21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)258 F
vom 23. November 2026

Schriftliche Stellungnahme

von Prof. Dr. Sarah Rachut, Technische Universität Braunschweig vom 23. November 2026

zu dem

Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung
BT-Drucksache 21/8275

Dem Ausschuss ist das vorliegende Dokument in nicht barrierefreier Form zugeleitet worden.

Technische Universität
Braunschweig
Institut für Rechtswissenschaften
Bienroder Weg 87
38106 Braunschweig

Prof. Dr. Sarah Rachut
Direktorin

Tel. +49 (0) 531 391-2440
sarah.rachut@tu-braunschweig.de
https://www.tu-braunschweig.de/recht

Datum: 23. November 2026

Gutachterliche Stellungnahme

für den Innenausschuss
des Deutschen Bundestages

zum Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung
(KI-Migrationsverwaltungsgesetz – KIMVG)

BT-Drucksache 21/8275

Technische Universität Braunschweig
Institut für Rechtswissenschaften
Juniorprofessur für Öffentliches Recht, Recht der Digitalisierung und Hochschulrecht
Prof. Dr. Sarah Rachut

Inhalt

Vorbemerkung 3
A. Einleitung 4
B. Allgemeine Rechtsgrundlagen, § 7 Abs. 1 AsylG-E, § 86 Abs. 1 AufenthG-E 5
C. Entwicklung von (KI-)Anwendungen, § 7 Abs. 2a AsylG-E, § 86 Abs. 2 AufenthG-E 6
D. Verfahrensmonitoring, § 7a AsylG-E, § 90d AufenthG-E 8
E. Internetabgleich, § 7b AsylG-E, § 90e AufenthG-E 11
F. „Diskriminierungsfreie Algorithmen“ 12
G. Weiterführende Maßnahmen und Evaluierung 13
H. Fazit und Empfehlungen 14

Technische Universität Braunschweig
Institut für Rechtswissenschaften
Juniorprofessur für Öffentliches Recht, Recht der Digitalisierung und Hochschulrecht
Prof. Dr. Sarah Rachut

Vorbemerkung

Der Gesetzentwurf für ein KI-Migrationsverwaltungsgesetz soll als **Artikelgesetz** das Asylgesetz (AsylG) sowie das Aufenthaltsgesetz (AufenthG) anpassen. Die jeweils vorgesehenen Änderungen gleichen sich im Wesentlichen und beziehen sich auf grundlegende Vorgaben zur Verarbeitung personenbezogener Daten (B.), die Entwicklung von (KI-)Anwendungen (C.), das Verfahrensmonitoring (D.) sowie die Möglichkeit eines Internetabgleichs (E.). Aus diesem Grund behandelt die folgende Stellungnahme die vorgesehenen Normierungen thematisch und fasst die geplanten Änderungen von AsylG-E und AufenthG-E zusammen. Den an mehreren Stellen vorkommenden Vorgaben für „diskriminierungsfreie Algorithmen“ ist ein eigener Abschnitt gewidmet (F.).

Ausgehend von der Expertise der Verfasserin konzentriert sich die gutachterliche Stellungnahme auf rechtliche Aspekte und hierbei die Grundrechte sowie das Datenschutz- und KI-Recht.

Das gesteckte Regulierungsziel steht dabei in dem **Spannungsverhältnis**, einen für die jeweiligen Gegebenheiten und technischen Entwicklungen offenen Einsatz zu ermöglichen und zugleich durch konkrete Schutzmaßnahmen die Betroffenenrechte zu schützen. Im Rahmen der Migrationsverwaltung ist hierbei zu beachten, dass einerseits eine Vielzahl von Daten – auch besonders sensible Daten – Gegenstand der Verarbeitung sind und die betroffene Personengruppe andererseits regelmäßig besonders vulnerabel ist und faktisch nur eingeschränkte Kompetenzen hat, Maßnahmen zu überprüfen oder sich gegen diese zu wehren.

Bei der Regulierung komplexer (digitaler) Sachverhalte wie dem KI-Einsatz in der Migrationsverwaltung ist weiter zu beachten, dass hierdurch verschiedene und ebenenübergreifende Rechtsregime betroffen sind. Neben dem nationalen (Migrations-)Verwaltungsrecht betrifft dies insbesondere das (unionale) Datenschutzrecht, die Regulierung von KI-Systemen sowie den Grundrechtsschutz und die Grundrechtsverwirklichung der betroffenen Personen.

Der tatsächliche Rechtsrahmen ergibt sich erst aus einer Zusammenschau mehrerer Normen und unter Berücksichtigung der Grundrechtsauswirkungen im Einzelfall. Welcher Technologieeinsatz daher (noch) zulässig ist und welche konkreten Schutzmaßnahmen zu ergreifen sind, hängt maßgeblich auch von den verarbeiteten Daten, der technischen Ausgestaltung und dem Verfahren ab. Legistisch kann mit diesen Umständen unterschiedlich umgegangen werden: Zum einen kann durch ausdrückliche Verweise und Bezugnahmen oder sogar eine gewisse Redundanz die Anwendbarkeit erleichtert werden. Zum anderen kann mit selbiger Begründung auf genau solche Bezugnahmen verzichtet werden, um den Normtext nicht zu überfrachten. Ob und wie sich die Regulierungstechnik auf die Wirkung der jeweiligen Rechtsnormen auswirkt, lässt sich im Vorhinein nicht vorhersagen, sollte jedoch Gegenstand von Evaluation und Wirkungsanalyse sein.

Technische Universität Braunschweig
Institut für Rechtswissenschaften
Juniorprofessur für Öffentliches Recht, Recht der Digitalisierung und Hochschulrecht
Prof. Dr. Sarah Rachut

A. Einleitung

Der vorliegende Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (KIMVG-E) geht auf ein Eckpunktepapier des Auswärtigen Amtes und des Bundesministeriums des Innern vom 28.10.2025 zurück. Darin wurden die Potenziale eines KI-Einsatzes in der Migrationsverwaltung – insbesondere im Visaverfahren – beschrieben und die Notwendigkeit eines grundrechts- und datenschutzkonformen Rechtsrahmens dargelegt.

