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

Zusammenfassung

Am 21. April 2021 legte die Europäische Kommission ihren Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (im Folgenden „Vorschlag“) vor. Der EDSA und der EDSB begrüßen, dass der Gesetzgeber bedenklichen Aspekten der Verwendung künstlicher Intelligenz (KI) in der Europäischen Union (EU) entgegenwirkt, und heben hervor, dass der Vorschlag besonders wichtige **Auswirkungen auf den Datenschutz** hat.

Der EDSA und der EDSB stellen fest, dass die **Rechtsgrundlage** für den Vorschlag in erster Linie Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ist. Darüber hinaus beruht der Vorschlag auch auf Artikel 16 AEUV, insofern er spezifische Regeln über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten enthält, vor allem Einschränkungen der Verwendung von KI-Systemen zur biometrischen Fernidentifizierung in Echtzeit in öffentlich zugänglichen Räumen für die Zwecke der Strafverfolgung. Der EDSA und der EDSB erinnern daran, dass Artikel 16 AEUV nach der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) eine geeignete Rechtsgrundlage darstellt, wenn der Schutz personenbezogener Daten eines der wesentlichen Ziele oder Komponenten der vom Unionsgesetzgeber erlassenen Regeln ist. Mit der Anwendung von Artikel 16 AEUV geht, was die Anforderungen an die Verarbeitung personenbezogener Daten betrifft, das **Erfordernis** einher, **die Überwachung der Einhaltung der Regeln durch eine unabhängige Stelle sicherzustellen**, was auch nach Artikel 8 der Charta der Grundrechte der Europäischen Union erforderlich ist.

Was den **Anwendungsbereich des Vorschlags** angeht, wird der Umstand, dass sich dieser auf die Bereitstellung und Verwendung von KI-Systemen durch Organe, Einrichtungen oder sonstige Stellen der EU erstreckt, von EDSA und EDSB nachdrücklich begrüßt. Der im Vorschlag vorgesehene **Ausschluss der internationalen Zusammenarbeit im Bereich der Strafverfolgung aus dem Anwendungsbereich** gibt dem EDSA und dem EDSB jedoch Anlass zu ernsthaften Bedenken, weil durch diesen Ausschluss eine erhebliche Umgehungsgefahr entsteht (dass z. B. öffentliche Stellen in der EU auf Drittländer oder internationale Organisationen, die Hochrisiko-Anwendungen betreiben, zurückgreifen).

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.

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**.

Der EDSA und der EDSB begrüßen die **Benennung des EDSB als die zuständige Behörde und Marktüberwachungsbehörde für die Aufsicht über die Organe, Einrichtungen und sonstigen Stellen der Union**. Die Rolle und die Aufgaben des EDSB sollten jedoch genauer spezifiziert werden, vor allem in Bezug auf seine Rolle als Marktüberwachungsbehörde. Des Weiteren sollte in der künftigen KI-Verordnung die **Unabhängigkeit der Aufsichtsbehörden** in der Wahrnehmung ihrer Aufsichts- und Durchsetzungsaufgaben klargestellt werden.

Die Benennung der Datenschutzbehörden (DSB) als nationale Aufsichtsbehörden würde einen einheitlicheren Regulierungsansatz ermöglichen und dazu beitragen, dass die Mitgliedstaaten die Datenverarbeitungsvorschriften einheitlich auslegen und Widersprüche in deren Durchsetzung vermeiden. Der EDSA und der EDSB sind deshalb der Auffassung, dass **die Datenschutzbehörden als zuständige nationale Aufsichtsbehörden im Sinne von Artikel 59 des Vorschlags benannt werden sollten**.

Im Vorschlag wird der Kommission eine vorherrschende Rolle im „Europäischen Ausschuss für künstliche Intelligenz“ (EAKI) zugewiesen. Diese Rolle steht mit dem Erfordernis eines von politischem Einfluss unabhängigen europäischen KI-Gremiums im Konflikt. Zur Gewährleistung seiner Unabhängigkeit sollte in der künftigen KI-Verordnung **mehr Autonomie für den EAKI** vorgesehen und auch sichergestellt werden, dass dieser auf eigene Initiative handeln kann.

In Anbetracht der Verbreitung von KI-Systemen im Binnenmarkt und der Wahrscheinlichkeit grenzüberschreitender Fälle sind eine einheitliche Durchsetzung sowie eine ordnungsgemäße Zuweisung der Zuständigkeiten unter den nationalen Aufsichtsbehörden unbedingt erforderlich. Der EDSA und der EDSB schlagen vor, **einen Mechanismus** vorzusehen, **der für jedes KI-System eine einzige Anlaufstelle für die von der gesetzlichen Regelung betroffenen natürlichen und juristischen Personen garantiert**.

Was die **Reallabore** angeht, empfehlen der EDSA und der EDSB, **deren Gegenstand und Ziele zu präzisieren**. Im Vorschlag sollte auch klar festgelegt werden, dass die Rechtsgrundlage derartiger Reallabore den Anforderungen genügen muss, die sich aus dem bestehenden Datenschutzregelwerk ergeben.

Dem im Vorschlag umrissenen **Zertifizierungssystem fehlt die klare Bezugnahme auf das Datenschutzrecht der Union** wie auch das für jeden „Bereich“ von Hochrisiko-KI-System geltende sonstige Recht der Union und der Mitgliedstaaten; außerdem berücksichtigt es nicht die **Grundsätze der Datenminimierung und des Datenschutzes durch Technikgestaltung** als einen der **für die Erlangung der CE-Kennzeichnung** zu berücksichtigenden Aspekte. Der EDSA und der EDSB empfehlen deshalb, den Vorschlag dahingehend zu ändern, dass das Verhältnis zwischen den aufgrund der genannten Verordnung erteilten Zertifikaten sowie den Datenschutzzertifikaten, -siegeln und -prüfzeichen klargestellt wird. Letztlich sollten die Datenschutzbehörden auch bei der Erstellung und Festlegung harmonisierter Normen und gemeinsamer Spezifikationen mitwirken.

Was die **Verhaltenskodizes** angeht, halten der EDSA und der EDSB es **für erforderlich, klarzustellen**, ob der Schutz personenbezogener Daten als eine der „zusätzlichen Anforderungen“ anzusehen ist, die in solchen Verhaltenskodizes festgelegt werden können, sowie sicherzustellen, dass die „technischen Spezifikationen und Lösungen“ nicht mit den Vorschriften und Grundsätzen des bestehenden Datenschutzregelwerks der Union in Konflikt stehen.

INHALT

Der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte –

gestützt auf Artikel 42 Absatz 2 der 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[1],

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, insbesondere auf Anhang XI und das Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung,[2]

gestützt auf das Ersuchen vom 22. April 2021 um eine gemeinsame Stellungnahme des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten bezüglich des Vorschlags für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz),

HABEN FOLGENDE GEMEINSAME STELLUNGNAHME ANGENOMMEN:

1 EINLEITUNG

1. In der Technologieentwicklung wie auch in der Art und Weise der Interaktion zwischen Mensch und Technologie stellen Systeme künstlicher Intelligenz (KI-Systeme) eine sehr wichtige Entwicklungsstufe dar. KI umfasst eine Reihe von Schlüsseltechnologien, die unseren Lebensalltag, sei es in gesellschaftlicher oder in wirtschaftlicher Hinsicht, grundlegend verändern werden. In den kommenden Jahren ist mit maßgeblichen Entscheidungen auf dem Gebiet der KI zu rechnen, da KI uns in vielen Bereichen – u. a. Gesundheit, Mobilität, öffentliche Verwaltung und Bildung – hilft, einige der größten Herausforderungen, denen wir uns heute gegenübersehen, zu bewältigen.

2. Die in Aussicht gestellten Fortschritte sind jedoch nicht risikofrei. Diese Risiken sind in der Tat von hoher Relevanz, da es bislang nur wenig Erfahrung mit den Auswirkungen von KI-Systemen auf den Einzelnen und die Gesellschaft gibt. Auf automatisierte Weise Inhalte zu erzeugen, Vorhersagen zu machen oder Entscheidungen zu treffen, so wie KI-Systeme es mittels maschinellen Lernens bzw. logischer und probabilistischer Inferenzregeln tun, unterscheidet sich von der Art und Weise, wie Menschen derartige Tätigkeiten ausführen, indem sie kreative oder theoretische Überlegungen anstellen und dabei die volle Verantwortung für die Folgen tragen.

[1] ABl. L 295 vom 21.11.2018, S. 39-98.
[2] Soweit hierin auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.

3. In vielen Gebieten wird KI deutlich mehr Vorhersagen ermöglichen, angefangen mit messbaren Korrelationen zwischen Daten, die zwar nicht für den Menschen, jedoch für Maschinen erkennbar sind. Das wird unser Leben erleichtern und sehr viele Probleme lösen, gleichzeitig werden wir jedoch weniger gut in der Lage sein, zu begründen, welche Ursachen zu einem bestimmten Ergebnis geführt haben; unseren Vorstellungen von Transparenz, menschlicher Kontrolle, Rechenschaftspflicht und Ergebnishaftung läuft das in hohem Maße zuwider.

4. (Personenbezogene wie auch nicht-personenbezogene) Daten sind in der KI vielfach die Hauptvoraussetzung für autonome Entscheidungen, die unweigerlich das Leben natürlicher Personen auf verschiedenen Ebenen berühren. Dies ist der Grund dafür, dass der EDSA und der EDSB bereits jetzt nachdrücklich darauf hinweisen, dass der Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) („Vorschlag“)[3] **wichtige datenschutzrechtliche Implikationen** hat.

5. Wird Maschinen die Aufgabe zugewiesen, auf Grundlage von Daten Entscheidungen zu treffen, werden sich nicht nur Risiken für die Rechte und Freiheiten natürlicher Personen sowie Auswirkungen auf deren Privatleben ergeben, sondern möglicherweise auch Gruppen oder sogar die Gesellschaft insgesamt Schaden nehmen. Der EDSA und der EDSB betonen, dass die Rechte auf Achtung des Privatlebens und den Schutz personenbezogener Daten, die mit der dem Konzept der KI zugrunde liegenden Annahme der Entscheidungsautonomie der Maschinen in Konflikt stehen, eine der Säulen der Werte der Union sind, so wie diese in der Allgemeinen Erklärung der Menschenrechte (Artikel 12), der Europäischen Menschenrechtskonvention (Artikel 8) und der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) (Artikel 7 und 8) anerkannt sind. Das Ziel, die durch KI-Anwendungen gebotenen Wachstumsaussichten mit der zentralen und vorrangigen Stellung des Menschen gegenüber den Maschinen in Einklang zu bringen, ist sehr hoch gesteckt, aber notwendig.

