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt"*.[24]

29. Vor dem Hintergrund des Vorsorgeprinzips empfiehlt der EDSB daher, das Verfahren zur Bestimmung des hohen Risikos bei der Verarbeitung personenbezogener Daten wie folgt zu ändern:

    - Um das Kriterium „schädliche Nutzung und Wirkung" des Weißbuchs zu erfüllen, sollte der Verantwortliche verpflichtet werden, eine Datenschutz-Folgenabschätzung durchzuführen, um festzustellen, ob die KI-Anwendung als hochriskant einzustufen ist.
    - Die Kriterien zur Bestimmung des Risikoniveaus sollten den genannten Leitlinien des Europäischen Datenschutzausschusses entsprechen und daher Folgendes umfassen: Bewertung oder Einstufung; automatisierte Entscheidungsfindung mit rechtlichen oder ähnlichen erheblichen Auswirkungen; systematische Überwachung; sensible Daten; Daten, die in großem Maßstab verarbeitet werden; abgeglichene oder kombinierte Datensätze; Daten über gefährdete betroffene Personen; innovative Nutzung oder Anwendung technologischer oder organisatorischer Lösungen; grenzüberschreitende Datenübermittlung außerhalb der Europäischen Union; die Frage, ob die Verarbeitung

[23] Beitrag des EDSA zur Bewertung der DSGVO nach Artikel 97 (S. 4) https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en

[24] Der Europäische Datenschutzausschuss billigte die von der Artikel 29-Datenschutzgruppe 2017 verfassten Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und zur Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" auf seiner ersten Plenarsitzung am 25. Mai 2018.https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

an sich die betroffenen Personen daran hindert, ein Recht auszuüben oder eine Dienstleistung oder einen Vertrag in Anspruch zu nehmen.

- Darüber hinaus sollte die Kommission anerkennen, dass „Risiken im Zusammenhang mit potenziellen negativen Auswirkungen auf die Rechte, Freiheiten und Interessen der betroffenen Person unter Berücksichtigung spezifischer objektiver Kriterien wie der Art der personenbezogenen Daten (z. B. sensible oder nicht sensible Daten), der Kategorie der betroffenen Person (z. B. minderjährig oder nicht), der Zahl der betroffenen Personen und des Zwecks der Verarbeitung bestimmt werden sollten. Die Schwere und Wahrscheinlichkeit der Auswirkungen auf die Rechte und Freiheiten der betroffenen Person sind Elemente, die bei der Bewertung der Risiken für die Privatsphäre der betroffenen Person zu berücksichtigen sind.“[25]
- Das im Weißbuch genannte Kriterium des „Sektors“ sollte nicht als Kriterium, sondern vielmehr als Anhaltspunkt dafür dienen, dass *standardmäßig* eine Bewertung (im Wege einer DSFA) der durch die KI-Anwendung entstehenden Risiken erforderlich ist und dass ein solches Risiko noch schwerwiegender sein könnte als in einem anderen Sektor.

30. Auch der Begriff des Risikos von Auswirkungen scheint im Weißbuch zu eng definiert zu sein. Abgesehen von den „Auswirkungen auf die betroffenen Parteien“ ist der EDSB der Auffassung, dass sich die Bewertung des Risikos einer bestimmten Nutzung von KI auch auf **umfassendere gesellschaftliche Erwägungen** stützen sollte, einschließlich der Auswirkungen auf den demokratischen Prozess, das ordnungsgemäße Verfahren und die Rechtsstaatlichkeit, das öffentliche Interesse, das Potenzial für eine verstärkte allgemeine Überwachung, die Umwelt[26] und (Konzentrationen von) Marktmacht.

31. Bezüglich der Auswirkungen speziell auf den Einzelnen räumt das Weißbuch ein, dass der durch KI verursachte Schaden sowohl materieller als auch immaterieller Art sein kann.[27] In Bezug auf die Art des Schadens, der bei der Bestimmung des (hohen) Risikostatus berücksichtigt wird, geht das Weißbuch jedoch von einer viel geringeren Bandbreite von Schäden und Risiken aus.[28] Bei der Beantwortung der Frage, ob KI-Anwendungen als hochriskant einzustufen sind, empfiehlt der EDSB der Kommission, sich nicht auf derart enge Erwägungen zu beschränken und die **sehr große Bandbreite von Schäden und Risiken, denen Einzelpersonen ausgesetzt sind**, zu berücksichtigen.

32. Ferner wird im Weißbuch zwar eingeräumt (S. 13), dass KI-Anwendungen aufgrund von „Fehlern in der Gestaltung der KI-Systeme [...] oder von Fehlern bei der Verwendung von Daten riskant sein können, wenn etwaige Verzerrungen nicht korrigiert werden“, doch

[25] Artikel 29-Datenschutzgruppe, 2014, *Erklärung über die Rolle eines risikobasierten Ansatzes in Rechtsrahmen für den Datenschutz*, S. 4.

[26] Die Umweltauswirkungen des Trainings einer KI-Anwendung und des ausgiebigen Einsatzes von KI könnten den Umweltzielen der EU abträglich sein:https://www.technologyreview.com/2019/06/06/239031/training-a-single-ai-model-can-emit-as-much-carbon-as-five-cars-in-their-lifetimes/

[27] „können sowohl materiell (Sicherheit und Gesundheit des Einzelnen, einschließlich Verlust von Menschenleben, Sachschäden) als auch immateriell (Verlust der Privatsphäre, Einschränkung des Rechts auf freie Meinungsäußerung, Menschenwürde, Diskriminierung z. B. beim Zugang zu Beschäftigung) sein und sich in einer Vielzahl von Risiken manifestieren“, Weißbuch S. 12.

[28] „...rechtliche oder ähnlich erhebliche Auswirkungen auf die Rechte einer natürlichen Person oder eines Unternehmens,Verletzungs- oder Lebensgefahr oder erheblicher immaterieller Schaden, Anwendungen, deren Auswirkungen von natürlichen oder juristischen Personen realistischerweise nicht vermieden werden können.“ Weißbuch, S. 21.

empfiehlt der EDSB, auch anzuerkennen, dass KI-Anwendungen Risiken verursachen können, weil sie parteiisch oder sogar willkürlich sind, Variablen falsch zuordnen oder bestimmte Daten nicht klassifiziert werden. Darüber hinaus sollte anerkannt werden, dass *allein die Übertragung* von Aufgaben auf Maschinen (hier KI), die zuvor Menschen zugewiesen wurden, Risiken mit sich bringen kann. **Die Entscheidung, ein gesellschaftliches Problem mit einer KI-Anwendung „zu lösen", birgt zusätzliche Risiken, die gegen jegliche vermeintliche Effizienzsteigerung abzuwägen sind.**