Das KIMVG nimmt sich dieses Anliegens an und übersetzt es in konkrete Regulierungsvorschläge im Asylgesetz (AsylG) und Aufenthaltsgesetz (AufenthG). Dabei verfolgt es das Ziel, durch den Einsatz digitaler Verfahren die Effizienz, Einheitlichkeit, Qualität und Sicherheit der Migrations-, Visum- und Asylbearbeitung zu erhöhen, wobei insbesondere die Nutzung von Künstlicher Intelligenz (KI) ermöglicht werden soll.[1] Durch u.a. Mustererkennungen und eine systematische Betrachtung der Verfahren sollen Verwaltungsabläufe beschleunigt und Ressourcen zielgerichteter nutzbar gemacht werden.[2] Der Gesetzentwurf setzt somit auf drei Ebenen an: bei individuellen Verfahren, der Ausgestaltung von Verfahren sowie der tatsächlichen Verwaltungspraxis. **Im Vergleich zum vorangegangenen Referentenentwurf aus dem BMI vom 25.06.2026 zeigt der hiesige Entwurf an vielen Stellen ein insgesamt höheres Schutzniveau.**

Die **Intention** des KIMVG-E, die Potenziale digitaler Technologien, insb. KI, für die Migrationsverwaltung zu realisieren, ist **zu begrüßen**. Sinnvoll digitalisierte, ggf. automatisierte Verfahren sowie ein effizienter Ressourceneinsatz stellen im besten Fall sicher, dass Verfahren schneller durchlaufen, in rechtskonformen – insb. vergleichbaren – Entscheidungen münden und nicht zuletzt die Anliegen der Betroffenen besser adressiert werden. Angesichts vielfältig bestehender und sich abzeichnender Herausforderungen für die öffentliche (Migrations-)Verwaltung bietet der Einsatz digitaler Technologien das Potenzial, die Leistungs- und Funktionsfähigkeit der Verwaltung zu erhalten und zu gewährleisten.

Mit dem KIMVG-E sollen hierfür notwendige Rechtsgrundlagen geschaffen und u.a. die notwendige Datenverarbeitung sowie der Einsatz von Künstlicher Intelligenz ermöglicht werden. Dabei gilt es zu beachten, dass in diesem Zusammenhang **vielfach personenbezogene Daten verarbeitet** werden und jede Verarbeitung von Daten und insbesondere die Zusammenführung besonders sensibler Daten in den Rechtskreis der Betroffenen hineinwirkt, (technische) Angriffspunkte erzeugt und Missbrauchspotenziale schafft. Nicht zuletzt birgt der Einsatz dieser Technologien Diskriminierungspotenziale. Entsprechend werden hierbei die Grundrechte aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1, Art. 3 Abs. 1, 3 GG bzw. Art. 7, 8, 20 f. EU-GrCh tangiert, sodass etwaige Eingriffe zu rechtfertigen und dabei insbesondere am Maßstab der Verhältnismäßigkeit zu messen sind. Den Risiken ist durch **regulatorische Ausgestaltung, technische und organisatorische Maßnahmen** sowie eine **kontinuierliche Evaluation** der neuen Prozesse zu begegnen. Mit Blick auf das KIMVG-E sind auch die durch das BVerfG entwickelten Maßstäbe zur automatisierten Datenauswertung heranzuziehen.

Hinsichtlich der KI-VO ist zu beachten, dass die Vorgaben zu den Hochrisiko-Systemen gem. Art. 113 KI-VO erst ab dem 2.12.2027 gelten. Insoweit im Rahmen des Gesetzgebungsverfahrens auf die

[1] BT-Drs. 21/8275, S. 1.

[2] BT-Drs. 21/8275, S. 1.

Regelungswirkung der KI-VO verwiesen wird, greift dies erst zu diesem Stichtag. Zuvor kann allenfalls vermutet werden, dass sich öffentliche Stellen aus rechtsstaatlichen Gesichtspunkten bereits an die absehbar geltenden Vorgaben der KI-VO halten. Nichtsdestotrotz bestünde in der Zwischenzeit ein **Regelungsdefizit und damit ein Risiko für einen grundrechtswidrigen KI-Einsatz**.

Die praktischen Auswirkungen des KIMVG-E lassen sich bisher nicht absehen. So ist nicht ersichtlich, wie viele der mit der Ausführung von AsylG und AufenthG betrauten Behörden tatsächlich über die notwendigen Voraussetzungen verfügen, einen solchen KI-Einsatz zu realisieren. Jedoch kann das KIMVG-E ebenso als Ermöglichungsgesetz gesehen werden, das den grundlegenden rechtlichen Rahmen schafft, zum Sammeln von Erfahrungswerten beiträgt und so die Modernisierung und Digitalisierung der Migrationsverwaltung fördert.

B. Allgemeine Rechtsgrundlagen, § 7 Abs. 1 AsylG-E, § 86 Abs. 1 AufenthG-E

§ 7 Abs. 1 AsylG-E und § 86 Abs. 1 AufenthG-E stellen die allgemeinen (datenschutzrechtlichen) Rechtsgrundlagen für die Verarbeitung personenbezogener Daten im jeweiligen Anwendungskontext der Gesetze dar und sind praktisch wortgleich. Die hier vorgesehenen Anpassungen schaffen eine Harmonisierung im Wortlaut zwischen den Gesetzen und dem allgemeinen Datenschutzrecht. Die Verwendung des Begriffs „Verarbeitung“ statt „Erhebung“ stellt klar, dass sämtliche Datenverarbeitungen – und nicht nur die Erhebung – von § 7 Abs. 1 AsylG-E bzw. § 86 Abs. 1 AufenthG-E umfasst sind.

Des Weiteren nehmen die Normen Bezug auf besondere Kategorien personenbezogener Daten, die in der Migrationsverwaltung typischerweise auch Gegenstand der dortigen Verarbeitungskontexte sind. Dies sind gem. Art. 9 Abs. 1 DSGVO Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. „Biometrische Daten zur eindeutigen Identifizierung“ umfassen gem. Art. 4 Nr. 14 DSGVO daktyloskopische Daten sowie solche mit speziellen technischen Verfahren gewonnenen personenbezogenen Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen.

Diese Anpassung von § 7 Abs. 1 AsylG-E und § 86 Abs. 1 AufenthG-E ist rechtlich unproblematisch und aus Harmonisierungsgründen zu begrüßen.