6. Der EDSA und der EDSB begrüßen die Einbeziehung aller Interessenträger entlang der Wertschöpfungskette im Bereich der künstlichen Intelligenz wie auch die Einführung besonderer Anforderungen für Lösungsanbieter, da diese hinsichtlich der Produkte, für die ihre Systeme verwendet werden, eine wichtige Rolle spielen. Allerdings ist es erforderlich, die Verantwortlichkeiten der verschiedenen Beteiligten – Nutzer, Anbieter, Importeur bzw. Händler eines KI-Systems – klar abzugrenzen und zuzuweisen. Insbesondere bei der Verarbeitung personenbezogener Daten ist darauf zu achten, dass diese mit den Funktionen und Zuständigkeiten in Einklang stehen muss, die im Datenschutzregelwerk für die Verantwortlichen und Auftragsverarbeiter vorgesehen sind, da die beiden Normen nicht deckungsgleich sind.

7. Im Vorschlag wird dem Begriff der menschlichen Aufsicht (Artikel 14) ein hoher Stellenwert eingeräumt, was der EDSA und der EDSB begrüßen. Wie bereits erwähnt, können gewisse KI-Systeme erhebliche Auswirkungen auf Einzelpersonen oder Gruppen von Einzelpersonen haben; deshalb sollte, soweit die betreffenden Systeme auf der Verarbeitung

[3] COM(2021) 206 final.

personenbezogener Daten beruhen oder zur Erledigung ihrer Aufgabe personenbezogene Daten verarbeiten, für die zentrale Rolle, die dem Menschen zukommt, auf hochqualifizierte menschliche Aufsicht und rechtmäßige Verarbeitung gesetzt werden, um zu gewährleisten, dass das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, geachtet wird.

8. Da viele KI-Anwendungen sehr datenintensiv sind, sollte der Vorschlag darauf hinwirken, dass auf jeder Ebene Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen zum Einsatz kommt, um so die wirksame Umsetzung der (in Artikel 25 DSGVO und Artikel 27 EU-DSVO vorgesehenen) Datenschutzgrundsätze mittels modernster Technologie zu fördern.

9. Abschließend betonen der EDSA und der EDSB, dass mit dieser gemeinsamen Stellungnahme lediglich eine vorläufige Analyse des Vorschlags vorgelegt wird, die weiteren Bewertungen und Stellungnahmen zu den Auswirkungen des Vorschlags und seiner Vereinbarkeit mit dem Datenschutzrecht der Union nicht vorgreift.

2 ANALYSE DER HAUPTGRUNDSÄTZE DES VORSCHLAGS

2.1 Anwendungsbereich des Vorschlags und Verhältnis zum bestehenden Rechtsrahmen

10. Laut der Begründung zum Gesetzentwurf ist die **Rechtsgrundlage** für den Vorschlag zunächst Artikel 114 AEUV, der die Annahme von Maßnahmen für die Errichtung und das Funktionieren des Binnenmarkts vorsieht.[4] Darüber hinaus beruht der Vorschlag *hinsichtlich der darin enthaltenen spezifischen Regeln über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten*, d. h. vor allem der Einschränkungen der Verwendung von KI-Systemen zur biometrischen Fernidentifizierung in Echtzeit in öffentlich zugänglichen Räumen für die Zwecke der Strafverfolgung, auch auf Artikel 16 AEUV[5].

11. Der EDSA und der EDSB erinnern daran, dass Artikel 16 AEUV nach der Rechtsprechung des EuGH eine geeignete Rechtsgrundlage darstellt, wenn der Schutz personenbezogener Daten eine(s) der wesentlichen Ziele oder Komponenten der vom Unionsgesetzgeber erlassenen Regeln ist[6]. Was die Anforderungen an die Verarbeitung personenbezogener Daten betrifft, ist es bei Anwendung von Artikel 16 AEUV (wie auch nach Artikel 8 der Charta) erforderlich, die Überwachung der Einhaltung der Regeln durch eine unabhängige Stelle sicherzustellen.

[4] Begründung, S. 5.
[5] Begründung, S. 6. Siehe auch Erwägungsgrund 2 des Vorschlags.
[6] Gutachten vom 26. Juli 2017, PNR Canada, Gutachten 1/15 des Gerichtshofs (Große Kammer), ECLI:EU:C:2017:592, Nr. 96.

12. Der EDSB und der EDSA erinnern daran, dass es bereits ein aufgrund Artikel 16 AEUV angenommenes umfassendes Datenschutzregelwerk gibt, das aus der Datenschutz-Grundverordnung (DSGVO)[7], der Datenschutzverordnung für die Organe, Einrichtungen und sonstigen Stellen der Union (EU-DSVO)[8] und der Strafverfolgungsrichtlinie (LED)[9] besteht. Im Vorschlag heißt es, dass es lediglich die im Vorschlag vorgesehenen zusätzlichen Einschränkungen bezüglich der Verarbeitung biometrischer Daten sind, die als auf Artikel 16 AEUV – und damit auf dieselbe Rechtsgrundlage wie die DSGVO, die EU-DSVO und die LED – gestützt angesehen werden können. Daraus ergeben sich wichtige Implikationen für das Verhältnis des Vorschlags zur DSGVO, EU-DSVO und LED im Allgemeinen, die im Folgenden dargelegt werden.

13. Was den **Anwendungsbereich des Vorschlags** angeht, wird der Umstand, dass sich der Vorschlag auf die Bereitstellung und Verwendung von KI-Systemen durch Organe, Einrichtungen oder sonstige Stellen der EU erstreckt, vom EDSA und EDSB nachdrücklich begrüßt. Da die Verwendung von KI-Systemen durch diese Stellen, ähnlich wie bei der Verwendung innerhalb von Mitgliedstaaten der EU, auch erhebliche Auswirkungen auf die Grundrechte natürlicher Personen haben kann, ist es unbedingt erforderlich, dass der neue Rechtsrahmen für KI sowohl auf die Mitgliedstaaten der EU als auch auf die Organe, Einrichtungen und sonstigen Stellen der EU Anwendung findet, um einen unionsweit einheitlichen Ansatz zu gewährleisten. Da Organe, Einrichtungen und sonstige Stellen der EU sowohl als Anbieter als auch als Nutzer von KI-Systemen handeln können, ist es nach Ansicht des EDSB und des EDSA völlig angemessen, diese Stellen aufgrund Artikel 114 AEUV in den Anwendungsbereich des Vorschlags einzubeziehen.

14. Allerdings haben der EDSA und der EDSB ernsthafte Bedenken hinsichtlich des Ausschlusses der internationalen Zusammenarbeit im Bereich der Strafverfolgung vom Anwendungsbereich gemäß Artikel 2 Absatz 4 des Vorschlags . Durch diesen Ausschluss entsteht eine erhebliche Umgehungsgefahr (dass nämlich öffentliche Stellen in der EU auf Drittländer oder internationale Organisationen, die Hochrisiko-Anwendungen betreiben, zurückgreifen).

15. Die Entwicklung und Verwendung von KI-Systemen wird vielfach mit der Verarbeitung personenbezogener Daten verbunden sein. Es ist daher von höchster Wichtigkeit, das Verhältnis dieses Vorschlags zu den bestehenden Datenschutzvorschriften der Union klarzustellen. Der Vorschlag ergänzt die DSGVO, die EU-DSVO und die LED und lässt sie ansonsten unberührt. Obwohl in den Erwägungsgründen des Vorschlags klargestellt ist, dass

[7] 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) (ABl. L 119 vom 4.5.2016, S. 1-88).

[8] 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 (ABl. L 295 vom 21.11.2018, S. 39 bis 98).

[9] 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 (ABl. L 119 vom 4.5.2016, S. 89-131).

die Verwendung von KI-Systemen auch dem Datenschutzrecht genügen muss, **empfehlen der EDSA und der EDSB dringend , in Artikel 1 des Vorschlags klarzustellen, dass die Unionsvorschriften zum Schutz personenbezogener Daten**, insbesondere die DSGVO, die EU-DSVO, die ePrivacy-Richtlinie[10] und die LED, auf jede in den Anwendungsbereich des Vorschlags fallende Verarbeitung personenbezogener Daten anwendbar sind. In einem entsprechenden Erwägungsgrund sollte gleichermaßen klargestellt werden, dass der Vorschlag die Anwendung der bestehenden Unionsrechtsvorschriften über die Verarbeitung personenbezogener Daten unberührt lassen soll, wozu auch die Aufgaben und Befugnisse der für die Überwachung der Einhaltung dieser Instrumente zuständigen unabhängigen Aufsichtsbehörden zählen.

2.2 Risikobasierter Ansatz

16. Der EDSA und der EDSB **begrüßen den risikobasierten Ansatz**, der dem Vorschlag zugrunde liegt. Der Vorschlag würde auf alle KI-Systeme angewendet, auch auf diejenigen, bei denen zwar keine Verarbeitung personenbezogener Daten erfolgt, die aber dennoch Auswirkungen auf Interessen oder Grundrechte und Grundfreiheiten haben können.

17. Der EDSA und der EDSB merken an, dass in einigen Bestimmungen des Vorschlags die Risiken für Gruppen von natürlichen Personen oder für die Gesellschaft als Ganzes nicht berücksichtigt wurden (z. B. kollektive Auswirkungen von besonderer Bedeutung, etwa im Falle gruppenbezogener Diskriminierung oder politischer Meinungsäußerung im öffentlichen Raum) . Der EDSA und der EDSB empfehlen, dass von KI-Systemen ausgehende gesellschaftliche / gruppenbezogene Risiken ebenfalls berücksichtigt und gemindert werden sollten.