So erfordern diese Systeme beispielsweise riesige Datenmengen, die erhoben und gespeichert werden müssen, wodurch Risiken für Privatsphäre und Datenschutz entstehen; KI-Anwendungen sind möglicherweise nicht in der Lage, menschliche Faktoren zu berücksichtigen, die sich nicht aus den Daten ergeben; KI-Anwendungen können von übermäßigem Vertrauen der Menschen profitieren und den Anschein der objektiven Wahrheit oder der wissenschaftlichen Zuverlässigkeit erwecken. Wenn also die KI-Anwendung personenbezogene Daten verarbeitet, sollte es Belege für die Notwendigkeit und Verhältnismäßigkeit dieser Verarbeitung geben.[29]

33. In Bezug auf den neuen Rahmen, der *nur* für KI-Anwendungen *mit hohem Risiko* gilt, werden im Weißbuch *spezifische* Risiken und Schäden eingeräumt, die von KI-Anwendungen ausgehen können (siehe oben auf S. 15). Zu diesem Zweck schlägt es vor, bestimmte EU-Rechtsvorschriften zu aktualisieren und, sofern nicht alle Risiken und Schäden von den bestehenden Rechtsvorschriften abgedeckt würden, in einem neuen „Rechtsrahmen für KI" KI-spezifische Garantien vorzuschlagen.

34. Die im Weißbuch (in Abschnitt B) vorgeschlagenen Aktualisierungen der EU-Rechtsvorschriften decken jedoch nicht alle diese Schäden und Risiken ab, und die neuen Garantien (in Abschnitt D) decken nur die Risiken ab, die von KI-Anwendungen *mit hohem Risiko* ausgehen. Nach dem Verständnis des EDSB erkennt das Weißbuch zwar eine Vielzahl von Risiken und Schäden an, die speziell von KI-Anwendungen ausgehen, doch würden die von ihm vorgeschlagenen Maßnahmen nur einen Teil davon betreffen, nämlich die Kategorie „mit hohem Risiko".

35. Dieser Ansatz spiegelt nicht den Vorsorgeansatz wider, den die Europäische Union bei den Rechtsvorschriften über den Schutz personenbezogener Daten verfolgt.[30] Der in der DSGVO (und in der EU-DSVO) gewählte Ansatz ist ebenfalls risikobasiert, doch entscheidend ist, dass er abgestuft ist, während das KI-Weißbuch anscheinend einen „Alle oder nichts"-Ansatz verfolgt:

    - Die Vorschriften der DSGVO gehen davon aus, dass es keine Verarbeitung personenbezogener Daten mit einem „Nullrisiko" gibt. Jede Verarbeitung personenbezogener Daten birgt Risiken (wenn auch möglicherweise nur minimale Risiken), insbesondere eine automatisierte Verarbeitung, und insbesondere bei Einsatz neuer Technologien. Daher gibt es eine Reihe von Verpflichtungen, die in jedem Fall bei allen Verarbeitungstätigkeiten erfüllt werden sollten. *Darüber hinaus gilt*: Steigen die Risiken (hochriskant), nehmen auch die Verpflichtungen zu.

[29] Der Grund für die Einführung des KI-Systems sollte klar dargelegt und im Falle von Kosteneffizienz und Wirksamkeit gut belegt werden.
[30] Siehe insbesondere Artikel 29-Datenschutzgruppe, 2014, Erklärung zur Rolle eines risikobasierten Ansatzes in Rechtsrahmen für den Datenschutz, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

- Im Gegensatz zu diesem Ansatz scheint im Weißbuch vorgeschlagen zu werden, dass nur KI-Anwendungen mit hohem Risiko besondere zusätzliche Verpflichtungen (zusätzlich zu den bereits geltenden) erfordern und dass die zusätzlichen Verpflichtungen im Falle eines Schwindens der Risiken entfallen.

36. Das in der EU traditionell angewandte Vorsorgeprinzip[31] verlangt vorsorgliche Maßnahmen, wenn 1) unbekannte Risiken nicht bewertet werden können oder 2) schwerwiegende Risiken bestehen, die Wahrscheinlichkeit eines Eintretens jedoch nicht ausreichend vorhergesagt werden kann. Das Vorsorgeprinzip senkt in der Praxis den Schwellenwert für regulatorische (regulatorische oder sonstige) Eingriffe[32], und seine Anwendung auf den KI-Kontext erscheint besonders wichtig.[33] Der EDSB ist daher der Auffassung, dass die Risiken und Schäden, die die Voraussetzungen für eine Einstufung als „hohes Risiko" nicht erfüllen, *dessen ungeachtet* so weit wie möglich vermieden oder gemindert werden müssen. Zu diesem Zweck schlägt der EDSB Folgendes vor: Sollte die Kommission einen neuen KI-spezifischen Rechtsrahmen vorlegen, sollte eine Reihe angemessener Garantien für *alle* KI-Anwendungen *unabhängig* vom Risikoniveau gelten, wie etwa vollständige Transparenz bestehender technischer und organisatorischer Maßnahmen (einschließlich Dokumentation[34]) in Bezug auf die Ziele, die Verwendung und die Gestaltung eingesetzter algorithmischer Systeme[35]; Gewährleistung der Robustheit des KI-Systems; oder Umsetzung von und Transparenz bezüglich der verfügbaren Regelungen für Rechenschaftspflicht, Rechtsbehelf und unabhängige Aufsicht.

37. Während die Kommission in ihrem KI-Ansatz darauf abzielt, „nicht übermäßig präskriptiv" zu sein, um „insbesondere für KMU einen unverhältnismäßigen Aufwand" zu vermeiden (S. 20), könnte das Ergebnis eines solchen Ansatzes stattdessen zu einer unverhältnismäßigen Belastung der Grundrechte und Interessen des Einzelnen führen. Der EDSB schlägt vor, sich an der ähnlichen Debatte während der Diskussionen und Verhandlungen über die Datenschutz-Grundverordnung zu orientieren, und ist der Auffassung, dass der sich daraus ergebende **abgestufte Ansatz in der DSGVO ein besseres Gleichgewicht zwischen Lasten und Nutzen schafft**.

[31] Das Vorsorgeprinzip wird von der Kommission als anwendbar betrachtet, wenn „wissenschaftliche Erkenntnisse unzureichend, nicht schlüssig oder unsicher sind und aufgrund einer vorläufigen objektiven wissenschaftlichen Bewertung Hinweise darauf vorliegen, dass begründete Bedenken bestehen, dass die potenziell gefährlichen Auswirkungen (...) nicht mit dem gewählten Schutzniveau vereinbar sein könnten." Siehe Europäische Kommission, Mitteilung über das Vorsorgeprinzip (KOM(2000) 1 endg.), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52000DC0001&from=DE.