C. Entwicklung von (KI-)Anwendungen, § 7 Abs. 2a AsylG-E, § 86 Abs. 2 AufenthG-E

§ 7 Abs. 2a AsylG-E und § 86 Abs. 2 AufenthG-E normieren das Entwickeln von KI-Systemen sowie anderer automatisierter Anwendungen und bilden die Rechtsgrundlage dafür, dass personenbezogene Daten auch für die Entwicklung von KI-Anwendungen sowie anderer automatisierter Anwendungen verarbeitet werden dürfen. Personenbezogene Daten dürfen grundsätzlich nur für festgelegte, eindeutige und legitime Zwecke, Art. 5 Abs. 1 lit. b DSGVO (**Zweckbindungsgrundsatz**), verarbeitet werden. Die Verarbeitung personenbezogener Daten zur Entwicklung einer (KI-)Anwendung unterscheidet sich von dem in § 7 Abs. 1 AsylG-E bzw. § 86 Abs. 1 AufenthG-E genannten Verarbeitungszweck, da die Entwicklung einer solchen Anwendung nicht für die „Erfüllung der Aufgaben erforderlich ist“. Vielmehr geht die Entwicklung solcher Anwendungen darüber hinaus und soll – wie auch in der Gesetzesbegründung beschrieben – allgemein zur Verbesserung der Verfahren und einem effizienteren Ressourceneinsatz beitragen.

Die hierfür notwendigen gesetzlichen Grundlagen – die eine Verarbeitung auf die benannten Zwecke ausweiten – werden durch § 7 Abs. 2a AsylG-E und § 86 Abs. 2 AufenthG-E geschaffen und müssen sich an den Vorgaben des Art. 6 Abs. 4 iVm Art. 23 Abs. 1 DSGVO messen lassen.

Davon zu unterscheiden ist die Vorgabe des Art. 6 Abs. 3 S. 2 DSGVO, wonach der Zweck der Verarbeitung in der Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gem. Art. 6 Abs. 1 lit. e DSGVO für die Erfüllung einer Aufgabe erforderlich sein muss, die im öffentlichen Interesse liegt. Der Erhalt bzw. die Verbesserung der Funktions- und Leistungsfähigkeit der Migrationsverwaltung ist eine solche Aufgabe, die im öffentlichen Interesse liegt.

Die § 7 Abs. 2a AsylG-E und § 86 Abs. 2 AufenthG-E bestimmen und begrenzen den Zweck der Datenverarbeitung durch folgende Vorgaben.

- die Bezugnahme auf Art. 3 Nr. 1 KI-VO für den Begriff des KI-Systems,
- die Klarstellung, dass auch „andere automatisierte Anwendungen“ erfasst sind,
- die Erläuterung, dass „Entwickeln“ insbesondere das Trainieren, Validieren und Testen umfasst,
- die Beschränkung der Entwicklung auf Anwendungen, die der eigenen Aufgabenerfüllung dienen, sowie auf personenbezogene Daten, die zu der Ausführung des jeweiligen Gesetzes erhoben wurden und für die Entwicklung erforderlich sind (Erforderlichkeitsvorbehalt).

Aus der spezialgesetzlichen Vorgabe des § 78 Abs. 1 S. 1, 3 SGB X folgt zudem, dass Sozialdaten hiervon nicht umfasst sind, da für diese eine Zweckänderung ausgeschlossen ist.

Allgemeine Vorgaben zur Datenverarbeitung ergeben sich bereits aus der DSGVO, insbesondere den **Datenschutzgrundsätzen** (Art. 5 DSGVO), und sind auch im Rahmen von § 7 Abs. 2a AsylG-E und § 86 Abs. 2 AufenthG-E zu berücksichtigen.

§ 7 Abs. 2a AsylG-E und § 86 Abs. 2 AufenthG-E müssen weiter dem **Verhältnismäßigkeitsgrundsatz** entsprechen und somit **angemessene Maßnahmen zum Schutz** der von der Datenverarbeitung betroffenen Personen treffen.

Positiv hervorzuheben ist hierbei, dass die Rechtsgrundlage nicht nur den Einsatz von KI, sondern ebenso von „nur“ Automatisierungsanwendungen ermöglicht. Durch diese technikneutrale Formulierung wird zum einen sichergestellt, dass die Regelung nicht auf die nach Art. 3 Nr. 1 KI-VO definierten

KI-Systeme beschränkt bleibt und ebenso andere (auch künftige) Technologien umfasst sind.[3] Zum anderen wird verhindert, dass ein Anreiz für den Einsatz potenziell risikobehafteter KI-Anwendungen geschaffen wird, wenn sich der Zweck ebenso mit einem risikoärmeren und damit weniger grundrechtsinvasiven Automatisierungsansatz verfolgen ließe.

Unklar bleibt jedoch, **welche konkreten Anwendungen** auf Basis von § 7 Abs. 2a AsylG-E, § 86 Abs. 2 AufenthG-E entwickelt werden können. Die Eingrenzung auf solche, die der Aufgabenerfüllung dienen, erscheint angesichts der mit der Entwicklung verbundenen hohen Eingriffsintensität als **nicht bestimmt genug**. Auch fehlt es an einem Kernbereichsschutz, wie er in den weiteren Regelungen des KIMVG-E normiert ist.

Neben dem Erforderlichkeitsvorbehalt (§ 7 Abs. 2a S. 2 AsylG-E bzw. § 86 Abs. 2 S. 2 AufenthG-E), der auf den **Grundsatz der Datenminimierung** (Art. 5 Abs. 1 lit. c DSGVO) einzahlt, sehen § 7 Abs. 2a S. 3 AsylG-E bzw. § 86 Abs. 2 S. 3 AufenthG-E **erforderliche technische und organisatorische Maßnahmen zur Risikoreduktion** vor, die dabei im Ermessen der jeweiligen Behörde stehen. Diese müssen hierbei sicherstellen, „dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden“ (→ hierzu unter F.) sowie eine angemessene Löschfrist festlegen. Mit Blick auf die Löschfristen im Kontext der Entwicklung von KI-Anwendungen ergibt sich die Befürchtung, dass sich eine nahezu unbegrenzte Speicherdauer rechtfertigen ließe, da die für das Training genutzten personenbezogenen Daten weiterhin für die Validierung benötigt würden. Um diesem Risiko zu begegnen, bietet sich eine Klarstellung oder die Festlegung einer gesetzlichen Speicherhöchstdauer an.

Insoweit es sich bei der Anwendung um KI-Systeme iSv Art. 3 Nr. 1 KI-VO handelt, gelten (zukünftig) zudem die **Vorgaben der KI-VO**, die gem. Art. 6 Abs. 2 iVm Anhang III Nr. 7 KI-VO KI-Systeme im Bereich von Migration und Asyl regelmäßig dem Hochrisikobereich zuordnen. Als Konsequenz dessen sind dann – vorbehaltlich der Ausnahmen von Art. 6 Abs. 3 KI-VO – die Anforderungen nach Art. 8 ff. KI-VO zu berücksichtigen. Diese umfassen Vorgaben zu Risikomanagementmaßnahmen, Regelungen zu Daten und Daten-Governance, Dokumentation und Aufzeichnung, Transparenz, menschliche Aufsicht sowie Genauigkeit, Robustheit und Cybersicherheit. Die Regelungen der KI-VO gelten direkt und unmittelbar (vgl. Art. 288 AEUV) und bedürfen keiner weiteren Umsetzung in das nationale Recht; sie sind daher unabhängig von etwaigen Bezugnahmen oder Verweisen durch die Behörden zu befolgen und konkretisieren so, was als erforderliche technische und organisatorische Maßnahmen zur Risikoreduktion iSv § 7 Abs. 2a AsylG-E bzw. § 86 Abs. 2 AufenthG-E zu fordern ist. Die diesbezüglichen Vorgaben gelten gem. Art. 113 KI-VO jedoch erst ab dem 2.12.2027.