18. Der EDSA und der EDSB sind der Ansicht, dass der risikobasierte Ansatz des Vorschlags präzisiert werden und der Begriff „Risiko für die Grundrechte“ **mit der DSGVO in Einklang gebracht** werden sollte, soweit Aspekte zum Tragen kommen, die den Schutz personenbezogener Daten betreffen. . Egal, ob Endnutzer, von der Verarbeitung personenbezogener Daten betroffene Personen oder sonstige vom KI-System betroffene Personen – das vom KI-System betroffene Individuum kommt im Wortlaut des Vorschlags nicht vor; insoweit hat der Vorschlag wohl einen blinden Fleck. Die den Akteuren auferlegten Verpflichtungen gegenüber den betroffenen Personen sollten sich noch konkreter aus dem Schutz der Einzelperson und ihrer Rechte ergeben. Der EDSA und der EDSB fordern die Gesetzgeber auf, im Vorschlag ausdrücklich anzugeben, welche **Rechte und Rechtsbehelfe den Einzelnen zur Verfügung stehen,** die von den KI-Systemen betroffen sind.

19. Der EDSA und der EDSB nehmen zur Kenntnis, dass dafür optiert wurde, eine erschöpfende Liste aller **Hochrisiko-KI-Systeme** aufzustellen. Dadurch könnte ein Schwarz-Weiß-Effekt entstehen, wodurch hochriskante Situationen nur unzureichend erfasst werden, was den risikobasierten Ansatz, der dem Vorschlag zugrunde liegt, untergraben wird. Außerdem fehlen

[10] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), in der durch Richtlinie 2006/24/EG und Richtlinie 2009/136/EG geänderten Fassung.

bei dieser Liste von Hochrisiko-KI-Systemen, die im Einzelnen in den Anhängen II und III des Vorschlags aufgeführt sind, einige Arten von Anwendungen, die erhebliche Risiken bergen, etwa die Verwendung von KI zur Bestimmung der Versicherungsprämie oder zur Bewertung medizinischer Behandlungen oder für die Zwecke der Gesundheitsforschung. Der EDSA und der EDSB heben auch hervor, dass diese Anhänge regelmäßig zu aktualisieren sind, damit die erfassten Anwendungsbereiche angemessen bleiben.

20. Nach dem Vorschlag sind die **Anbieter** eines KI-Systems gehalten, eine Risikoabschätzung vorzunehmen; zumeist sind jedoch die (für die Datenverarbeitung) Verantwortlichen die **Nutzer** und nicht die Anbieter von KI-Systemen (so ist z. B. der Nutzer eines Gesichtserkennungssystems ein „Verantwortlicher" und deshalb nicht an die nach dem Vorschlag für Anbieter von Hochrisiko-KI geltenden Anforderungen gebunden).

21. Überdies wird es **dem Anbieter nicht immer möglich sein, eine Bewertung sämtlicher Verwendungen** des KI-Systems vorzunehmen. Die anfängliche Risikoabschätzung wird deshalb eher allgemeinerer Art sein als diejenige, die der Nutzer des KI-Systems vornimmt. Selbst wenn die vom Anbieter vorgenommene erste Risikoabschätzung nicht darauf hindeutet, dass es sich um ein Hochrisiko-KI-System im Sinne des Vorschlags handelt, sollte dies **eine spätere (differenziertere) Abschätzung** (Datenschutz-Folgenabschätzung („DSFA") gemäß Artikel 35 DSGVO, Artikel 39 EU-DSVO oder Artikel 27 LED), **die vom Nutzer des Systems durchzuführen ist** und bei der der Kontext der Nutzung und die spezifische Anwendung berücksichtigt werden, nicht ausschließen. Die Auslegung, ob eine Art der Verarbeitung nach der DSGVO, der EU-DSVO bzw. der LED wahrscheinlich zu einem hohen Risiko führt, ist unabhängig vom Vorschlag vorzunehmen. Wird allerdings ein KI-System wegen seiner Grundrechtsauswirkungen als „Hochrisiko" eingestuft,[11] **ist zu vermuten, dass es sich, soweit personenbezogene Daten verarbeitet werden, um ein „hohes Risiko" im Sinne der DSGVO, der EU-DSVO bzw. der LED handelt.**

22. **Darüber hinaus stimmen der EDSA und der EDSB mit dem Vorschlag insoweit überein, als die Einstufung eines KI-Systems als hochriskant nicht zwangsläufig bedeuten sollte, dass es per se mit geltendem Recht vereinbar ist und vom Nutzer entsprechend verwendet werden kann. Die verantwortliche Stelle wird unter Umständen weitere sich aus dem Datenschutzrecht der Union ergebende Anforderungen einhalten müssen.** Des Weiteren sollte der dem Artikel 5 des Vorschlags zugrundeliegende Gedanke, dass Hochrisiko-Systeme, anders als verbotene Systeme, grundsätzlich zulässig sein können, aus dem Vorschlag gestrichen werden, zumal auch die vorgeschlagene CE-Kennzeichnung nicht bedeutet, dass die damit verbundene Verarbeitung personenbezogener Daten rechtmäßig ist.

[11] Die Agentur der Europäischen Union für Grundrechte (FRA) hat sich bereits zu dem Erfordernis geäußert, bei der Verwendung von KI oder damit zusammenhängenden Technologien eine Abschätzung der Grundrechtsauswirkungen vorzunehmen. In ihrem 2020 erschienenen Bericht „Getting the future right – Artificial intelligence and fundamental rights" hat die FRA festgestellt, dass es „Gefahren bei der Verwendung von KI, z. B. für prädikative Polizeiarbeit, medizinische Diagnosen, Sozialdienste und zielgerichtete Werbung" gibt, und hervorgehoben, dass „private und öffentlich-rechtliche Organisationen abschätzen sollten, welche Grundrechtsgefährdungen von KI ausgehen könnten", um negative Auswirkungen auf Einzelpersonen gering zu halten.

23. Allerdings 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 empfehlen deshalb, das **Erfordernis, die Einhaltung der DSGVO und der EU-DSVO sicherzustellen, in Titel III Kapitel 2 des Vorschlags aufzunehmen**. Die Einhaltung dieser Anforderungen sollte gemäß dem Grundsatz der Rechenschaftspflicht vor der CE-Kennzeichnung (durch Dritte) überprüft werden. Im Zusammenhang mit dieser von Dritten vorgenommenen Überprüfung wird die vom Anbieter durchgeführte erste Folgenabschätzung von besonderer Relevanz sein.

24. Was die sich aus der Entwicklung von KI-System ergebenden Komplexitäten angeht, ist darauf hinzuweisen, dass die technischen Merkmale von KI-Systemen (z. B. die Art des KI-Ansatzes) zu größeren Risiken führen können. Bei jeder für ein KI-System durchgeführten Risikoabschätzung sind deshalb **die technischen Merkmale** sowie **die spezifischen Anwendungen und der Kontext**, in dem das System betrieben wird, zu berücksichtigen.

25. Vor diesem Hintergrund empfehlen der EDSA und der EDSB, im Vorschlag anzugeben, dass **der Anbieter** die erste Risikoabschätzung für das KI-System **unter Berücksichtigung der Anwendungsfälle** durchzuführen hat (die im Vorschlag zu spezifizieren sind – z. B. als Ergänzung zu Anhang III, 1a), wo die Anwendungen von biometrischen KI-Systemen nicht erwähnt sind), und dass der **Nutzer** des KI-Systems in seiner Eigenschaft als Verantwortlicher im Sinne des Datenschutzrechts der Union (soweit relevant) die DSFA wie in Artikel 35 DSGVO, Artikel 39 EU-DSVO und Artikel 27 LED vorgesehen durchzuführen hat, wobei nicht nur die technischen Merkmale und die **Anwendung**, sondern **auch der spezifische Kontext**, in dem die KI eingesetzt wird, zu berücksichtigen sind.

26. Darüber hinaus sollten einige der in Anhang III des Vorschlags verwendeten Begriffe präzisiert werden, z. B. der Begriff „grundlegende private und öffentliche Dienste und Leistungen“ oder KI-Systeme für die Kreditwürdigkeitsprüfung, die von Kleinanbietern für den Eigengebrauch in Betrieb genommen werden.

2.3 Verbotene Verwendungen von KI

27. Nach Ansicht des EDSA und des EDSB sind **in Rechte eingreifende Formen der KI** – insbesondere solche, die die Menschenwürde verletzen – als unter Artikel 5 des Vorschlags fallende verbotene KI-Systeme anzusehen und nicht einfach als „Hochrisiko-KI-System“ im Sinne von Anhang III des Vorschlags einzustufen, wie etwa die unter Nr. 6 aufgeführten. Dies gilt insbesondere für Datenabgleiche, die, bei Anwendung im großen Maßstab, auch Personen betreffen können, die keinen oder nur geringen Grund für polizeiliche Beobachtung gegeben haben, sowie für Verarbeitungsvorgänge, die dem datenschutzrechtlichen Grundsatz der Zweckbindung zuwiderlaufen. Die Verwendung von KI im Bereich Polizei und Strafverfolgung erfordert bereichsspezifische, präzise, vorhersehbare und verhältnismäßige Regeln, die die Interessen der betroffenen Personen sowie die Auswirkungen auf das Funktionieren der demokratischen Gesellschaft berücksichtigen müssen.

28. Es besteht die Gefahr, dass Artikel 5 des Vorschlags lediglich ein Lippenbekenntnis zu den „Werten“ und zum Verbot von KI-Systemen, die im Widerspruch zu diesen Werten stehen darstellt. So bewirken die in Artikel 5 genannten Voraussetzungen, bei deren Vorliegen KI-Systeme einen Verbotstatbestand erfüllen, **eine Begrenzung des Anwendungsbereichs des Verbots**, die so weit geht, dass sich das Verbot in der Praxis als bedeutungslos erweisen könnte (z. B. „einen physischen oder psychischen Schaden zufügt oder zufügen kann“ in Artikel 5 Absatz 1 Buchstaben a und b; Beschränkung auf Behörden in Artikel 5 Absatz 1 Buchstabe c; vage Formulierung sowie Ziffern i und ii in Buchstabe c; Beschränkung lediglich auf biometrische Echtzeit-Fernidentifizierungssysteme ohne klare Begriffsbestimmung usw.).