[32] Anstelle von Verboten, Moratorien oder Ausstiegsmaßnahmen können Vorsorgemaßnahmen genauso einfach in Form strengerer Normen, Eindämmungsstrategien, Lizenzvereinbarungen, Überwachungsmaßnahmen, Kennzeichnungsvorschriften, Haftungsbestimmungen oder Entschädigungsregelungen erfolgen. Siehe Artikel 191 Absatz 2 AEUV; vgl. ferner Rechtssache C-180/96. Vereinigtes Königreich gegen Kommission, 1998 Slg. I-2269, Rn. 99.

[33] Der EDSB ist der Auffassung, dass dieser Grundsatz auf die Risiken für die Privatsphäre und den Schutz personenbezogener Daten anwendbar ist, und schlägt daher vor, seine Anwendung in Bezug auf die von KI ausgehenden Risiken zu prüfen. Siehe Leitlinien des EDSB zur Verhältnismäßigkeit, Fußnote 53, Seite 24: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

[34] Eine transparente Dokumentation ist ein unerlässliches internes Instrument für Verantwortliche, um der Rechenschaftspflicht wirksam nachzukommen, und für Ex-post-Kontrollen durch Datenschutzbehörden sowie für die Ausübung der Rechte durch betroffene Personen. Sie geht über die Informationen hinaus, die den betroffenen Personen zur Verfügung gestellt werden müssen, und könnte den Schutz erhöhen, bis ein vollwertiger Ex-ante-Überprüfungsmechanismus – mit all seinen erforderlichen Ressourcen, Kenntnissen und dem nötigen politischen Konsens – verwirklicht ist.

[35] Geschäftsgeheimnisse und Rechte des geistigen Eigentums schützen nur teilweise gegen Transparenzanforderungen und können nur insoweit geltend gemacht werden, als dies zum Schutz der Interessen ihrer Inhaber unbedingt erforderlich ist.

38. Der EDSB weist ferner darauf hin, dass der Schutz der Grundrechte in bestimmten Fällen nicht nur spezifische Garantien, sondern auch **eine klare Beschränkung der Nutzung von KI rechtfertigen könnte, wenn bestimmte Nutzungen der Technologie offensichtlich mit den Grundrechten unvereinbar sind**.[36] Der EDSB schlägt daher vor, einige hochriskante KI-Szenarien **von vornherein zu untersagen**: Gemäß dem europäischen Vorsorgeprinzip und insbesondere dann, wenn die Auswirkungen auf den Einzelnen und die Gesellschaft insgesamt noch nicht vollständig bekannt sind, sollte ein vorübergehendes Verbot in Erwägung gezogen werden. Nach Ansicht des EDSB sollten diese potenziellen Situationen in einem möglichen künftigen Rechtsrahmen ausdrücklich behandelt werden. Der EDSB schlägt in diesem Zusammenhang vor, den von der Deutschen Datenethikkommission vorgeschlagenen „vorsichtigen" und „risikoangepassten" Ansatz zu übernehmen und algorithmische Systeme „mit unhaltbarem Schadenspotenzial" ganz oder teilweise zu verbieten.[37]

39. Neben neuen Anforderungen, die die Kommission möglicherweise für KI-Anwendungen festlegt, und im Einklang mit den Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte sollte die Kommission auch die **Pflicht des Privatsektors** hervorheben, **die gebotene Sorgfalt walten zu lassen und kontinuierliche, dokumentierte, proaktive und reaktive Maßnahmen zum Schutz der Menschenrechte zu ergreifen**. Risikobewertungen, die in technischen Umgebungen, in denen sich die Betreiber mit ihren eigenen operativen Risiken befassen, sehr sinnvoll sind, entsprechen möglicherweise nicht der Bandbreite, die für die Bewertung der Auswirkungen auf die Grundrechte erforderlich ist, und eine Datenschutz-Folgenabschätzung (DSFA) (bei der gegebenenfalls auch andere Rechte als das Recht auf Datenschutz berücksichtigt werden) ist angemessener.

4.2. Datenschutz-Folgenabschätzung

40. Die DSFA gemäß Artikel 35 DSGVO [*Artikel 39 EU-DSVO*] ist ein Instrument für das **Management von Risiken** für die Rechte und Freiheiten des Einzelnen. Eine DSFA ist vor der Verarbeitung von Daten unter Verwendung innovativer Technologien obligatorisch, wenn die Verarbeitung wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten des Einzelnen führen wird. Der EDSB bedauert, dass DSFA im Weißbuch nicht ausdrücklich erwähnt werden, obwohl es sich ja dazu bekennt, die von KI ausgehenden Risiken betreffend „die Anwendung von Vorschriften zum Schutz von Grundrechten" so gering wie möglich zu halten.

41. Die Einführung von KI-Systemen dürfte höchstwahrscheinlich mindestens eines der in Artikel 35 Absatz 3 DSGVO [*Artikel 39 Absatz 3 EU-DSVO*] festgelegten Kriterien erfüllen.[38] Darüber hinaus gibt Artikel 35 Absatz 4 DSGVO [*Artikel 39 Absatz 4 EU-DSVO*] den Datenschutzaufsichtsbehörden der einzelnen EU-Mitgliedstaaten (und dem EDSB) die Möglichkeit, eine Liste von Arten von Verarbeitungsvorgängen zu veröffentlichen, für die

[36]Der EDSB schlägt ferner vor, dass in Bezug auf die Verwendung einer KI-Anwendung ethische Überlegungen angestellt werden sollten.

[37]https://datenethikkommission.de/wp-content/uploads/191023_DEK_Kurzfassung_en_bf.pdf

[38] Datenverarbeitungstätigkeiten sind DSFA-pflichtig, wenn 1) eine systematische und umfassende Bewertung persönlicher Aspekte einer Person auf der Grundlage einer automatisierten Verarbeitung einschließlich Profiling erfolgt und ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung oder ähnlich erhebliche Wirkung entfalten, 2) eine umfangreiche Verarbeitung sensibler Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten erfolgt oder 3) die Verarbeitung eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche umfasst.

eine DSFA vorgeschrieben ist. Der EDSB hat detaillierte Leitlinien für die Beantwortung der Frage veröffentlicht, wann die Durchführung einer DSFA obligatorisch ist.[39] Unter anderem verlangen die Aufsichtsbehörden Polens, Italiens, Griechenlands, Österreichs und der Tschechischen Republik eine DSFA für einige oder alle Nutzungen von KI-Anwendungen. (Beispielsweise ist in Polen eine DSFA für die „Beurteilung der Kreditwürdigkeit unter Verwendung von KI-Algorithmen" erforderlich, während in der Tschechischen Republik eine solche DSFA für „automatisierte Expertensysteme einschließlich KI" erforderlich ist, wenn sie für die Analyse oder Profilerstellung von IT-KI-Systemen verwendet werden).