Die Vorgaben der § 7 Abs. 2a S. 3 AsylG-E bzw. § 86 Abs. 2 S. 3 AufenthG-E sind auch darüber hinaus erforderlich, da von der Rechtsgrundlage auch solche Anwendungen erfasst sind, die nicht als KI-System einzuordnen sind und daher nicht unter die KI-VO fallen.

[3] Vgl. BT-Drs. 21/8275, S. 13.

Technische Universität Braunschweig
Institut für Rechtswissenschaften
Juniorprofessur für Öffentliches Recht, Recht der Digitalisierung und Hochschulrecht
Prof. Dr. Sarah Rachut

D. Verfahrensmonitoring, § 7a AsylG-E, § 90d AufenthG-E

Mit § 7a Abs. 1 AsylG-E bzw. § 90d Abs. 1 AufenthG-E wird eine weitere Rechtsgrundlage für die Verarbeitung personenbezogener Daten geschaffen – hier zum Zweck eines automatisierten Verfahrensmonitorings.[4] Gegenstand dieses Verfahrensmonitorings sind ausschließlich abgeschlossene Verfahren sowie die bisherige Entscheidungspraxis, sodass sich hieraus verallgemeinerungsfähige Erkenntnisse für die Qualitätsverbesserung künftiger Entscheidungen ableiten lassen. Bewertet werden somit nicht laufende Verfahren oder Einzelfälle.

Auch wenn in § 7a AsylG-E, § 90d AufenthG-E lediglich die Bezeichnung „automatisierte Anwendungen“ genutzt wird und nicht – wie bei § 7 Abs. 2a AsylG-E, § 86 Abs. 2 AufenthG-E – ausdrücklich auch KI in den Wortlaut eingeschlossen wird, erstreckt sich die Rechtsgrundlage durch diese technikoffene Formulierung ebenso auf Anwendungen Künstlicher Intelligenz.[5]

Im Vergleich zu § 7 Abs. 2a AsylG-E und § 86 Abs. 2 AufenthG-E werden in § 7a Abs. 1 AsylG-E und § 90d Abs. 1 AufenthG-E deutlich detailliertere Vorgaben zum Schutz der Betroffenen normiert. Dies folgt u.a. daraus, dass KI-Anwendungen, die Ergebnisse einer zuvor abgeschlossenen menschlichen Tätigkeit verbessern, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern erkennen oder vorbereitende Aufgaben ausführen, – unter weiteren Voraussetzungen – nicht als Hochrisiko-Systeme iSv Art. 6 Abs. 2 iVm Anhang III KI-VO eingeordnet werden, Art. 6 Abs. 3 KI-VO. Entsprechend gelten für diese von § 7a AsylG-E bzw. § 90d AufenthG-E erfassten Einsatzszenarien dann auch nicht die Vorgaben der Art. 8 ff. KI-VO.

Weiter gilt es zu beachten, dass der Zusammenführung von personenbezogenen Daten und der automatisierten Datenanalyse oder -auswertung ein **eigenes Eingriffsgewicht** zukommt, das über das Eingriffsgewicht der ursprünglichen Erhebung hinausgehen kann.[6] Das konkrete Eingriffsgewicht in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) bestimmt sich zum einen durch das Gewicht der zugrundeliegenden Datenerhebungseingriffe und zum anderen aus den zusätzlichen Belastungseffekten durch die Zusammenführung und automatisierte Auswertung. Das Bundesverfassungsgericht hat sich bereits mit der automatisierten Datenanalyse von Polizeidaten befasst und die diesbezüglichen Anforderungen an den Gesetzgeber konkretisiert.[7] Automatisierte Datenanalyse oder -auswertung können demnach einen schwerwiegenden Eingriff in die informationelle Selbstbestimmung bedeuten, welcher sich nur unter sehr engen Voraussetzungen rechtfertigen ließe und Regelungen insbesondere zur Begrenzung von Art und Umfang der Daten und zur Beschränkung der Datenverarbeitungsmethoden normenklar und hinreichend bestimmt erfordert. Die konkreten Anforderungen an die Rechtsgrundlage richten sich nach dem Maßstab der Verhältnismäßigkeit somit im Kern nach dem mit der automatisierten Datenverarbeitung verbundenen Eingriffsintensität in die Grundrechte der Betroffenen. Das hier gegenständliche automatisierte Verfahrensmonitoring unterscheidet sich in seinem Eingriffsgewicht von den automatisierten Datenauswertungen im Polizeikontext, wie sie Gegenstand der bisherigen BVerfG-Rechtsprechung

---

[4] Bzgl. der Notwendigkeit einer eigenen Rechtsgrundlage bei Zweckänderung s. bereits die Ausführungen unter C.

[5] Dies lässt sich auch mittelbar der Begründung entnehmen, die auf Art. 6 Abs. 3 KI-VO Bezug nimmt, BT-Drs. 21/8275, S. 16.

[6] BVerfGE 165, 363, Leitsatz 2, Rn. 66 ff.

[7] BVerfGE 165, 363.

waren.[8] So werden durch das automatisierte Verfahrensmonitoring lediglich verallgemeinerungsfähige Erkenntnisse für künftige Verfahren gewonnen. Die Erkenntnisse aus dem automatisierten Verfahrensmonitoring dienen somit nicht dem Erkenntnisgewinn im Einzelfall – anders im Kontext der Polizei – und die erlangten Erkenntnisse wirken in der Regel nicht auf die Betroffenen, deren Daten automatisiert ausgewertet wurden. Eingriffserhöhend wirkt sich indes aus, dass Art und Umfang der einbezogenen Daten und die Analysemethoden in § 7a AsylG-E, § 90d AufenthG-E nur grundständig geregelt und im Übrigen der Verwaltung überlassen werden.