29. Insbesondere die in Artikel 5 Absatz 1 Buchstabe c des Vorschlags vorgesehene Verwendung von KI für „Social Scoring“, die zu Diskriminierung führen kann, verletzt die Grundwerte der Union. Nach dem Vorschlag sind derartige Praktiken lediglich verboten, wenn sie „über einen bestimmten Zeitraum“ oder „durch Behörden oder in deren Auftrag“ erfolgen. Privatunternehmen, etwa Anbieter von sozialen Medien und Cloud-Diensten, sind in der Lage, enorme Mengen personenbezogener Daten zu verarbeiten und Social Scoring vorzunehmen. Folglich **sollte der Vorschlag das Verbot jeder Art der Bewertung des sozialen Verhaltens (Social Scoring) vorsehen**. Es ist zu beachten, dass im Bereich der Strafverfolgung diese Art von Aktivitäten bereits durch Artikel 4 LED so erheblich eingeschränkt ist, dass dies praktisch auf ein Verbot hinausläuft.

30. Die **biometrische Fernidentifizierung** natürlicher Personen in öffentlich zugänglichen Räumen birgt ein hohes Risiko der Verletzung der Privatsphäre des Einzelnen. Von EDSA und EDSB wird deshalb **ein strengerer Ansatz für notwendig erachtet**. Die Verwendung von KI-Systemen kann ernsthafte Verhältnismäßigkeitsprobleme aufwerfen, da es dabei dazu kommen kann, dass Daten einer unverhältnismäßigen Anzahl betroffener Personen (z. B. Flug- oder Fahrgäste in Flughäfen und Bahnhöfen) unterschiedslos verarbeitet werden, um lediglich einige wenige Einzelpersonen zu identifizieren. Da Systeme für die biometrische Fernidentifizierung ihrer Art nach **verdeckt** funktionieren, werden auch Transparenzprobleme sowie Probleme in Bezug auf die unionsrechtliche Rechtsgrundlage (LED, DSGVO, EU-DSVO) für die Verarbeitung aufgeworfen. Das Problem der ordnungsgemäßen Unterrichtung von Einzelpersonen über diese Verarbeitung ist noch genauso ungelöst wie das der wirksamen und rechtzeitigen Ausübung von Einzelpersonen zustehenden Rechten. Dasselbe gilt für die **irreversiblen, gravierenden Auswirkungen** auf die (angemessene) **Erwartung der Bevölkerung, im öffentlichen Raum anonym zu bleiben**, womit wiederum direkte negative Auswirkungen auf die Ausübung der Meinungs-, Versammlungs- und Vereinigungsfreiheit sowie der Freizügigkeit einhergehen.

31. In Artikel 5 Absatz 1 Buchstabe d des Vorschlags ist eine umfangreiche **Liste von Ausnahmetatbeständen** vorgesehen, in denen die biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken gestattet ist. Der EDSA und der EDSB halten **diesen Ansatz für fehlerhaft**, und zwar in mehrfacher Hinsicht: Erstens ist unklar, was unter „erhebliche Verzögerung“ zu verstehen sein soll und inwiefern eine solche einen mildernden Faktor darstellen sollte, wenn man bedenkt, dass ein System zur Massenidentifizierung in der Lage ist, in nur wenigen Stunden die Identitäten von tausenden

Personen festzustellen. Hinzu kommt, dass die mit der Verarbeitung einhergehenden Grundrechtseingriffe nicht immer davon abhängig sind, ob die Identifizierung in Echtzeit erfolgt oder nicht. Im Zusammenhang mit einem politischen Protest dürfte die nachträgliche biometrische Fernidentifizierung erheblich davor abschrecken, Grundrechte und Grundfreiheiten, etwa die Versammlungs- und Vereinigungsfreiheit und allgemein die zu den Gründungsprinzipien der Demokratie zählenden Rechte auszuüben. Zweitens sind die mit der Verarbeitung verbundenen Grundrechtseingriffe nicht immer von deren Zweck abhängig. Bei der Verwendung dieses Systems für andere Zwecke, etwa für private Sicherheitszwecke, sind die Grundrechte der Achtung des Privat- und Familienlebens sowie der Schutz personenbezogener Daten gleichermaßen gefährdet. Selbst innerhalb der vorgesehenen Beschränkungen wird die potenzielle Anzahl der Verdächtigen oder Straftäter letztendlich so gut wie immer „hoch genug“ sein, die kontinuierliche Verwendung von KI-Systemen zur Erkennung von Verdächtigen zu rechtfertigen, ungeachtet der weiteren Voraussetzungen in Artikel 5 Absatz 2 bis 4 des Vorschlags. Bei den dem Vorschlag zugrunde liegenden Überlegungen scheint übersehen worden zu sein, dass bei der Überwachung offener Bereiche die sich aus dem Datenschutzrecht der Union ergebenden Verpflichtungen nicht nur in Bezug auf die Verdächtigen, sondern auch in Bezug auf alle diejenigen erfüllt sein müssen, die in der Praxis überwacht werden.

32. Aus allen diesen Gründen erheben der EDSA und der EDSB die **Forderung, die Verwendung von KI zur automatischen Erkennung von personenbezogenen Merkmalen – zum Beispiel Gesichtszügen, aber auch Gangart, Fingerabdrücken, DNA, Stimme, Tastenanschlagsmuster und anderen biometrischen Merkmalen oder Verhaltenssignalen – in öffentlich zugänglichen Räumen in jeglichem Zusammenhang allgemein zu verbieten**. In seiner derzeitigen Fassung folgt der Vorschlag dem Ansatz, alle KI-Systeme, die verboten sein sollten, anzugeben und aufzulisten. Aus Gründen der Einheitlichkeit sollten **KI-Systeme für die groß angelegte Fernidentifizierung in Online-Räumen** gemäß Artikel 5 des Vorschlags verboten sein. Mit Rücksicht auf die LED, die DSGVO und die EU-DSVO vermögen der EDSB und der EDSA nicht zu erkennen, wie diese Art von Verfahren den Notwendigkeits- und Verhältnismäßigkeitserfordernissen genügen könnte, die sich letztendlich daraus ergeben, welche Grundrechtseingriffe vom EuGH und EGMR für hinnehmbar gehalten werden.

33. Des Weiteren **empfehlen** der EDSA und der EDSB ein sowohl für Behörden als auch für private Rechtspersonen geltendes **Verbot von KI-Systemen, die natürliche Personen anhand biometrischer Merkmale (z. B. aus der Gesichtserkennung) bestimmten Kategorien zuordnen, etwa nach ethnischer Herkunft, Geschlecht, politischer oder sexueller Orientierung oder nach sonstigen gemäß Artikel 21 der Charta verbotenen Diskriminierungsgründen,** bzw. von KI-Systemen, deren wissenschaftliche Validität nicht erwiesen ist oder die wesentlichen Werten der Union direkt zuwiderlaufen (z. B. Lügendetektor, Anhang III Nummer 6 Buchstabe b und Nummer 7 Buchstabe a). Folglich sollte die „**biometrische Kategorisierung**“ nach **Artikel 5 verboten** sein.

34. . Es berührt die Menschenwürde, wenn ein Computer unabhängig vom eigenen freien Willen das künftige Verhalten bestimmt oder klassifiziert. KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden für individuelle Risikobewertungen natürlicher Personen verwendet werden sollen, um das Risiko abzuschätzen, dass eine natürliche Person Straftaten begeht oder erneut begeht, vgl. Anhang III Nummer 6 Buchstabe a; oder um das Auftreten oder erneute Auftreten einer tatsächlichen oder potenziellen Straftat auf der Grundlage des Profils einer natürlichen Person vorherzusagen oder um Persönlichkeitsmerkmale und Eigenschaften oder vergangenes kriminelles Verhalten vorherzusagen, vgl. Anhang III, Nummer 6 Buchstabe e, führen bei bestimmungsgemäßer Verwendung dazu, dass ihnen die Entscheidungsfindung von Polizei und Gerichten maßgeblich unterworfen wird, wodurch der betroffene Mensch zum Objekt gemacht wird. Derartige KI-Systeme, die den Kerngehalt der Menschenwürde berühren, sind nach Artikel 5 zu verbieten.

35. Des Weiteren sind der EDSA und der EDSB der Ansicht, dass die Verwendung von KI **zur Ermittlung des emotionalen Zustands einer natürlichen Person höchst unerwünscht ist und verboten werden sollte**, außer in gewissen, genau umgrenzten Anwendungsfällen, etwa zu Gesundheits- oder Forschungszwecken (z. B. für Patienten, bei denen die Erkennung des Gemütszustands wichtig ist), wobei stets angemessene Garantien bestehen und sämtliche sonstigen datenschutzrechtlichen Bedingungen und Einschränkungen (einschließlich der Zweckbindung) selbstverständlich eingehalten sein müssen.

2.4 Hochrisiko-KI-Systeme

2.4.1 Erfordernis einer von externen Dritten durchgeführten Ex-ante-Konformitätsbewertung

36. Der EDSA und der EDSB begrüßen, dass KI-Systeme, die ein hohes Risiko darstellen, vorab einer Konformitätsbewertung unterzogen werden müssen, bevor sie in den Verkehr gebracht oder in sonstiger Weise in der EU in Betrieb gesetzt werden können. Dieses Regulierungsmodell wird grundsätzlich begrüßt, da es ein ausgewogenes Verhältnis zwischen Innovationsfreundlichkeit und einem hohen Maß an proaktivem Grundrechtsschutz bietet. Die Anwendung in bestimmten Umgebungen, etwa in Entscheidungsprozessen von öffentlichen Diensten oder kritischer Infrastruktur, setzt voraus, dass dargelegt wird, wie der volle Quellcode untersucht werden kann.