42. Artikel 35 DSGVO [*Artikel 39 EU-DSVO*] spricht von einem voraussichtlich hohen Risiko „für die Rechte und Freiheiten natürlicher Personen". Die Bezugnahme auf die „Rechte und Freiheiten" betroffener Personen **betrifft in erster Linie das Recht auf Datenschutz und Privatsphäre**, **kann aber auch andere Grundrechte** wie Meinungsfreiheit, Gedankenfreiheit, Freizügigkeit, Diskriminierungsverbot, Recht auf Freiheit, Gewissensfreiheit und Religion **umfassen**.[40]

43. Es sei darauf hingewiesen, dass die Anforderungen der DSGVO an eine DSFA nicht nur eine Risikobewertung, sondern auch eine detaillierte Beschreibung der geplanten Datenverarbeitung umfassen. Der Teil Risikobewertung befasst sich mit der Ermittlung der Risiken und den Maßnahmen zur Bewältigung und Minderung dieser Risiken. Die Risiken müssen gegeneinander abgewogen werden und einen Wert oder eine Punktzahl erhalten, der/die sie skalierbar macht. Dieser Wert sollte sich nach der Wahrscheinlichkeit und Schwere der Risiken richten. Die Beschreibung der geplanten Datenverarbeitung sollte Auskunft über den Umfang, die Art, den Kontext und die Zwecke der Datenverarbeitung geben.

44. Die DSFA erfordert ferner eine **Prüfung der Notwendigkeit und Verhältnismäßigkeit** der Verarbeitung. Die Prüfung der Notwendigkeit sollte erbringen, dass der Einsatz von KI tatsächlich das am besten geeignete Instrument ist, um das Ziel einer spezifischen Datenverarbeitung zu erreichen. Wenn es andere, weniger einschneidende Methoden mit geringeren potenziellen Risiken gibt, die ebenfalls dazu beitragen könnten, den Zweck der Verarbeitung zu erreichen, muss mit spezifischen Argumenten belegt werden, warum sich der Verantwortliche für die Nutzung von KI entschieden hat.

    Bei der Prüfung der Verhältnismäßigkeit sollte eine ganze Reihe von Faktoren berücksichtigt werden, insbesondere:

    - das Interesse der Verantwortlichen sowie die Rechte und Freiheiten der natürlichen Personen und
    - die vernünftigen Erwartungen der Personen und der Zweck der Datenverarbeitung.

[39] Die Artikel 29-Datenschutzgruppe hat ein Dokument mit dem Titel „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" angenommen, das detaillierte Aussagen dazu enthält, wie und wann eine DSFA durchzuführen ist.

[40] Europäischer Datenschutzausschuss, „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt"", WP 248 rev.01.

Der EDSB weist auf Folgendes hin: Ergibt die Datenschutz-Folgenabschätzung, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen würde, es sei denn, der Verantwortliche ergreift Maßnahmen zur Minderung des Risikos, besteht die Verpflichtung zur Konsultation der Aufsichtsbehörde gemäß Artikel 36 Absatz 1 DSGVO [*Artikel 40 EU-DSVO*]. **Der EDSB schlägt daher vor, dass in einem künftigen Rechtsrahmen die Anforderung einer Folgenabschätzung für *jede* geplante Einführung von KI-Systemen festgelegt werden sollte.** Geht es um die Verarbeitung personenbezogener Daten, ist den Anforderungen der DSGVO an eine DSFA Genüge zu tun; in anderen Situationen sollte die vorgeschlagene KI-Folgenabschätzung die folgenden Hauptbestandteile enthalten:

1. Ermittlung der betroffenen Grundrechte
    a. Welche Grundrechte sind betroffen oder potenziell betroffen?
    b. Welcher Art sind diese Grundrechte? Ist ein absolutes Recht betroffen?
2. Ermittlung der Risiken für diese Rechte in der Entwicklungsphase und in der Einführungsphase
    a. Welche Risikofaktoren gibt es?
    b. Wie hoch ist die Wahrscheinlichkeit, dass die Risiken offenkundig werden?
    c. Inwieweit würden sich die Risiken auf die Grundrechte auswirken?
3. Ermittlung der Maßnahmen zur Minderung der Auswirkungen auf die betroffenen Rechte
    a. Welche technischen oder organisatorischen Methoden stehen zur Verfügung, um sicherzustellen, dass der Wesensgehalt der Grundrechte nicht beeinträchtigt wird?
4. Abwägen von Interessen und Risiken
    a. Welche positiven/negativen Auswirkungen hat die Einschränkung auf die Grundrechte?
    b. Welche positiven/negativen Auswirkungen hat die Verarbeitung für den Einzelnen?[41]

Nach Auffassung des EDSB steht die Einführung einer solchen Risikobewertung mit der Strategie der Kommission zur besseren Umsetzung der Charta der Grundrechte durch die Europäische Union im Einklang.[42] Obwohl es sich eigentlich nicht um eine völlig neue Idee handelt, sollte doch ihre Anwendung für die Verarbeitung personenbezogener Daten unter Verwendung von KI in Erwägung gezogen werden, da die Technologie schwerwiegende Auswirkungen hat und innovativ ist.

45. Schließlich empfiehlt der EDSB, nach Möglichkeit die Ergebnisse solcher Bewertungen oder zumindest die wichtigsten Ergebnisse und Schlussfolgerungen der DSFA als vertrauens- und transparenzsteigernde Maßnahme **zu veröffentlichen**.

[41] Siehe Heleen L. Janssen, *„An approach for a fundamental rights impact assessment to automated decision-making*“, International Data Privacy Law, Band 10, Ausgabe 1, Februar 2020, Seiten 76–106, https://doi.org/10.1093/idpl/ipz028.
[42] Mitteilung der Europäischen Kommission, *„Strategie zur wirksamen Umsetzung der Charta der Grundrechte durch die Europäische Union*“, KOM(2010) 573 endg., Brüssel, 19.10.2010.

4.3. Rechenschaftspflicht und Durchsetzung

46. Auf Seite 11 des Weißbuchs heißt es, dass „bestimmte Besonderheiten der KI (z. B. die Opazität) die Anwendung und Durchsetzung dieser Rechtsvorschriften erschweren“ können. Dem Dokument zufolge müsste bei solchen Schwierigkeiten bei der Durchsetzung geprüft werden, „ob die geltenden Rechtsvorschriften den KI-Risiken gewachsen sind und wirksam durchgesetzt werden können oder ob sie angepasst werden müssen bzw. neue Rechtsvorschriften erforderlich sind“.

47. Auf Seite 14 des Weißbuchs werden die problematischen Merkmale, die bei vielen KI-Anwendungen auftreten, näher ausgeführt, wobei unter anderem „Opazität („Blackbox-Effekt“), Komplexität, Unvorhersehbarkeit und teilautonomes Verhalten“ aufgeführt werden und darauf hingewiesen wird, dass sie „die Prüfung der Vereinbarkeit und die wirksame Durchsetzung von EU-Rechtsvorschriften zum Schutz der Grundrechte erschweren“. Solche Merkmale sind jedoch nicht ausschließlich KI-Anwendungen vorbehalten. So kann beispielsweise die Verarbeitung personenbezogener Daten durch Big Data-Techniken genauso komplex sein, und manche Anwendungen, die keine KI nutzen (z. B. solche für das Management automatisierter Züge[43]), sind teilweise oder vollständig autonom.