Im Rahmen von § 7a AsylG-E und § 90d AufenthG-E ergeben sich grundsätzlich zwei unterschiedliche Betroffenenkreise: zum einen Personen, deren Daten aus ihren abgeschlossenen Verfahren in die automatisierte Auswertung einfließen und zum anderen Personen, deren Verfahren durch die Erkenntnisse aus der automatisierten Auswertung angepasst werden. Das Eingriffsgewicht für die erste Gruppe liegt somit in den weiteren Verarbeitungsschritten und den damit verbundenen allgemeinen Risiken (etwa hinsichtlich der IT-Sicherheit oder der Übermittlung von sensiblen Informationen an Dritte), gewonnene Erkenntnisse wirken sich aber nicht auf ihre bereits abgeschlossenen Verfahren aus. Die zweite Betroffenengruppe könnte aufgrund der Erkenntnisse aus dem automatisierten Monitoring einer veränderten Prüfungstiefe unterliegen und durch eine Verschärfung der Verwaltungspraxis in ihren Grundrechten betroffen sein. Darüber hinaus ergibt sich für die zweite Gruppe durch das automatisierte Verfahrensmonitoring ein besonderes Diskriminierungspotenzial, das sich durch die Verallgemeinerung und Übersetzung der Erkenntnisse auf eine Vielzahl von Personen auswirken kann und dem damit hohes Schädigungspotenzial innewohnt.

Aus der Gesetzesbegründung ergibt sich, dass diese grundrechtsrelevanten Risiken grundsätzlich erkannt worden sind. Die in den verschiedenen Absätzen der § 7a AsylG-E bzw. § 90d AufenthG-E vorgesehenen Schutzmaßnahmen für die beiden Betroffenengruppen umfassen dabei:

- Begrenzung der Verarbeitung auf abgeschlossene Verfahren und bereits erhobene Daten
- Erforderlichkeitsvorbehalt
- grds. Ausschluss der Verarbeitung biometrischer Daten
- Zweckbegrenzung auf verallgemeinerungsfähige Erkenntnisse für künftige Verfahren
- abschließender Katalog für die Weiterverarbeitung im Rahmen des Verfahrensmonitorings[9]
- Ausschluss von Profiling
- Ausschluss von diskriminierenden Algorithmen[10]
- Kernbereichsschutz
- besondere Schulungspflicht
- technische und organisatorische Maßnahmen
- Begrenzung der zulässigen Auftragsverarbeitung

Aus der spezialgesetzlichen Vorgabe des § 78 Abs. 1 S. 1, 3 SGB X folgt zudem, dass Sozialdaten hiervon nicht umfasst sind, da für diese eine Zweckänderung ausgeschlossen ist.

Das grundrechtliche Schutzniveau sollte durch folgende Maßnahmen weiter erhöht werden:

---

[8] BVerfGE 150, 244; BVerfGE165, 363..

[9] Der abschließende Charakter ergibt sich aus dem Wortlaut und der Zusammenschau von Abs. 1 und Abs. 2.

[10] S. hierzu unter F.

Der Normtext bezieht sich auf „von [den Behörden] erhoben[e] personenbezogene[e] Daten“ und ist daher in zweifacher Hinsicht unklar. Zum einen könnte die Bezugnahme auf die eigene Erhebung dahingehend ausgelegt werden, dass nur Daten, die originär bzw. erstmalig von der jeweiligen Behörde erhoben wurden, erfasst sein sollen. Insoweit ist nicht klar, welche konkrete Begrenzung hiermit verbunden sein soll. Zum anderen ist dies nicht auf personenbezogene Daten „zum Zweck der

Ausführung des Gesetzes“ begrenzt – wie etwa in § 7 Abs. 2a AsylG-E und § 86 Abs. 2 AufenthG-E vorgesehen. Hier würde ein einheitlicher Wortlaut Rechtsunsicherheiten vermeiden und eine konsistente Anwendung erleichtern.

Zudem sollte klargestellt werden, in welchem Verhältnis die verallgemeinerungsfähigen Erkenntnisse zu der Bearbeitung des Einzelfalls stehen.

Weiter könnte der Kernbereichsschutz dahingehend ausgeweitet werden, dass der Ausschluss nicht nur für „ausschließlich“ dem Kernbereich der privaten Lebensführung zuzuordnenden Erkenntnisse gilt, sondern auch für solche Erkenntnisse besteht, die „im Wesentlichen“ dem Kernbereich zuzuordnen sind. Im Vergleich zu § 7b Abs. 3 AsylG-E bzw. § 90e Abs. 3 AufenthG-E fehlt die Vorgabe, dass die Erfassung von Kernbereichsdaten bereits technisch soweit möglich auszuschließen ist.

Schließlich sollte der Ausschluss der Übermittlung von Informationen an den Herkunftsstaat sowie Personen oder Stellen, die dem Herkunftsstaat zuzurechnen sind, in den Normtext integriert werden, da dies eines der zentralen Risiken für die Betroffenen darstellt. Bisher findet sich dies lediglich in der Gesetzesbegründung.[11]

In der Gesamtschau und durch verfassungskonforme Auslegung schaffen die vorgesehenen Regelungen wohl bereits ein den Risiken angemessenes Schutzniveau, das sich punktuell jedoch noch verbessern ließe. Die durch das BVerfG für die automatisierte Datenauswertung im Polizeikontext aufgestellten Maßstäbe lassen sich aufgrund des anderen Risikoprofils zwar nicht unmittelbar übertragen, zeigen jedoch auf, dass den mit einer automatisierten Datenauswertung verbundenen Eingriffen ein eigenes Gewicht zukommt, dem es durch verhältnismäßige Schutzmaßnahmen zu begegnen gilt. Angesichts dessen, dass dem automatisierten Verfahrensmonitoring besonders sensible Daten (in Ausnahmefällen auch biometrische Daten) zugrunde liegen und sich für künftige Verfahren ein bedeutendes Diskriminierungsrisiko ergibt, wird angeregt, die aufgezeigten Anpassungen zur Erhöhung des Schutzniveaus aufzunehmen.

Insoweit in der Gesetzesbegründung[12] auf die umfassenden Vorgaben der KI-VO verwiesen wird, so wird verkannt, dass die auf Grundlage von § 7a AsylG-E bzw. § 90d AufenthG-E eingesetzten KI-Anwendungen mitunter nicht in den Hochrisikobereich der KI-VO fallen dürften und daher die beschriebenen Vorgaben aus Art. 8 ff. KI-VO gerade nicht greifen. Zu solchen gem. Art. 6 Abs. 3 KI-VO von der Einordnung als Hochrisiko-System ausgenommenen Anwendungen zählen u.a. solche, die Ergebnisse einer zuvor abgeschlossenen menschlichen Tätigkeit verbessern, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern erkennen oder vorbereitende Aufgaben ausführen. Dies kann bei der Gewinnung von verallgemeinerungsfähigen Erkenntnissen über das Verwaltungsverfahren und die Verwaltungspraxis der Fall sein. § 7a AsylG-E bzw. § 90d AufenthG-E zielen gerade nicht auf die Entscheidung im Einzelfall ab und sollen menschliche Entscheidungen nicht

[11] BT-Drs. 21/8275, S. 18.