37. Der EDSA und der EDSB raten dazu, das in Artikel 43 des Vorschlags vorgesehene Verfahren für die Konformitätsbewertung dahingehend zu ändern, dass **für Hochrisiko-KI grundsätzlich eine von Dritten durchgeführte Ex-ante-Konformitätsbewertung erforderlich** ist. Eine von Dritten durchgeführte Konformitätsbewertung für eine Hochrisiko-Verarbeitung personenbezogener Daten ist zwar weder in der DSGVO noch in der EU-DSVO vorgesehen, doch die mit KI-Systemen verbundenen Risiken werden bislang noch nicht vollends verstanden. Die allgemeine Aufnahme einer Verpflichtung zu einer von Dritten vorgenommenen Konformitätsbewertung würde daher die Rechtssicherheit und das Vertrauen in alle Hochrisiko-KI-Systeme weiter stärken.

2.4.2 Anwendungsbereich der Verordnung muss alle bereits genutzten KI-Systeme erfassen

38. Gemäß Artikel 43 Absatz 4 des Vorschlags, sollten Hochrisiko-KI-Systeme bei jeder wesentlichen Änderung einem neuen Konformitätsbewertungsverfahren unterzogen werden. Es ist richtig, sicherzustellen, dass KI-Systeme während ihres gesamten Lebenszyklus den Anforderungen der KI-Verordnung genügen. KI-Systeme, die bereits in Verkehr gebracht oder in Betrieb genommen wurden, bevor die vorgeschlagene Verordnung Anwendung findet (oder, im Falle der in Anhang IX aufgeführten IT-Großsysteme, 12 Monate danach) sind aus deren Anwendungsbereich ausgenommen, sofern die Systeme nicht einer „wesentlichen Änderung" der Konzeption oder Zweckbestimmung unterliegen (Artikel 83).

39. Allerdings ist unklar, ab wann es sich um eine „wesentliche Änderung" handelt. In Erwägungsgrund 66 des Vorschlags ist eine niedrigere Schwelle für eine neue Konformitätsbewertung angegeben, nämlich „wenn eine Änderung eintritt, die die Einhaltung dieser Verordnung durch das System beeinträchtigen könnte". Für Artikel 83 wäre eine ähnliche Schwelle, zumindest für Hochrisiko-KI-Systeme, angemessen. Zusätzlich ist es, um etwaige Schutzlücken zu schließen, erforderlich, dass auch bereits bestehende und in Betrieb befindliche KI-Systeme – nach einer gewissen Implementierungsphase – allen Anforderungen der KI-Verordnung genügen.

40. Die Sicherheit von KI-Systemen wird auch durch die vielfältigen Möglichkeiten der Verarbeitung personenbezogener Daten sowie externe Risiken beeinträchtigt. Artikel 83 fokussiert auf eine „wesentliche Änderung der Konzeption oder Zweckbestimmung", ohne jedoch Änderungen externer Risiken zu erwähnen. In Artikel 83 des Vorschlags sollte daher auf Änderungen der Gefährdungslage Bezug genommen werden, die sich aus externen Risiken ergeben, z. B. Cyberangriffe, feindliche Angriffe und begründete Beschwerden von Verbrauchern.

41. Da überdies der Geltungsbeginn erst 24 Monate nach dem Inkrafttreten der künftigen Verordnung vorgesehen ist, erscheint es dem EDSB und dem EDSA unangemessen, bereits in Verkehr gebrachte KI-Systeme für einen noch längeren Zeitraum von der Anwendung auszunehmen. Auch wenn der Vorschlag außerdem vorsieht, dass die Anforderungen der Verordnung bei der Bewertung jedes IT-Großsystems zu berücksichtigen sind, so wie dies in den in Anhang IX aufgeführten Rechtsakten bestimmt ist, sind der EDSA und der EDSB der Ansicht, dass die Anforderungen für die Inbetriebnahme von KI-Systemen ab dem Datum des Geltungsbeginns der künftigen Verordnung anwendbar sein sollten.

2.5 Leitungsstruktur und Europäischer Ausschuss für künstliche Intelligenz

2.5.1 Leitungsstruktur

42. Der EDSA und der EDSB begrüßen die Benennung des EDSB als die zuständige Behörde und Marktüberwachungsbehörde für die Aufsicht über die in den Anwendungsbereich dieses Vorschlags fallenden Organe, Einrichtungen und sonstigen Stellen der Union. Der EDSB steht bereit, seine neue Rolle als KI-Regulierungsbehörde für die öffentliche Verwaltung der Union zu erfüllen. Die Rolle und die Aufgaben des EDSB sind allerdings noch nicht hinreichend

detailliert und sollten im Vorschlag präzisiert werden, vor allem in Bezug auf seine Rolle als Marktüberwachungsbehörde.

43. Der EDSA und der EDSB nehmen die Zuweisung der Finanzmittel zur Kenntnis, die im Vorschlag für den Ausschuss und den EDSB, handelnd als notifizierende Stelle, vorgesehen sind. Die Erfüllung der für den EDSB vorgesehenen neuen Pflichten würde jedoch, wenn dieser als notifizierende Stelle handelt, erheblich höhere finanzielle und personelle Ressourcen erfordern.

44. Erstens, weil nach dem Wortlaut von Artikel 63 Absatz 6 für in den Anwendungsbereich des Vorschlags fallende Organe, Einrichtungen und sonstige Stellen der Union der EDSB „die Funktion der für sie zuständigen Marktüberwachungsbehörde [übernimmt]“, woraus jedoch nicht klar wird, ob der EDSB als voll ausgestattete „Marktüberwachungsbehörde“ im Sinne der Verordnung (EU) 2019/1020 anzusehen ist. Dies wirft Fragen hinsichtlich der Pflichten und Befugnisse des EDSB in der Praxis auf. Zweitens ist, wenn man davon ausgeht, dass die vorstehende Frage bejaht wird, unklar, wie die Rolle des EDSB, so wie diese in der EU-DSVO vorgesehen ist, die in Artikel 11 der Verordnung (EU) 2019/1020 vorgesehene Aufgabe wahrnehmen kann, zu der nicht nur „in ihrem Hoheitsgebiet die effektive Marktüberwachung von online … bereitgestellten Produkten“ gehört, sondern auch „anhand angemessener Stichproben physische Überprüfungen und Laborprüfungen [durchzuführen]“. Es besteht das Risiko, dass die Übernahme neuer Aufgaben, ohne weitere Klarstellungen im Vorschlag, die Erfüllung seiner Verpflichtungen als Datenschutzbeauftragter gefährden könnte.

45. Der EDSA und der EDSB heben jedenfalls hervor, dass einige Bestimmungen des Vorschlags, in denen die Aufgaben und Befugnisse der verschiedenen nach der KI-Verordnung zuständigen Behörden, ihr Verhältnis untereinander, ihr Charakter und die Garantie ihrer Unabhängigkeit festgelegt werden, in der jetzigen Phase noch unklar erscheinen. Während es in der Verordnung 2019/1020 heißt, dass die Marktüberwachungsbehörde unabhängig sein muss, ist es nach dem Verordnungsentwurf nicht erforderlich, dass die Aufsichtsbehörden unabhängig sind; diese sind sogar gehalten, der Kommission Bericht zu erstatten über gewisse Aufgaben, die von Marktüberwachungsbehörden, bei denen es sich auch um andere Einrichtungen handeln kann, wahrgenommen werden. Da es im Vorschlag außerdem heißt, dass die Datenschutzbehörden die Marktüberwachungsbehörden für zu Strafverfolgungszwecken eingesetzte KI-Systeme sind (Artikel 63 Absatz 5), bedeutet dies auch, dass sie, möglicherweise über ihre nationale Aufsichtsbehörde, den Berichtspflichten gegenüber der Kommission unterliegen (Artikel 63 Absatz 2); dies dürfte mit ihrer Unabhängigkeit unvereinbar zu sein.

46. Der EDSA und der EDSB halten es deshalb für erforderlich, diese Bestimmungen zu präzisieren, um sie mit der Verordnung 2019/1020, der EU-DSVO und der DSGVO in Einklang zu bringen; außerdem sollte in der KI-Verordnung klar festgelegt werden, dass die Aufsichtsbehörden nach der KI-Verordnung völlige Unabhängigkeit in der Wahrnehmung ihrer Aufgaben genießen müssen, da dies eine wesentliche Garantie für die ordnungsgemäße Beaufsichtigung und Durchsetzung der künftigen Verordnung wäre.

47. Der EDSA und der EDSB möchten auch daran erinnern, dass die Datenschutzbehörden (DSB) in Bezug auf KI-Systeme, die personenbezogene Daten enthalten, bereits die DSGVO, die EU-DSVO und die LED durchsetzen, um den Schutz der Grundrechte und insbesondere das Recht auf Datenschutz sicherzustellen. Deshalb verfügen die DSB bereits in gewissem Umfang über ein Verständnis von KI-Technologien, Daten und Datenverarbeitung, Grundrechten sowie Fachwissen über die Bewertung der von neuen Technologien ausgehenden Grundrechtsrisiken, so wie dies nach dem Vorschlag für die nationalen Aufsichtsbehörden erforderlich ist. Hinzu kommt, dass im Falle von KI-Systemen, die auf der Verarbeitung personenbezogener Daten beruhen oder personenbezogene Daten verarbeiten (was bei den meisten der unter die Verordnung fallenden KI-Systemen der Fall sein wird), die Bestimmungen des Vorschlags und die des Rechtsrahmens für den Datenschutz direkt ineinandergreifen. Deshalb wird es hinsichtlich der Zuständigkeiten Querverbindungen zwischen Aufsichtsbehörden im Sinne des Vorschlags und zwischen den DSB geben.

48. Würden also die DSB als die nationale Aufsichtsbehörden benannt, würde dies einen einheitlicheren Regulierungsansatz ermöglichen und zur kohärenten Auslegung der Datenverarbeitungsvorschriften beitragen sowie vermeiden, dass die Vorschriften in den verschiedenen Mitgliedstaaten in widersprüchlicher Weise durchgesetzt würden. Es käme auch allen Interessenträgern entlang der KI-Wertschöpfungskette zugute, wenn es eine einzige Anlaufstelle für alle in den Anwendungsbereich des Vorschlags fallenden, personenbezogene Daten betreffenden Verarbeitungsvorgänge gäbe, so dass sich die Interaktion zwischen den beiden Regulierungsbehörden, die für die unter den Vorschlag bzw. unter die DSGVO fallenden Verarbeitungen zuständig sind, in Grenzen hielte. Der EDSA und der EDSB sind deshalb der Auffassung, dass **die DSB als die nationalen Aufsichtsbehörden im Sinne von Artikel 59 des Vorschlags benannt werden sollten**.