48. Die Opazität, die einigen Arten von AI-Anwendungen zugeschrieben wird, hat mit der Unfähigkeit des Menschen zu tun, die Gründe für die Entscheidung einer KI-Anwendung zu erklären. Dieses Problem ergibt sich aus der Art und Weise, in der diese Anwendungen das Wissen und die Erfahrung darstellen, auf die sie bei ihren Entscheidungen zurückgreifen. Der EDSB schlägt daher vor, dass die in Abschnitt 5.F im Zusammenhang mit vorab vorzunehmenden Konformitätsbewertungen erwähnten **transparenten Test- und Prüfverfahren** Teil jeder KI-Anwendung sein sollten, mit der personenbezogene Daten verarbeitet werden. Die öffentliche Verfügbarkeit solcher Verfahren würde sicherstellen, dass die Aufsichtsbehörden ihre Aufgaben wahrnehmen können, würden aber auch das Vertrauen der Nutzer in die KI-Anwendungen stärken.

49. Für den Fall. dass, wie es im Weißbuch heißt, Opazität oder andere KI-spezifische Merkmale eine Überarbeitung der bestehenden Rechtsvorschriften erforderlich machen sollten, **unterstreicht der EDSB die Notwendigkeit einer gründlichen Analyse der Regulierungslücken in den Folgenabschätzungen**, wie sie in den Leitlinien der Kommission für eine bessere Rechtsetzung[44] und in der Interinstitutionellen Vereinbarung zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Europäischen Kommission über bessere Rechtsetzung[45] gefordert werden. Eine solche Analyse würde die relevanten KI-Merkmale, die Lücken in den zu ändernden geltenden Rechtsvorschriften und den Ansatz der vorgeschlagenen Änderungen beschreiben, mit denen diese Lücken geschlossen werden sollen.

50. Im Weißbuch wird die Frage gestellt, ob zuständige Behörden und betroffene Einzelpersonen „nachvollziehen können, wie eine bestimmte Entscheidung unter Einsatz von KI gefällt wurde, und somit auch nicht verifizieren können, ob die einschlägigen Vorschriften eingehalten wurden“. Der EDSB erinnert an den der DSGVO zugrunde liegenden Grundsatz der

[43] https://en.wikipedia.org/wiki/List_of_automated_train_systems
[44] https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox_en
[45] ABl. L 123 vom 12.5.2016, S. 1.

Rechenschaftspflicht, wonach der Verantwortliche die Einhaltung der DSGVO nachweisen muss. Behauptungen über das Fehlen einer menschlichen (oder sonstigen) diskriminierenden Voreingenommenheit einer KI-Anwendung sollten nachprüfbar sein.[46]

51. Das Weißbuch äußert Bedenken[47] wegen eines eventuellen Mangels an den für die Durchsetzung bestehender Vorschriften über KI erforderlichen Mitteln. Der EDSB teilt diese Bedenken und betont, dass die Aufsichtsbehörden mit den erforderlichen Mitteln ausgestattet werden müssen, um nicht nur mit KI, sondern auch mit allen anderen technologischen Entwicklungen Schritt halten zu können.[48] **Die Bewertung der DSGVO durch den EDSA hat ergeben[49], dass die meisten Datenschutzbehörden ihre „personellen, finanziellen und technischen Ressourcen" nicht für ausreichend hielten.** Zusammenarbeit und gemeinsame Untersuchungen aller einschlägigen Aufsichtsgremien, einschließlich der Datenschutzaufsichtsbehörden, sollten gefördert werden.

52. Im Weißbuch heißt es (S. 16): „Der Mangel an Transparenz (Opazität der KI) macht es schwer, etwaige Verstöße gegen Rechtsvorschriften aufzudecken und nachzuweisen; dies betrifft auch Bestimmungen zum Schutz der Grundrechte, zur Lösung von Haftungsfragen und über die Voraussetzungen für die Geltendmachung von Schadenersatz." Der EDSB ist der Auffassung, dass Transparenz bei KI-Anwendungen über die Verständlichkeit hinausgeht und die Bereitstellung klarer Informationen für die Nutzer über den Einsatz von KI-Systemen umfasst.

4.4. Rechtliche Anforderungen

53. Der EDSB begrüßt die in Abschnitt 5.D enthaltene Liste der rechtlichen Anforderungen, die sich zumeist mit den bestehenden Datenschutzvorschriften und der oben genannten **Erklärung zur Ethik und zum Datenschutz im Bereich KI** überschneiden. Er ist jedoch der Ansicht, dass Anforderungen wie „Fehlen einer unfairen Diskriminierung" oder „Robustheit und Genauigkeit" so grundlegend sind, dass sie für alle KI-Anwendungen gelten sollten, nicht nur für KI-Anwendungen mit „hohem Risiko".

54. Nach Ansicht des EDSB fallen die meisten der in Abschnitt 5.D beschriebenen Anforderungen, wie „Robustheit und Genauigkeit" oder „klare und deutliche Hinweise für natürliche Personen, wenn sie mit einem KI-System interagieren, und nicht mit einem Menschen" unter die bereits bestehenden Datenschutzvorschriften. Der EDSB begrüßt das Konzept der Kontrolle durch den Menschen, das im Einklang mit der individuellen Ermächtigung steht, die in der oben genannten **Erklärung der ICDPPC zur Ethik und zum Datenschutz im Bereich KI** vorgesehen ist, und über die Anforderungen von Artikel 22 DSGVO (automatisierte individuelle Entscheidungsfindung, einschließlich Profiling) hinausgeht [*Artikel 24 EU-DSVO*].

[46] So behauptete beispielsweise ein prominenter Softwareentwickler im November 2019, Apple Credit Card verhalte sich „sexistisch" gegenüber Frauen, die einen Kredit beantragen. Die Komplexität des KI-Systems ermöglichte es dem Kreditinstitut nicht, seine Fairness nachzuweisen. Das New York State Department of Financial Services untersucht derzeit den Fall.
https://www.nytimes.com/2019/11/10/business/Apple-credit-card-investigation.html

[47] „... Strafvollzugsbehörden können in eine Situation kommen, in der sie [...] nicht über die geeigneten technischen Kapazitäten zur Inspektion dieser Systeme verfügen."

[48] In einem im April 2020 veröffentlichten Bericht wurde eine Bewertung des Fachpersonals und des Budgets von Datenschutzbehörden in der EU seit dem Inkrafttreten der DSGVO vorgenommen und wurde Kritik an der Entwicklung ihrer technischen Kapazitäten für die Durchsetzung formuliert.