[12] BT-Drs. 21/8275, S. 18.

durch automatisierte ersetzen. **Die entsprechenden Ausführungen in der Begründung sollten daher angepasst werden.**

Redaktionell bereinigt werden sollte darüber hinaus die Doppelung von „gewichtet werden“ in § 7a Abs. 2 S. 2 Nr. 3 AsylG-E.

E. Internetabgleich, § 7b AsylG-E, § 90e AufenthG-E

Das Bundesamt bzw. die mit der Ausführung des AufenthG betrauten Behörden werden durch § 7b AsylG-E und § 90e AufenthG-E ermächtigt, einen automatisierten Abgleich mit öffentlich zugänglichen Daten aus dem Internet durchzuführen. Im Vergleich zur Fassung im Referentenentwurf zeigen sich hier die größten Unterschiede, da sich § 7b AsylG-E nun nur noch auf das Bundesamt (und nicht alle mit der Ausführung dieses Gesetzes betrauten Behörden) erstreckt, die Verarbeitung auf das Abgleichen von entscheidungserheblichen Informationen im Einzelfall beschränkt und bzgl. biometrischer Daten ausgeschlossen sowie die Weiterverarbeitung zu anderen Zwecken ausgeschlossen wird. Durch diese Vorgaben wurde das mit dem automatisierten Abgleich verbundene **Eingriffsgewicht reduziert**.

Durch die Beschränkung auf einen Abgleich im Einzelfall bei tatsächlichen Anhaltspunkten für begründete Zweifel an der Richtigkeit decken § 7b AsylG-E und § 90e AufenthG-E nur einen kleinen Teil davon ab, was allgemein als Open Source Intelligence-Analyse (OSINT) bezeichnet wird. Die Normen ermöglichen **keine allgemeine Informationssammlung aus öffentlich zugänglichen Quellen**, um durch deren Analyse Erkenntnisse für das Verwaltungsverfahren zu gewinnen.

Der Wortlaut sollte jedoch im Vergleich auf die Ausgestaltung von § 7a AsylG-E und § 90d AufenthG-E, § 15b AsylG sowie in Hinblick auf die in der Begründung getätigten Ausführungen ergänzt und konkretisiert werden.

Hierzu zählt die Bezugnahme auf „zugängliche öffentliche Quellen“, die mutmaßlich anders als bei § 15b AsylG (dort „allgemein zugängliche öffentliche Quellen“) zu verstehen sein soll. In diesem Fall ist auf gesetzlicher Ebene zu konkretisieren, welche Datenquellen genutzt werden dürfen.

Weiter ergibt sich die Beschränkung auf einen weniger eingriffsinvasiven methodisch einfachen Datenabgleich lediglich aus einer Auslegung des Begriffs „Abgleich“ in Abgrenzung zu „Analyse“ oder „Auswertung“. Die nach der Begründung geforderte Begrenzung auf methodisch einfache Abgleichverfahren sollte in den Normtext aufgenommen werden.

Durch Abs. 5 wird auf die Vorgaben des § 7a Abs. 5, 6 AsylG-E bzw. § 90d Abs. 5, 6 AufenthG-E verwiesen, sodass auf die diesbezüglichen Ausführungen (z.B. hinsichtlich der Übermittlung von Daten an den Herkunftsstaat) verwiesen wird.

Außerdem sieht Abs. 4 S. 3 jeweils eine Dokumentation des Abgleichs, des Ergebnisses des Abgleichs sowie des Löschens der Daten vor. Hier sollte der Anlass des Abgleichs in die Dokumentation aufgenommen werden, um sicherzustellen, dass die Voraussetzungen nach Abs. 1 überhaupt vorlagen,

insbesondere tatsächliche – und welche konkreten – Anhaltspunkte für begründete Zweifel an der Richtigkeit der Informationen gegeben waren.[13]

Schließlich soll ausweislich der Begründung für „tatsächliche Anhaltspunkte“ ausreichen, dass für „konkrete Erkenntnisse aus der Beobachtung vergangener Verfahren vorliegen, dass bestimmte Dokumente oder Angaben von bestimmten Orten oder Regionen besonders häufig als falsch aufgefallen sind und daher besonders kritischer Überprüfung bedürfen“.[14] Diese generalisierten Verdachtsmomente – gewonnen womöglich aus dem automatisierten Verfahrensmonitoring – lassen sich nicht (mehr) mit der in Abs. 1 geforderten Einzelfallüberprüfung aufgrund tatsächlicher Anhaltspunkte vereinen. Die diesbezüglichen Ausführungen sollten aus der Begründung entfernt und die Anforderungen an die „tatsächlichen Anhaltspunkte“ konkretisiert werden. Hierbei sollte klargestellt werden, dass nicht nur die Auswertung der Ergebnisse des Abgleichs, sondern bereits die Voraussetzungen für den Abgleich manuell zu überprüfen sind, um nicht erforderliche Abgleiche auszuschließen.

F. „Diskriminierungsfreie Algorithmen“

Das KIMVG-E sieht an mehreren Stellen vor, dass die Behörden sicherzustellen haben, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Diese Vorgabe dürfte sich bereits aufgrund der konkreten Anwendungsfälle, die gerade die statistische Auswertung aufgrund von bestimmten Merkmalen wie Herkunft, Religion, Alter, sexueller Orientierung oder Geschlecht erfordern, als kaum umsetzbar erweisen. Technisch kommt hinzu, dass Anwendungen, die auf Daten trainiert werden, auch die in diesen enthaltenen unmittelbaren oder mittelbaren Ungleichbehandlungen übernehmen, fortführen und sogar verstärken können. Eine „Diskriminierungsfreiheit“ dürfte sich in diesem Sinne daher nicht ohne Weiteres realisieren lassen. Vielmehr bedarf es konkreter Vorgaben dafür, welche Anforderungen ein solcher Algorithmus zu erfüllen hat und wie die im Rahmen von automatisierten Anwendungen erzeugten Erkenntnisse nicht diskriminierend in das Verwaltungsverfahren wirken. Hierfür ist zunächst ein vertieftes Verständnis über die grundsätzliche Funktionsweise und daraus folgende Limitationen, die Datenquellen und deren Vollständigkeit und Qualität sowie die Robustheit eines Systems erforderlich. Sodann müssen Anforderungen an die Qualitätssicherung, die (menschliche) Kontrolle und ebenso den Rechtsschutz hinsichtlich der auf solchen Ausgaben beruhenden Entscheidungen getroffen werden. Zentral sind somit Vorgaben zur Transparenz und Nachvollziehbarkeit der behördlichen Entscheidungen – auch darüber, ob und inwieweit die Erkenntnisse aus solchen automatisierten Anwendungen in eine Entscheidung eingeflossen sind bzw. einfließen konnten. Zu berücksichtigen sind hierbei auch die Erkenntnisse über das Zusammenwirken von Menschen und Maschine (automation bias, confirmation bias, Ankereffekt u.ä.).