49. Jedenfalls insoweit, als der Vorschlag auf Artikel 16 AEUV beruhende spezifische Regeln über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten enthält, **muss** die Einhaltung dieser Regeln, insbesondere der Einschränkungen der Verwendung von KI-Systemen zur biometrischen Fernidentifizierung in Echtzeit in öffentlich zugänglichen Räumen für die Zwecke der Strafverfolgung, **der Kontrolle unabhängiger Behörden unterliegen**.

50. Im Vorschlag ist jedoch keine ausdrückliche Bestimmung vorgesehen, nach der die Zuständigkeit für die Sicherstellung der Einhaltung dieser Regeln der Kontrolle unabhängiger Behörden zugewiesen würde. Die einzige Bezugnahme auf für den Datenschutz nach der DSGVO oder der LED zuständige Aufsichtsbehörden findet sich in Artikel 63 Absatz 5 des Vorschlags, jedoch nur in Bezug auf „Marktüberwachungsbehörden“ bzw., alternativ, auf einige andere Behörden. Nach Ansicht des EDSA und des EDSB wird damit die Einhaltung der sich aus Artikel 16 Absatz 2 AEUV und Artikel 8 der Charta ergebenden Anforderung der unabhängigen Überwachung nicht sichergestellt.

2.5.2 Der Europäische Ausschuss für künstliche Intelligenz

51. Der Vorschlag sieht die Einrichtung eines „Europäischen Ausschusses für künstliche Intelligenz“ (EAKI) vor. Der EDSA und der EDSB erkennen an, dass es einer kohärenten und einheitlichen Anwendung des vorgeschlagenen Rahmenwerks wie auch der Mitwirkung unabhängiger Experten bei der Entwicklung der KI-Politik der Union bedarf. Gleichzeitig wird aber der Kommission im Vorschlag eine vorherrschende Rolle zugewiesen. Letztere wäre nicht nur Mitglied im EAKI, sondern würde auch den Vorsitz im Ausschuss führen und hätte ein Vetorecht bei der Annahme der Geschäftsordnung des EAKI. Mit dem Erfordernis, dass das europäische KI-Gremium von politischem Einfluss unabhängig sein muss, steht dies in Konflikt. Der EDSA und der EDSB sind deshalb der Ansicht, dass die künftige KI-Verordnung **dem EAKI mehr Autonomie** einräumen sollte, um ihm zu ermöglichen, die einheitliche Anwendung der Verordnung im Binnenmarkt wirklich sicherzustellen.

52. Der EDSA und der EDSB nehmen auch zur Kenntnis, dass dem EAKI keine Befugnis zur Durchsetzung der vorgeschlagenen Verordnung übertragen wird. In Anbetracht der Verbreitung von KI-Systemen im Binnenmarkt und der Wahrscheinlichkeit grenzüberschreitender Fälle sind jedoch die einheitliche Durchsetzung sowie die ordnungsgemäße Zuständigkeitszuweisung unter den nationalen Aufsichtsbehörden unbedingt erforderlich. Der EDSA und der EDSB empfehlen deshalb, die Mechanismen für die Zusammenarbeit zwischen den nationalen Aufsichtsbehörden in der künftigen KI-Verordnung festzulegen. Der EDSA und der EDSB regen an, einen Mechanismus einzuführen, der für jedes KI-System für die von den Vorschriften betroffenen natürlichen und juristischen Personen eine einzige Anlaufstelle garantiert, wobei für Organisationen, deren Aktivitäten sich auf mehr als die Hälfte der Mitgliedstaaten der Union erstrecken, der EAKI die nationale Behörde benennen kann, die für die Durchsetzung der KI-Verordnung für das betreffende KI-System zuständig ist.

53. Des Weiteren sollte der Ausschuss, im Hinblick auf die Unabhängigkeit der Behörden, aus denen er zusammengesetzt ist, nicht nur berechtigt sein, die Kommission zu beraten und zu unterstützen, sondern auch, aus eigenem Antrieb zu handeln. Der EDSA und der EDSB heben deshalb hervor, dass es erforderlich ist, den dem Ausschuss zugewiesenen Auftrag zu erweitern, der außerdem nicht den im Vorschlag aufgeführten Aufgaben entspricht.

54. Zur Erfüllung dieser Zwecke **sollten dem EAKI ausreichende und angemessene Befugnisse zukommen** und sein rechtlicher Status sollte klargestellt werden. Damit der sachliche Anwendungsbereich der Verordnung relevant bleibt, scheint es insbesondere notwendig, die für ihre Anwendung zuständigen Behörden in die Weiterentwicklung der Verordnung einzubeziehen. Der EDSA und der EDSB empfehlen deshalb, den EAKI zu ermächtigen, der Kommission Änderungen des Anhangs I, in dem Techniken und Konzepte der künstlichen Intelligenz definiert sind, und des Anhangs III, in dem Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2 aufgeführt sind, vorzuschlagen. Der EAKI sollte auch vor jeder Änderung dieser Anhänge von der Kommission konsultiert werden.

55. In Artikel 57 Absatz 4 des Vorschlags ist der Austausch zwischen dem Verwaltungsrat und anderen Einrichtungen, Ämtern, Agenturen und Beratungsgruppen der Union vorgesehen. Unter Berücksichtigung der bisherigen Arbeit der Agentur der Europäischen Union für Grundrechte auf dem Gebiet der KI und ihres Fachwissens im Bereich der Menschenrechte empfehlen EDSA und EDSB, diese als einen der Beobachter des Ausschusses in Betracht zu ziehen.

3 ZUSAMMENSPIEL MIT DEM DATENSCHUTZREGELWERK

3.1 Verhältnis des Vorschlags zum bestehenden Datenschutzrecht der Union

56. Wesentliche Voraussetzung für die Gewährleistung und Aufrechterhaltung der Einhaltung und Anwendung des Besitzstands der Union auf dem Gebiet des Schutzes personenbezogener Daten ist es, klar festzulegen, in welchem Verhältnis der Vorschlag zum bestehenden Datenschutzrecht steht. Dieses Unionsrecht, insbesondere die DSGVO, die EU-DSVO und die LED, sind als Grundstein anzusehen, auf dem weitere Legislativvorschläge aufbauen können, jedoch ohne Beeinträchtigungen oder Eingriffe in die bestehenden Vorschriften; dies gilt auch für die Zuständigkeit der Aufsichtsbehörden und die Leitungsstruktur.

57. EDSA und EDSB halten es deshalb für wichtig, im Vorschlag jegliche Unstimmigkeiten oder etwaige Konflikte mit der DSGVO, der EU-DSVO und der LED klar zu vermeiden. Dies liegt nicht nur im Interesse der Rechtssicherheit, sondern dient auch dazu, zu vermeiden, dass der Vorschlag unmittelbar oder mittelbar darauf hinausläuft, das Grundrecht auf den Schutz personenbezogener Daten, so wie dieses in Artikel 16 AEUV und Artikel 8 der Charta niedergelegt ist, zu gefährden.

58. Insbesondere im Falle selbstlernender Maschinen ist der Schutz personenbezogener Daten natürlicher Personen nur möglich, wenn dieser bereits im Konzept eingebettet ist. Unabhängig vom Zweck der Verarbeitung ist auch die sofortige Möglichkeit der Ausübung der in Artikel 22 DSGVO (Automatisierte Entscheidungen im Einzelfall einschließlich Profiling) bzw. Artikel 23 EU-DSVO niedergelegten Rechte natürlicher Personen von wesentlicher Bedeutung. Diesbezüglich müssen die sonstigen den betroffenen Personen nach den Datenschutzvorschriften zustehenden Rechte, etwa das Recht auf Löschung, das Recht auf Berichtigung, von Anfang an in den KI-Systemen vorgesehen sein, ganz unabhängig vom KI-Konzept oder von der technischen Architektur.

59. Werden für das Lernen der KI-Systeme personenbezogene Daten verwendet, kann das dazu führen, dass im Kern des KI-Systems verzerrte Entscheidungsfindungsmuster erzeugt werden. Deshalb sollten für solche Verfahren verschiedene Schutzvorkehrungen sowie insbesondere qualifizierte menschliche Aufsicht erforderlich sein, um sicherzustellen, dass die Rechte betroffener Personen geachtet und garantiert und jegliche und sämtliche negativen Auswirkungen auf natürliche Personen vermieden werden. Die zuständigen Behörden sollten auch Leitlinien für die Bewertung von Verzerrungen („Bias“) in KI-Systemen vorschlagen und die Ausübung einer menschlichen Aufsicht unterstützen.

60. Wenn personenbezogene Daten für KI-Training und/oder Vorhersagen verwendet werden, sind die betroffenen Personen stets darüber und über die Rechtsgrundlage für diese Verarbeitung zu informieren, sowie über eine allgemeine Erklärung der Logik (des Verfahrens) und des Anwendungsbereichs des KI-Systems. Diesbezüglich sollte in diesen Fällen stets das Recht der natürlichen Personen auf die Einschränkung der Verarbeitung (Artikel 18 DSGVO und Artikel 20 EU-DSVO) sowie auf die Löschung der Daten (Artikel 16 DSGVO und Artikel 19 EU-DSVO) garantiert sein. Des Weiteren sollte der Verantwortliche die ausdrückliche Verpflichtung haben, die betroffene Person über die einschlägigen Fristen für Widerspruch, Einschränkung, Datenlöschung usw. zu informieren. Das KI-System muss in der Lage sein, alle Datenschutzanforderungen durch geeignete technische und organisatorische Maßnahmen zu erfüllen. Durch ein Recht auf Erklärung sollte für zusätzliche Transparenz gesorgt werden.