[49] Beitrag des EDSA zur Bewertung der DSGVO nach Artikel 97 (S. 30) https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en

55. Der EDSB stimmt der Bedeutung der Verpflichtung zur Bereitstellung von Informationen zu. Dennoch dürfte die angemessene Granularität der Informationen in unterschiedlichen Zusammenhängen unterschiedlich sein. Daher empfiehlt der EDSB die **Entwicklung von Informationsstandards** zur Harmonisierung der Informationen, die Einzelpersonen für verschiedene Arten von KI-Anwendungen zur Verfügung gestellt werden.

4.5. Kontrollen und Governance

56. In Abschnitt 5.F des Weißbuchs wird eine objektive vorab vorzunehmende Konformitätsbewertung für KI-Systeme mit hohem Risiko vorgeschlagen. Die Europäische Kommission definiert[50] Konformitätsbewertungen als Risikoanalyse, mit der sichergestellt wird, dass Produkte bestimmten Vorschriften entsprechen, bevor sie in Verkehr gebracht werden, und die während der Entwurfs- und Produktionsphase durchgeführt wird.

57. Einerseits würde bei der vorab vorzunehmenden Konformitätsbewertung überprüft, ob die in Abschnitt 5.D dargestellten rechtlichen Anforderungen erfüllt sind. Andererseits würde eine DSFA (die für KI-Anwendungen mit hohem Risiko nach der DSGVO obligatorisch wäre) dem Verantwortlichen bei der Überprüfung der Einhaltung der DSGVO helfen. Der EDSB sieht einen potenziellen Konflikt zwischen diesen beiden Kontrollen, da sich ihre Anforderungen überschneiden. Abweichende Schlussfolgerungen bei den einzelnen Überprüfungen einer KI-Anwendung würden zu Verwirrung und Rechtsunsicherheit führen und sollten daher vermieden werden. Der EDSB empfiehlt der Kommission daher, dafür zu sorgen, dass der mögliche künftige Rechtsrahmen nicht zu Überschneidungen zwischen den Aufsichtsbehörden führt, und einen Mechanismus für die Zusammenarbeit zwischen diesen Behörden vorzusehen.

58. In dem Weißbuch wird die Einrichtung ähnlicher Konformitätsmechanismen gefordert, „wenn auf solche bestehenden Mechanismen nicht zurückgegriffen werden kann“, doch wird nicht klargestellt, welche zuständigen Behörden an einem solchen Konformitätsmechanismus beteiligt wären. Sollte die Europäische Kommission der Aufforderung zur Errichtung einer Europäischen Agentur für KI[51] folgen, ist unklar, wie Kompetenzüberschneidungen vermieden werden können.

59. Abschnitt 5.G schlägt ein freiwilliges Kennzeichnungssystem für KI-Systeme vor, die nicht als hochriskant eingestuft werden. Dieses Gütesiegel würde für diejenigen verwendet, die sich verpflichten, die rechtlichen Anforderungen gemäß Abschnitt 5.D oder eine Reihe ähnlicher Anforderungen zu erfüllen, die speziell für die Zwecke eines solchen Kennzeichnungssystems festgelegt wurden. Für KI gibt es jedoch keine Standards, die es Entwicklern von KI-Anwendungen ermöglichen, ihre Konformität kontinuierlich zu überprüfen. Ohne solche Standards hätte das freiwillige Kennzeichnungssystem bestenfalls begrenzten Wert.

60. Der EDSB begrüßt die Erwähnung der nachträglichen Durchsetzung und der Überwachung der Einhaltung der Vorschriften durch die zuständigen Behörden. Diese Kontrollen sollten sich jedoch nicht auf die Prüfung der Unterlagen und das Testen der Anwendungen beschränken. Weitere Aspekte wie die Prüfung der Transparenz (einschließlich der Fähigkeit, zu erklären,

[50] https://europa.eu/youreurope/business/product-requirements/compliance/conformity-assessment/index_de.htm
[51] Europäisches Parlament, Rechtsausschuss, Entwurf eines Berichts mit Empfehlungen an die Kommission zu einem Rahmen für ethische Aspekte von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologien. https://www.europarl.europa.eu/doceo/document/JURI-PR-650508_DE.pdf

wie Entscheidungen getroffen werden) und die Tests, die mit den Trainingsdaten durchgeführt werden, um deren Angemessenheit zu gewährleisten, könnten ebenfalls erforderlich sein.

61. Der EDSB unterstützt uneingeschränkt die im Weißbuch für eine europäische Governance-Struktur für KI festgelegten Ziele (*„Vermeidung einer Aufsplitterung der Zuständigkeiten, Ausbau der Kapazitäten in den Mitgliedstaaten und Gewährleistung, dass Europa sich schrittweise mit der für die Prüfung und Zertifizierung von KI-gestützten Produkten und Dienstleistungen erforderlichen Kapazität ausstatten kann“*). Wie es etwas später in dem Dokument heißt, wird es von entscheidender Bedeutung sein, dass es bei einer solchen Struktur keine Überschneidungen mit bestehenden Funktionen gibt, und dass die bestehenden Behörden auf EU-Ebene, wie etwa der Europäische Datenschutzausschuss, darin eingebunden werden.

5. WEITERE SPEZIFISCHE PROBLEME

5.1. Biometrische Fernidentifikation

62. Das Weißbuch sieht durchaus die Risiken für die Grundrechte, die von der biometrischen Fernidentifikation (Remote Biometric Identification – RBI) ausgehen, eine Bemerkung, der sich der EDSB anschließt. Die biometrische Fernidentifikation wirft zwei Probleme auf: die (aus der Ferne erfolgende, skalierbare und manchmal verdeckte) Identifikation natürlicher Personen und die (aus der Ferne erfolgende, skalierbare und manchmal verdeckte) Verarbeitung ihrer biometrischen Daten. Technologien im Zusammenhang mit einem dieser beiden Merkmale, unabhängig davon, ob sie auf KI beruhen oder nicht, können ähnlich problematisch sein und müssen möglicherweise denselben Beschränkungen unterliegen wie RBI.

63. Die von RBI-Systemen ausgehenden Risiken für die Rechte und Freiheiten des Einzelnen, wie z. B. die Live-Gesichtserkennung im öffentlichen Raum, müssen ordnungsgemäß ermittelt und eingedämmt werden, und in einen solchen Prozess sollten diejenigen einbezogen werden, die am stärksten von der Nutzung dieser Technologie betroffen sind. Einige der Risiken von RBI ergeben sich aus der Tatsache, dass RBI-Systeme leicht zu verstecken und unauffällig sind, oft als bloßes „Experiment“ dargestellt werden, aber leicht zu einem allgegenwärtigen und allumfassenden Überwachungskomplex werden können.