Ebenso unbestimmt ist, wie die menschliche Verantwortung und ein „menschliches Entscheiden“ behördenintern durch Technik- und Organisationsvorgaben gesichert werden kann, etwa welche

---

[13] Dies stellt zugleich sicher, dass keine milderen Mittel zur Überprüfung der Angaben zur Verfügung standen, vgl. hierzu auch BVerwG, Urt. v. 16.2.2023 – 1 C 19.21, Rn. 24.

[14] BT-Drs. 21/8275, S. 19.

Sorgfalts- und Prozesspflichten hier gelten, wie Fehler und Diskriminierungen erkannt und wie auf solche reagiert werden muss. Erforderlich erscheinen hier etwa Vorgaben zu Dateien und Datenkategorien, Löschverfahren und Protokollierung, Festlegung, Dokumentation, Überprüfung und Veröffentlichung der Kriterien, Prüfmethode und -abstände für Verzerrungen, Anforderungen an Auftragsverarbeiter, Betrieb und Hardware.

Bezüglich all dieser Punkte verschiebt das KIMVG-E die Verantwortung pauschal auf die nachgelagerten Stellen, hier die Behörden. **Angesichts der hohen grundrechtlichen Relevanz (Art. 3 GG) müssen die wesentlichen Vorgaben dafür, wie ein nicht diskriminierender Einsatz sichergestellt werden soll, indes durch den Gesetzgeber erfolgen.** Denkbar wäre es auch, diese um eine Verordnungsermächtigung zu ergänzen und eine weitere Konkretisierung auf Verordnungsebene vorzunehmen.

G. Weiterführende Maßnahmen und Evaluierung

Mit dem KIMVG-E werden ambitionierte Ziele verfolgt und hierzu der Einsatz von KI und weiteren automatisierenden Anwendungen normiert. Dem Gesetz kommt somit ein ermöglichender Charakter zu, wobei sich zeigen muss, wie sich der Einsatz solcher Anwendungen auf die Qualität und Effizienz sowie den Ressourceneinsatz in der Migrationsverwaltung auswirkt und welche Risiken sich für die Grundrechte der Betroffenen realisieren. Entsprechend sollten die mit dem KIMVG-E verfolgten Ziele nach einer angemessenen Zeit evaluiert und bewertet werden (**Wirksamkeitsbetrachtung**[15]), ob die Zielerreichung die vorgesehenen Datenverarbeitungen tatsächlich rechtfertigt und sich die vorgesehenen Schutzmaßnahmen (etwa bzgl. der diskriminierungsfreien Algorithmen) als ausreichend erwiesen haben.

Eine Evaluierung ist bisher nicht ausdrücklich vorgesehen, sondern soll sich nach dem Evaluierungskonzept der Bundesregierung richten.[16] Angesichts der grundrechtlichen Bedeutung und der vulnerablen Betroffenengruppe wäre eine ausdrückliche Evaluierungsvorgabe vorzugswürdig.

Daneben sieht das KIMVG-E bisher von Transparenz- und weitestgehend von Dokumentationspflichten ab. Solche können sich jedoch aus den Vorgaben der DSGVO ergeben, erstrecken sich jedoch nur auf die Verarbeitung der eigenen personenbezogenen Daten. Insoweit ist zu befürchten, dass der Einsatz von KI und automatisierten Anwendungen für die Betroffenen dennoch in Teilen unsichtbar bleibt, obwohl er geeignet ist, sich zumindest mittelbar auf die Verwaltungsentscheidungen auszuwirken. Dies ist z.B. dann der Fall, wenn das Verfahren aufgrund des automatisierten Verfahrensmonitorings angepasst wurde. Hierdurch wird unnötig ein gewisses rechtsstaatliches Risiko geschaffen. Aus rechtsstaatlichen Gesichtspunkten – u.a. in Hinblick auf die Transparenz staatlicher Entscheidungen – erscheint eine Ergänzung um Transparenzpflichten gegenüber den Betroffenen geboten.

Weiter können durch die geforderten Konkretisierungen gemeinsame Referenzmaßstäbe geschaffen und so auf eine einheitliche Verwaltungspraxis hingewirkt werden.

---

[15] Vgl. hierzu auch Rachut, Grundrechtsverwirklichung in digitalen Kontexten, 2025, S. 679.

[16] BT-Drs. 21/8275, S. 12.

Schließlich sollte das Risiko in der Übergangszeit bis zur Geltung der entsprechenden Vorgaben der KI-VO bedacht und normativ adressiert werden.

H. Fazit und Empfehlungen

Die **Zielsetzung** des KIMVG-E, die Migrationsverwaltung besser und effizienter zu gestalten und so nicht nur den Ressourceneinsatz zu optimieren, sondern zugleich den Anliegen der Betroffenen durch schnellere Entscheidungen gerecht zu werden, ist **begrüßenswert**.

Die hierfür **geplanten Regelungen** sind im Vergleich zur Fassung des Referentenentwurfs grundrechtsschonender ausgestaltet. Mit dem geplanten Einsatz von automatisierten Anwendungen sowie Künstlicher Intelligenz gehen Grundrechtseingriffe einher, die eine Rechtfertigung entsprechend ihrer jeweiligen Eingriffsintensität erforderlich machen. Dem Wunsch nach schlanken Regelungen zur Komplexitätsreduktion steht dabei nicht nur das Bedürfnis der Normadressaten und Betroffenen nach klaren und bestimmten Vorgaben, sondern auch die Wesentlichkeitsrechtsprechung des Bundesverfassungsgerichts gegenüber. Diese verlangt, dass grundrechtswesentliche Entscheidungen durch den Gesetzgeber zu treffen sind und nicht auf die Verwaltungsebene delegiert werden dürfen.