3.2 Reallabor und Weiterverarbeitung (Artikel 53 und 54 des Vorschlags)

61. Zur Förderung von Innovationen in Europa sind Maßnahmen wie Reallabore, die sich innerhalb der bestehenden rechtlichen und sittlichen Grenzen halten müssen, wichtig. Mit einem Reallabor ist es möglich, die Schutzvorkehrungen zu bieten, die erforderlich sind, um das Vertrauen in KI-Systeme und ihren Gebrauch zu stärken. Komplexe Umgebungen können den KI-Praktikern die ordnungsgemäße Abwägung sämtlicher Interessen erschweren. Insbesondere kleinen und mittleren Unternehmen, die nur über begrenzte Mittel verfügen, kann ein regulatorisches Reallabor schnelleren Erkenntnisgewinn und somit Innovationsförderung ermöglichen.

62. Artikel 53 Absatz 3 des Vorschlags bestimmt, dass die KI-Reallabore die Aufsichts- und Abhilfebefugnisse unberührt lassen. Wenn diese Klarstellung nützlich sein soll, ist es auch erforderlich, eine Anweisung oder Anleitung dazu zu geben, wie sich in Einklang bringen lässt, dass man einerseits eine Aufsichtsbehörde ist und andererseits im Rahmen eines Reallabors detaillierte Anleitungen erteilt.

63. Artikel 53 Abschnitt 6 bestimmt, dass die Modalitäten und Bedingungen für den Betrieb der Reallabore in Durchführungsrechtsakten festgelegt werden. Es ist wichtig, spezifische Leitlinien zu erstellen, um die Einheitlichkeit sowie die Unterstützung bei der Einrichtung und beim Betrieb der Reallabore sicherzustellen. Allerdings könnten verbindliche Durchführungsrechtsakte dem Spielraum, den der Mitgliedstaat bei der Anpassung von Reallaboren an die eigenen Bedürfnisse und örtlichen Gepflogenheiten hat, Grenzen setzen. Der EDSA und der EDSB sollten dem EAKI empfehlen, stattdessen Leitlinien für Reallabore zu erlassen.

64. Artikel 54 des Vorschlags soll eine Rechtsgrundlage für die Weiterverarbeitung personenbezogener Daten zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse im regulatorischen KI-Reallabor geben. Das Verhältnis von Artikel 54 Absatz 1 des Vorschlags zu Artikel 54 Absatz 2 und Erwägungsgrund 41 des Vorschlags und somit zum bestehenden Datenschutzrecht der Union ist nach wie vor unklar. Die DSGVO und die EU-DSVO sehen jedoch bereits eine Grundlage für die „Weiterverarbeitung“ vor. Insbesondere in Fällen, in denen es im öffentlichen Interesse liegt, die Weiterverarbeitung zu gestatten, braucht

die Abwägung der Interessen des Verantwortlichen mit den Interessen der betroffenen Person der Innovation nicht im Wege zu stehen. Zwei wichtige Punkte sind zurzeit noch nicht in Artikel 54 des Vorschlags geregelt: (i) unter welchen Voraussetzungen und unter Anwendung welcher (zusätzlichen) Kriterien die Interessen der betroffenen Personen abgewogen werden und (ii) ob diese KI-Systeme lediglich innerhalb des Reallabors verwendet werden. Der EDSA und der EDSB begrüßen, wenn personenbezogene Daten, die im Rahmen der LED erhoben wurden, in einem Reallabor verarbeitet werden, empfiehlt jedoch, das hier Geplante in einer Weise näher zu spezifizieren, die mit der DSGVO und der EU-DSVO in Einklang steht, indem vor allem klargestellt wird, dass die Rechtsgrundlage für solche Reallabore den in Artikel 23 Absatz 2 DSGVO und Artikel 25 EU-DSVO festgelegten Anforderungen entsprechen sollte, und dass jede Nutzung der Reallabore einer gründlichen Bewertung unterzogen werden muss. Dies gilt auch für die gesamte Liste der in Artikel 54 Absatz 1 Buchstaben b bis j angegebenen Bedingungen.

65. Einige zusätzliche Erwägungen bezüglich der Weiterverwendung von Daten in Artikel 54 des Vorschlags deuten darauf hin, dass der Betrieb eines Reallabor ressourcenintensiv ist und deshalb realistischerweise anzunehmen ist, dass nur eine geringe Anzahl von Unternehmen die Chance hätte, daran teilzunehmen. Die Beteiligung an einem Reallabor könnte einen Wettbewerbsvorteil darstellen. Für die Ermöglichung der Weiterverwendung von Daten wäre es erforderlich, sehr sorgfältig zu überlegen, auf welche Weise die Teilnehmer ausgewählt werden, um sicherzustellen, dass sie im Anwendungsbereich liegen, und unfaire Behandlung zu vermeiden. Der EDSA und der EDSB haben Bedenken, dass die Ermöglichung der Weiterverwendung von Daten im Rahmen des Reallabors vom Grundsatz der Rechenschaftspflicht in der DSGVO, wo die Rechenschaftspflicht dem Verantwortlichen, nicht der zuständigen Behörde auferlegt ist, abweicht.

66. Des Weiteren denken der EDSA und der EDSB, dass die Reallabore nicht in den Anwendungsbereich der LED fallen können, wenn man bedenkt, dass die Ziele, die damit verfolgt werden, die Entwicklung, Erprobung und Validierung von KI-Systemen sind. Die LED sieht zwar vor, Daten für wissenschaftliche Forschung weiterzuwenden, doch die für diesen sekundären Zweck verarbeiteten Daten unterliegen dann der DSGVO oder der EU-DSVO und nicht mehr der LED.

67. Unklar ist, was genau eine regulatorische Reallabor beinhalten wird. Es stellt sich die Frage, ob das vorgeschlagene regulatorische Reallabor eine IT-Infrastruktur in jedem Mitgliedstaat beinhaltet, mit einigen zusätzlichen Rechtsgrundlagen für die Weiterverarbeitung, oder ob man darin lediglich den Zugang zu Fachwissen und Anleitung auf dem Gebiet der Regulierung organisiert. Der EDSA und der EDSB legen dem Gesetzgeber dringend nahe, diesen Begriff im Vorschlag zu präzisieren sowie klar anzugeben, dass das regulatorische Reallabor nicht bedeutet, dass die zuständigen Behörden verpflichtet wären, ihre technische Infrastruktur zur Verfügung zu stellen. Jedenfalls sind den zuständigen Behörden die finanziellen und personellen Mitteln entsprechend der betreffenden Klarstellung zur Verfügung zu stellen.

68. Abschließend möchten der EDSA und der EDSB die Entwicklung grenzüberschreitender KI-Systeme, die für den gesamten europäischen digitalen Binnenmarkt zur Verfügung stehen

werden, hervorheben. Im Falle solcher KI-Systeme sollte das als Innovationsinstrument eingesetzte regulatorische Reallabor die grenzüberschreitende Entwicklung nicht behindern. Der EDSA und der EDSB empfehlen deshalb einen koordinierten grenzüberschreitenden Ansatz, der allen KMU auf nationaler Ebene in ausreichendem Umfang zur Verfügung gestellt wird und einen europaweiten gemeinsamen Rahmen bietet, ohne jedoch zu restriktiv zu sein. Es ist ein angemessener Ausgleich zwischen europäischer Koordinierung und nationalen Verfahren zu erzielen, um zu vermeiden, dass die künftige KI-Verordnung in widersprüchlicher Weise umgesetzt und die unionsweite Innovation dadurch behindert wird.

3.3 Transparenz

69. Der EDSA und der EDSB begrüßen, dass Hochrisiko-KI-Systeme in einer öffentlichen Datenbank (siehe Artikel 51 und Artikel 60 des Vorschlags) registriert werden sollen. Diese Datenbank sollte als Möglichkeit gesehen werden, die allgemeine Öffentlichkeit über den Umfang der Anwendung von KI-Systemen, über bekannte Mängel und Vorfälle, die deren Funktionsweise beeinträchtigen könnten, sowie über die von den Anbietern zu deren Verhinderung und Behebung ergriffenen Maßnahmen zu informieren.

70. Die wechselseitige Kontrolle und Kompetenzabgrenzung („Checks and Balances“) ist ein wichtiger demokratischer Grundsatz. Deshalb geht der Ausnahmetatbestand, der zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten verwendete KI-Systeme von der Transparenzverpflichtung ausnimmt, zu weit. Hier muss zwischen KI-Systemen, die zur Aufdeckung oder Verhütung verwendet werden, und KI-Systemen, die der Ermittlung oder Verfolgung von Straftaten dienen, unterschieden werden. Wegen der Unschuldsvermutung muss es im Bereich der Verhütung und Aufdeckung stärkere Schutzvorkehrungen geben. Des Weiteren bedauern der EDSA und der EDSB, dass der Vorschlag keine Warnhinweise enthält, da dies so verstanden werden könnte, dass sogar die Verwendung von nicht erprobten Hochrisiko-KI-Systemen oder -Anwendungen unbedenklich wäre.

71. In den Fällen, in denen der Öffentlichkeit selbst in einer gut funktionierenden Demokratie aus Geheimhaltungsgründen wenig oder gar keine Transparenz geboten werden kann, sollte es Schutzvorkehrungen geben: Die betreffenden KI-Systeme sollten bei der zuständigen Aufsichtsbehörde registriert sein und dieser gegenüber Transparenz bieten.

72. Das Ziel, bei KI-Systemen Transparenz sicherzustellen, ist eine sehr große Herausforderung. Der rein quantitative Ansatz, dem viele KI-Systeme für die Entscheidungsfindung folgen, unterscheidet sich wesentlich von der auf Kausalitäts- und theoretischen Erwägungen gestützten Vorgehensweise von Menschen und kann mit dem Erfordernis, die von einer Maschine hervorgebrachten Ergebnisse vorab in verständlicher Weise zu erklären, in Konflikt stehen. Die Verordnung sollte neue, stärker proaktive und zeitnahe Möglichkeiten fördern, die die Nutzer von KI-Systemen über den aktuellen Status (der Entscheidungsfindung) informieren und frühzeitig vor potenziell schädlichen Ergebnissen warnen, damit Personen, deren Rechte und Freiheiten möglicherweise durch autonome Entscheidungen der Maschine beeinträchtigt werden, reagieren oder gegen die Entscheidung vorgehen können.