64. Sobald die Infrastruktur für RBI installiert ist, kann sie leicht für andere Zwecke genutzt werden („schleichende Ausweitung der Zweckbestimmung“). Es hat kürzlich Stimmen gegeben, die behauptet haben, RBI-Systeme oder Teile anderer technischer Infrastrukturen zur Bekämpfung der anhaltenden Pandemie könnten noch auf andere Weise eingesetzt werden, beispielsweise zur Kontrolle des Abstandhaltens in Gesellschaft oder des Tragens von Masken oder für Temperaturmessungen (wenn Kameras über integrierte Thermometer verfügen). Einige dieser neuen Anwendungen fallen möglicherweise nicht in den Anwendungsbereich der DSGVO, würden aber dennoch eine abschreckende Wirkung in demokratischen Gesellschaften haben. Solche Verwendungen von KI und solche schleichenden Ausweitungen von Funktionen sollten daher in jeder KI-Regelung angemessen behandelt werden.

65. Obwohl RBI ernsthafte Probleme im Bereich Grundrechte hervorrufen kann, möchte der EDSB hervorheben, dass Technologien aus dem RBI-Bereich, die nicht auf die Identifikation natürlicher Personen abzielen, auch ernsthafte Bedenken hinsichtlich des Schutzes der

Privatsphäre aufwerfen: So kann beispielsweise die Ermittlung von Gefühlen - mit Echtzeit-Gesichtserkennung - einen Eingriff in die Gefühle von Personen bedeuten.[52]

66. Es ist unbedingt der Frage nachzugehen. ob die Technologie in der jeweiligen Situation, in der sie eingesetzt wird, notwendig oder verhältnismäßig ist – oder ob sie überhaupt erwünscht ist.[53] Zu diesem Zweck unterstützt der EDSB den Gedanken eines **Moratoriums für den Einsatz der automatischen Erkennung menschlicher Merkmale im öffentlichen Raum in der EU**, und zwar nicht nur von Gesichtern, sondern auch des Gangs, von Fingerabdrücken, DNA, Stimme, Tastenanschlägen und anderen biometrischen oder verhaltensgebundenen Signalen, damit eine fundierte und demokratische Debatte stattfinden kann, und zwar bis zu dem Zeitpunkt, zu dem die EU und die Mitgliedstaaten über alle geeigneten Garantien verfügen, einschließlich eines umfassenden Rechtsrahmens, der die Verhältnismäßigkeit der jeweiligen Technologien und Systeme für den konkreten Anwendungsfall gewährleistet.

67. Die **Nutzung von RBI durch Behörden** in Zeiten nationaler Notsituationen, etwa in grenzüberschreitenden oder nationalen Gesundheitskrisen, **sollte stets aus Gründen eines wesentlichen öffentlichen Interesses auf der Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erforderlich, transparent und rechenschaftspflichtig sein, in einem angemessenen Verhältnis zu dem verfolgten Ziel stehen, vorbehaltlich spezifischer Garantien erfolgen, eindeutig zeitlich begrenzt und mit dem Wesensgehalt der Grundrechte und der Achtung der Menschenwürde vereinbar sein.**

5.2. Schutzbedürftige Gruppen

68. Der EDSB begrüßt die Einsicht der Kommission, dass KI-Anwendungen tendenziell besondere Risiken für gefährdete Personengruppen bedeuten können. Im Weißbuch werden diese Risiken jedoch bei der Nutzung von Gesichtserkennungstechnik in Bezug auf Grundrechtefragen vor allem in Bezug auf „das Recht auf Achtung des Privatlebens und den Schutz personenbezogener Daten“ gesehen, wo es „potenzielle Auswirkungen im Bereich der Nichtdiskriminierung und der Rechte bestimmter Gruppen wie Kinder, ältere Menschen und Menschen mit Behinderungen“ gibt.

69. Erstens schlägt der EDSB in Ermangelung einer förmlich angenommenen rechtlichen Definition schutzbedürftiger Gruppen einen **kontextspezifischen, pragmatischen Ansatz** vor. Zu den schutzbedürftigen Personengruppen sollten Kinder, ältere Menschen und Menschen mit Behinderungen, ethnische Minderheiten oder historisch ausgegrenzte Gruppen, Frauen, LGBTQIA + Communities, Arbeitnehmer und andere von Ausgrenzung bedrohte Personen zählen.

70. Darüber hinaus ist der EDSB der Auffassung, dass das Thema schutzbedürftige Gruppen **nicht nur vor dem Hintergrund biometrischer Fernidentifikationssysteme**, sondern auch in einem viel breiteren Kontext **behandelt werden sollte**. Der EDSB betont, dass KI-Systeme fair sein und die Menschenwürde sowie die Rechte und Freiheiten des Einzelnen achten sollten. Im Zusammenhang mit schutzbedürftigen Gruppen bedeutet Fairness **Nichtdiskriminierung**. Willentliche und unbeabsichtigte Diskriminierung ist ein inhärentes Merkmal menschlicher Entscheidungsfindung, und wenn nicht sorgfältig gehandelt wird,

[52] Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements https://journals.sagepub.com/stoken/default+domain/10.1177%2F1529100619832930-FREE/pdf

[53] Eine Studie der Agentur der Europäischen Union für Grundrechte aus dem Jahr 2020 hat gezeigt, dass **mehr als 80 % der Europäer gegen die Weitergabe ihrer Gesichtsdaten an die Behörden sind.**

können KI-Systeme diese natürliche menschliche Voreingenommenheit widerspiegeln. Wie im Weißbuch zu Recht festgestellt wird, könnten in KI-Systemen „die gleichen Voreingenommenheiten eine viel größere Wirkung entfalten und viele Menschen beeinträchtigen und diskriminieren“. Dies kann direkte und indirekte Auswirkungen auf viele Aspekte des Lebens haben, wie soziale, wirtschaftliche und gesundheitliche Aspekte.

71. Auf jeden Fall besteht bei einer solchen KI-Anwendung ein hohes Risiko von Sachschäden (Sachschaden an Eigentum, quantifizierbarer Verlust) und immateriellen Schäden (Verlust der Privatsphäre, Einschränkung des Rechts auf Menschenwürde). Daher sollten die besonderen Interessen schutzbedürftiger Gruppen in allen Situationen berücksichtigt werden, die mit der oben genannten Liste vergleichbar sind. Der EDSB fordert die Kommission auf, eine nicht erschöpfende Liste von KI-Anwendungen aus verschiedenen Sektoren und für verschiedene Zwecke vorzulegen, die das Recht auf Gleichbehandlung und Nichtdiskriminierung gemäß Artikel 20 und 21 der Charta der Grundrechte der Europäischen Union gefährden könnten.

72. Der EDSB schlägt vor, dass schutzbedürftige Gruppen sowohl bei der Entwicklung als auch der Nutzung von KI berücksichtigt werden sollten, um solche nachteiligen Auswirkungen zu vermeiden. Selbst in den frühen Phasen des Trainings von KI-Systemen sollte besonders auf gefährdete Gruppen geachtet werden, da Ungenauigkeiten der KI zumeist auf eine falsche Kennzeichnung von Trainingsdaten oder nicht repräsentativen Datensätzen zurückzuführen sind. Wie es im Weißbuch heißt, könnte **die Auflage** ergehen, „angemessene Maßnahmen zu ergreifen, um sicherzustellen, dass eine solche spätere Nutzung von KI-Systemen nicht zu Ergebnissen führt, die eine verbotene Diskriminierung darstellen. Diese Auflagen könnten insbesondere die Verpflichtung umfassen, Datensätze zu verwenden, die ausreichend repräsentativ sind,. Damit soll vor allem sichergestellt werden, dass alle relevanten Aspekte wie Geschlecht, ethnische Zugehörigkeit und andere mögliche Gründe für verbotene Diskriminierung in diesen Datensätzen angemessen berücksichtigt werden.“ Solche Maßnahmen könnten beispielsweise eine Anforderung an die Eingangsebene zur Bewertung der Datenqualität, die Möglichkeit einer Kontrolle durch den Menschen, einen Rechtsbehelf oder ein „Recht auf Erläuterung“ umfassen, wenn der Einsatz von KI negative Auswirkungen auf den Einzelnen nach sich zieht, ähnlich den Bestimmungen von Artikel 22 Absatz 4 DSGVO über automatisierte Entscheidungsfindung einschließlich Profiling.

5.3. Datenzugang

73. Im Weißbuch wird „Edge Computing“ (dezentrale Rechenkapazität) als wichtiger Trend bei der Entwicklung und Weiterentwicklung von KI genannt. Diese Auffassung stimmt mit der in der Datenstrategie der Europäischen Kommission zum Ausdruck gebrachten überein. Allerdings wird weder im Weißbuch noch in der Datenstrategie erläutert, wie eine bessere physische Datenlokalisierung zu einer besseren Datenverfügbarkeit oder Vertrauenswürdigkeit von KI führen würde.

74. Während der Standort der Daten rechtliche Folgen haben kann (z. B. anwendbares Recht oder geltende Vorschriften für die internationale Übermittlung personenbezogener Daten), hängt die Verfügbarkeit der Daten nicht von ihrem physischen Standort ab, sondern von den technischen Kontrollen für den Zugang zu ihnen (z. B. über Anwendungsprogrammschnittstellen (API) und Datenaustauschformate). Daten in der Nähe von Nutzern (z. B. in einer intelligenten Uhr gespeicherte Daten) könnten für sie unzugänglich sein, es sei denn, es gibt eine API oder andere technische Mittel, mit denen auf diese Daten zugegriffen werden kann. Andererseits könnten in einer privaten Cloud gespeicherte Daten,

die Tausende Kilometer entfernt sind, verfügbar sein, wenn die Cloud-Speicherung für ihre Nutzer leicht zugänglich ist.

75. Der EDSB ist der Auffassung, dass die Kommission die Entwicklung und Annahme standardisierter Anwendungsprogrammschnittstellen[54] (API) fördern sollte. Die Annahme solcher API würde den Zugriff auf die Daten für befugte Nutzer unabhängig vom Standort dieser Daten erleichtern und wäre ein Motor für die Datenübertragbarkeit.

76. Der EDSB betont, dass der EU-Rechtsrahmen für Datensätze gelten sollte, die außerhalb der EU veröffentlicht, aber in der EU verwendet werden. KI-Anwendungen, die vom europäischen öffentlichen Sektor oder von Unternehmen entwickelt oder genutzt werden, können sich nicht auf Datensätze stützen, die nicht im Einklang mit den Datenschutzvorschriften der EU stehen oder gegen die Werte und Grundrechte der EU verstoßen.

6. SCHLUSSFOLGERUNGEN

77. Der EDSB stimmt voll und ganz mit der Kommission darin überein, dass ein europäisches Konzept für KI erforderlich ist, und er begrüßt in diesem Zusammenhang nachdrücklich das Bekenntnis des Weißbuchs zu den Grundrechten und europäischen Werten.

78. Der EDSB ist jedoch der Auffassung, dass die im Weißbuch enthaltenen Vorschläge in einigen relevanten Fragen weiter angepasst und präzisiert werden müssen. Zu den Themen, bei denen in künftigen Legislativvorschlägen mehr Klarheit erforderlich wäre, gehören der Zusammenhang zwischen den von KI ausgehenden Risiken und den entsprechenden Gesetzeslücken, der risikobasierte Ansatz für KI-Anwendungen und die Definition der KI selbst, die eine klare Festlegung des Geltungsbereichs der vorgeschlagenen Rechtsvorschriften ermöglichen sollte.

79. Der EDSB empfiehlt ferner, dass jeder neue Rechtsrahmen für KI

- **sowohl** für die EU-Mitgliedstaaten **als auch** für die Organe, Einrichtungen und sonstigen Stellen der EU gilt;

- so konzipiert ist, dass er nicht nur den Einzelnen, sondern auch Gemeinschaften und die Gesellschaft insgesamt **vor negativen Auswirkungen schützt**;

- ein **robusteres und nuancierteres Risikoklassifizierungssystem** vorschlägt, mit dem sichergestellt wird, dass jeder erhebliche potenzielle Schaden, der durch KI-Anwendungen entsteht, durch geeignete Risikominderungsmaßnahmen ausgeglichen wird;

- eine Folgenabschätzung enthält, in der **klar festgelegt ist, welche Regelungslücken** mit dem Rahmen geschlossen werden sollen;

- **Überschneidungen** zwischen verschiedenen Aufsichtsbehörden **vermeidet** und die Einführung eines Mechanismus für die Zusammenarbeit vorsieht.

[54] Kreditinstitute entwickeln API, um einen „objektiven, nichtdiskriminierenden und verhältnismäßigen“ Zugang zu Finanzdaten gemäß der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt zu gewährleisten.

80. In Bezug auf die biometrische Fernidentifikation unterstützt der EDSB den Gedanken **eines Moratoriums für die automatische Erkennung menschlicher Merkmale im öffentlichen Raum in der EU**, und zwar nicht nur des Gesichts, sondern auch des Gangs, von Fingerabdrücken, DNA, Stimme, Tastenanschlägen und anderen biometrischen oder verhaltensgebundenen Signalen, damit eine fundierte und demokratische Debatte stattfinden kann, und zwar bis zu dem Zeitpunkt, zu dem die EU und die Mitgliedstaaten über alle geeigneten Garantien verfügen, einschließlich eines umfassenden Rechtsrahmens, der die Verhältnismäßigkeit der jeweiligen Technologien und Systeme für den konkreten Fall gewährleistet.

81. Sollte es einen neuen Rechtsrahmen geben, wie es im Weißbuch und im Arbeitsprogramm der Kommission heißt, wird der EDSB die Kommission gemäß Artikel 42 EU-DSVO weiter beraten.

Brüssel, den 29. Juni 2020

Wojciech Rafał WIEWIÓROWSKI