Entsprechend bietet es sich an folgende Punkte des Gesetzentwurfs noch nachzuschärfen und insbesondere bisher nur in der Begründung vorgesehene Schutzvorkehrungen in den Normtext zu überführen:

1. Es gilt zu konkretisieren, **welche konkreten Anwendungen** auf Basis von § 7 Abs. 2a AsylG-E, § 86 Abs. 2 AufenthG-E entwickelt werden können. Die Eingrenzung auf solche, die der Aufgabenerfüllung dienen, erscheint angesichts der mit der Entwicklung verbundenen hohen Eingriffsintensität als noch **nicht bestimmt genug**.

2. Die Bestimmung und Einhaltung erforderlicher technischer und organisatorischer Maßnahmen zur Risikoreduktion wird den jeweiligen Behörden überlassen. Hier bietet es sich an, zumindest grundlegende Vorgaben normativ festzulegen (z.B. in Hinblick auf Speicherhöchstdauer und Löschfristen). Dies kann auf Gesetzesebene oder in Form einer Rechtsverordnung erfolgen. Etwaige Konkretisierungen durch die Art. 8 ff. KI-VO gelten erst ab dem 2.12.2027 und nur für solche Anwendungen, die als KI-System iSv Art. 3 Nr. 1 KI-VO einzuordnen sind.

3. Hinsichtlich des **Verfahrensmonitorings** nach § 7a AsylG-E, § 90d AufenthG-E sollten die Datenquellen konkretisiert und klargestellt werden, in welchem Verhältnis die verallgemeinerungsfähigen Erkenntnisse zu der Bearbeitung des Einzelfalls stehen. Etwaige Widersprüche zwischen Normtext und Begründung sollten aufgelöst werden. Hierzu zählt u.a. die Aufnahme des Herkunftslandschutzes in den Normtext. In der Gesamtschau und durch verfassungskonforme Auslegung schaffen die vorgesehenen Regelungen wohl bereits ein den Risiken angemessenes Schutzniveau, das sich punktuell jedoch noch verbessern ließe. Die durch das BVerfG für die automatisierte Datenauswertung im Polizeikontext aufgestellten Maßstäbe lassen sich aufgrund des anderen Risikoprofils zwar nicht unmittelbar übertragen, zeigen jedoch auf, dass den mit einer automatisierten Datenauswertung verbundenen Eingriffen ein eigenes Gewicht zukommt, dem es durch verhältnismäßige Schutzmaßnahmen zu begegnen gilt. Angesichts dessen, dass dem automatisierten Verfahrensmonitoring besonders sensible Daten (in Ausnahmefällen auch biometrische Daten)

zugrunde liegen und sich für künftige Verfahren ein bedeutendes Diskriminierungsrisiko ergibt, wird angeregt, die aufgezeigten Anpassungen zur Erhöhung des Schutzniveaus aufzunehmen.

4. § 7b AsylG-E, § 90e AufenthG-E ermöglichen zwar **keine umfassende OSINT-Analyse**, der Wortlaut sollte jedoch im Vergleich auf die Ausgestaltung von § 7a AsylG-E und § 90d AufenthG-E, § 15b AsylG sowie in Hinblick auf die in der Begründung getätigten Ausführungen ergänzt und konkretisiert werden. So ergibt sich die Beschränkung auf einen **weniger eingriffsinvasiven methodisch einfachen Datenabgleich** lediglich aus einer Auslegung des Begriffs „Abgleich" in Abgrenzung zu „Analyse" oder „Auswertung". Die nach der Begründung geforderte Begrenzung auf methodisch einfache Abgleichverfahren ist daher in den Normtext aufzunehmen. Insoweit Abs. 4 S. 3 jeweils eine **Dokumentation** des Abgleichs, des Ergebnisses des Abgleichs sowie des Löschens der Daten vorsieht, sollte dies um den **Anlass des Abgleichs** ergänzt werden, um sicherzustellen, dass die Voraussetzungen nach Abs. 1 überhaupt vorlagen, insbesondere tatsächliche – und welche konkreten – Anhaltspunkte für begründete Zweifel an der Richtigkeit der Informationen gegeben waren. Die insoweit in der Begründung beschriebenen generalisierten Verdachtsmomente – gewonnen womöglich aus dem automatisierten Verfahrensmonitoring – lassen sich nicht (mehr) mit der in Abs. 1 geforderten Einzelfallüberprüfung aufgrund tatsächlicher Anhaltspunkte vereinen. Die diesbezüglichen Ausführungen sollten aus der Begründung entfernt und die **Anforderungen an die „tatsächlichen Anhaltspunkte"** konkretisiert werden. Hierbei sollte klargestellt werden, dass nicht nur die Auswertung der Ergebnisse des Abgleichs, sondern bereits die Voraussetzungen für den Abgleich manuell zu überprüfen sind, um nicht erforderliche Abgleiche auszuschließen.

5. Das KIMVG ist weiter um **konkrete Vorgaben zum Diskriminierungsschutz** sowie der **Transparenz** des KI-Einsatzes gegenüber den Betroffenen zu ergänzen. Die bisherige Vorgabe zur Sicherstellung, dass diskriminierende Algorithmen nicht herausgebildet und verwendet werden, ist zu unbestimmt.

6. Mit Blick auf den gestreckten **Geltungsbeginn der KI-VO** kann zwischen Inkrafttreten des KIMVG und der Geltung der KI-spezifischen Vorgaben auf EU-Ebene (insbesondere hinsichtlich der Anforderungen an Hochrisiko-Systeme) eine **regulatorische Lücke** entstehen. Hier sollte sichergestellt werden, dass die Regelungen des KIMVG, die die Geltung von Regelungen aus der KI-VO voraussetzen, auf den diesbezüglichen Geltungsbeginn abgestimmt sind oder die Berücksichtigung dieser bereits jetzt als verpflichtend normieren.

7. Angesichts der geplanten Ausweitung der Datenverarbeitung, der Unklarheit über die konkrete Wirkweise sowie die Vulnerabilität der Betroffenen sollte eine zeitnahe **Evaluation** der mit dem KIMVG verfolgten Maßnahmen erfolgen, um bewerten zu können, ob die gewünschten Effizienzgewinne erzielt werden konnten, wie sich diese auf die Grundrechte der Betroffenen auswirken und ob und welche weniger eingriffsinvasiven Verarbeitungsprozesse gleichfalls geeignet wären.

8. Punktuell enthält der Gesetzentwurf noch **redaktionelle Fehler**, die es auszubessern gilt.