3.4 Verarbeitung von besonderen Datenkategorien und Straftaten betreffenden Daten

73. Die Verarbeitung besonderer Datenkategorien im Bereich der Strafverfolgung unterliegt den Bestimmungen des EU-Datenschutzregelwerks, wozu auch die LED und ihre nationale Umsetzungsbestimmungen zählen. In Erwägungsgrund 41 des Vorschlags heißt es ausdrücklich, dass die Verordnung keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten bildet, auch nicht für besondere Kategorien personenbezogener Daten. Währenddessen heißt es in Artikel 10 Absatz 5 des Vorschlags, dass „die Anbieter solcher Systeme besondere Kategorien personenbezogener Daten … verarbeiten [dürfen]“. Nach derselben Bestimmung sind allerdings zusätzliche Schutzvorkehrungen erforderlich, für die auch Beispiele angeführt werden. Der Vorschlag scheint insoweit in die Anwendung der DSGVO, der LED und der EU-DSVO einzugreifen. Der EDSA und der EDSB begrüßen den Versuch, für angemessene Schutzvorkehrungen zu sorgen, halten jedoch einen kohärenteren regulatorischen Ansatz für erforderlich, da die derzeitigen Bestimmungen nicht hinreichend klar zu sein scheinen, um eine Rechtsgrundlage für die Verarbeitung besonderer Datenkategorien zu bieten; es ist deshalb erforderlich, sie um zusätzliche Schutzmaßnahmen, die noch zu bewerten sind, zu ergänzen. Überdies werden, wenn personenbezogene Daten im Rahmen der LED erfasst worden sind, die etwaigen zusätzlichen Schutzvorkehrungen und Beschränkungen zu berücksichtigen sein, die sich aus den nationalen Bestimmungen zur Umsetzung der LED ergeben.

3.5 Compliance-Mechanismen

3.5.1 Zertifizierung

74. Eine der Hauptsäulen des Vorschlags ist die Zertifizierung. Das im Vorschlag umrissene Zertifizierungssystem, das auf den harmonisierten Normen gemäß der Verordnung (EU) Nr. 1025/2012 und von der Kommission zu erlassenden gemeinsamen Spezifikationen beruht, sieht eine Behördenstruktur (notifizierende Behörden / notifizierte Stellen / Kommission) sowie einen Mechanismus für die Konformitätsbewertung / Zertifizierung, der die für Hochrisiko-KI-Systeme geltenden zwingenden Anforderungen abdeckt, vor. Dieser Mechanismus unterscheidet sich von dem in den Artikeln 42 und 43 DSGVO geregelten Zertifizierungsverfahren, das auf die Sicherstellung der Einhaltung der Datenschutzregeln und -grundsätze abzielt. Anders als im Falle anderer Arten von Zertifikaten (siehe die in Artikel 42 Absatz 2 getroffene Regelung für gemäß der Verordnung (EU) 2019/881 erteilte Zertifizierungen) ist jedoch das Zusammenspiel zwischen den von notifizierten Stellen gemäß dem Vorschlag ausgestellten Bescheinigungen und den in der DSGVO vorgesehenen Datenschutzbescheinigungen, -siegeln und -prüfzeichen unklar.

75. Soweit Hochrisiko-KI-Systeme auf der Verarbeitung personenbezogener Daten beruhen oder personenbezogene Daten verarbeiten, um ihre Aufgabe zu erfüllen, können solche unzureichenden Abstimmungen der verschiedenen Vorschriften für alle beteiligten Stellen zu Rechtsunsicherheit führen, da der Fall eintreten kann, dass KI-Systeme, die gemäß dem Vorschlag zertifiziert und mit CE-Kennzeichnung versehen sind, nach dem Inverkehrbringen oder der Inbetriebnahme auf eine Weise verwendet werden, die nicht mit den Datenschutzvorschriften und -grundsätzen in Einklang steht.

76. Es ist unklar, in welchem Verhältnis der Vorschlag zu dem Datenschutzrecht der Union wie auch der Mitgliedstaaten steht, das für die Hochrisiko-KI-Systeme gilt, die in den einzelnen „Bereichen“ in Anhang III aufgeführt sind. Im Hinblick darauf, dass Hochrisiko-KI-Systeme in hohem Maße in die Grundrechte auf den Schutz der Privatsphäre und den Schutz personenbezogener Daten eingreifen können und es erforderlich ist, ein hohes Maß an Vertrauen in KI-Systeme sicherzustellen, sollten insbesondere die Grundsätze der Datenminimierung und des Datenschutzes durch Technikgestaltung als einer der Aspekte, die zu berücksichtigen sind, bevor eine CE-Kennzeichnung erlangt wird, in den Vorschlag aufgenommen werden. Der EDSA und der EDSB empfehlen deshalb, den Vorschlag dahingehend zu ändern, dass das Verhältnis zwischen den aufgrund der genannten Verordnung erteilten Zertifikaten sowie den Datenschutzbescheinigungen, -siegeln und -prüfzeichen klargestellt wird. Letztlich sollten die Datenschutzbehörden auch bei der Erstellung und Festlegung harmonisierter Normen und gemeinsamer Spezifikationen mitwirken.

77. Was Artikel 43 des Vorschlags, der die Konformitätsbewertung betrifft, angeht, scheint die in Artikel 47 vorgesehene Ausnahme vom Konformitätsbewertungsverfahren sehr weit gefasst, da sie zu viele Ausnahmen, etwa aus außergewöhnlichen Gründen der öffentlichen Sicherheit, des Schutzes des Lebens und der Gesundheit von Personen, des Umweltschutzes und des Schutzes wichtiger Industrie- und Infrastrukturanlagen umfasst. Wir würden den Gesetzgebern vorschlagen, die Ausnahmen enger zu fassen.

3.5.2 Verhaltenskodizes

78. Gemäß Artikel 69 des Vorschlags fördern und erleichtern die Kommission und die Mitgliedstaaten die Aufstellung von Verhaltenskodizes (Kodizes), mit denen erreicht werden soll, dass die Anbieter von KI-Systemen ohne hohes Risiko die Anforderungen, die auf Hochrisiko-KI-Systeme Anwendung finden, freiwillig anwenden. In Übereinstimmung mit Erwägungsgrund 78 der DSGVO empfehlen EDSA und EDSB festzustellen, welche Synergieeffekte zwischen diesen Instrumenten und den in der DSGVO vorgesehenen Verhaltensregeln die Einhaltung des Datenschutzes unterstützen, und diese festzulegen. In diesem Zusammenhang ist es von Belang, klarzustellen, ob der Schutz personenbezogener Daten als eine der „weiteren Anforderungen“ anzusehen ist, die in den in Artikel 69 Absatz 2 genannten Kodizes geregelt werden kann. Von Belang ist auch, sicherzustellen, dass die in den Kodizes zu regelnden „technischen Spezifikationen und Lösungen“ im Sinne von Artikel 69 Absatz 1, die die Einhaltung der Anforderungen im Entwurf der KI-Verordnung fördern sollen, nicht mit den Regeln und Grundsätzen der DSGVO und der EU-DSVO in Konflikt stehen. Wird dies getan, würde es einen Mehrwert darstellen, wenn Anbieter von KI-Systemen ohne hohes Risiko sich – soweit solche Systeme auf der Verarbeitung personenbezogener Daten beruhen oder zur Erfüllung ihrer Aufgabe personenbezogene Daten verarbeiten – an diese Instrumente hielten, da so sichergestellt wird, dass Verantwortliche und Auftragsverarbeiter bei der Verwendung dieser Systeme ihre Datenschutzpflichten erfüllen können.

79. Gleichzeitig liefe dies darauf hinaus, dass der rechtliche Rahmen für vertrauenswürdige KI um die Integration von Kodizes ergänzt würde, um das Vertrauen in die Verwendung dieser Technologie in einer sicheren und rechtskonformen Weise, die auch die Grundrechte achtet, zu

stärken. Die Gestaltung dieser Instrumente sollte jedoch dadurch gestärkt werden, dass Mechanismen vorgesehen werden, die darauf abzielen, zu überprüfen, dass derartige Kodizes als integraler Bestandteil wirksame „technische Spezifikationen und Lösungen“ bieten und „die Erreichung dieser Ziele anhand klarer Vorgaben und wesentlicher Leistungsindikatoren gemessen wird“. Überdies fehlt nicht nur jegliche Bezugnahme auf einen (zwingenden) Überwachungsmechanismus für Verhaltenskodizes, der darauf ausgelegt ist, zu überprüfen, dass die Anbieter von KI-Systemen ohne hohes Risiko die von ihnen aufgestellten Regeln einhalten, sondern es ist den einzelnen Anbietern auch möglich, diese Kodizes selbst festzulegen (und umzusetzen) (vgl. Abschnitt 5.2.7 der Begründung zum Gesetzentwurf), wodurch die Wirksamkeit und Durchsetzbarkeit dieser Instrumente weiter geschwächt werden könnte.

80. Abschließend bitten der EDSA und der EDSB um Klarstellung hinsichtlich der Arten von Initiativen, die die Kommission gemäß Erwägungsgrund 81 des Vorschlags ergreifen kann, „um den Abbau technischer Hindernisse zu erleichtern, die den grenzüberschreitenden Datenaustausch im Zusammenhang mit der KI-Entwicklung behindern“.

4 FAZIT

81. Auch wenn der EDSA und der EDSB den Vorschlag der Kommission begrüßen und eine solche Verordnung für erforderlich halten, um die Grundrechte der EU-Bürger und -Einwohner zu garantieren, sind sie der Ansicht, dass es erforderlich ist, den Vorschlag an verschiedenen Punkten zu überarbeiten, um seine Anwendbarkeit und Wirksamkeit sicherzustellen.

82. Da der Vorschlag wie auch die Fragen, die er zu regeln versucht, komplex sind, bleibt noch viel Arbeit zu leisten, bevor aus dem Vorschlag ein gut funktionierender rechtlicher Rahmen werden kann, der den mit der DSGVO angestrebten Grundrechtsschutz ergänzt und gleichzeitig Innovation fördert. Der EDSA und der EDSB stehen weiterhin zur Verfügung, ihre Unterstützung auf diesem Weg anzubieten.

Brüssel, den 18. Juni 2021

Für den Europäischen Datenschutzausschuss	Für den Europäischen Datenschutzbeauftragten
Die Vorsitzende	Der Datenschutzbeauftragte
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI