DVD Deutsche Vereinigung für Datenschutz e. V.

Reuterstraße 157
53113 Bonn

Telefon: 0228 / 22 24 98
Telefax: 0228 / 24 38 470

dvd@datenschutzverein.de
www.datenschutzverein.de

Datum: 02.07.2026

Stellungnahme der

Deutschen Vereinigung für Datenschutz e. V. (DVD)

zum Referentenentwurf eines

Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (KIMVG)

Verbändeanhörung, E-Mail vom 26.06.2026, Az. 260626_BMI MI1 und MI6

Stand 02.07.2026

Dr. Thilo Weichert

weichert@datenschutzverein.de
Waisenhofstraße 41, 24103 Kiel
www.datenschutzverein.de

Inhalt

1 Einführung 3
2 Generalklauseln zur Datenverarbeitung (§ 7 Abs. 1 AsylG, § 86 Abs. 1 AufenthG) 4
3 Entwickeln von automatisierten Anwendungen (KI-Systemen, § 7 Abs. 2 AsylG, § 86 Abs. 2 AufenthG) 5
3.1 Entwicklung von KI-Systemen – Allgemeines 5
3.2 Datengrundlage 6
3.3 Technisch-organisatorische Vorkehrungen 8
4 Automatisiertes Verfahrensmonitoring (Art. 7a AsylG, § 90 AufenthG) 10
4.1 Personenbezogene Datennutzung 10
4.2 Vorrang der menschlichen Entscheidung? 11
4.3 Schutzmaßnahmen 12
5 Automatisierter Abgleich mit Internetdaten (§ 7b AsylG, § 90e AufenthG) 14
6 Betroffenentransparenz 14
7 Evaluierung? 15
8 Ergebnis 16

Die Deutsche Vereinigung für Datenschutz e.V. (ab hier DVD) nimmt die Gelegenheit wahr zu dem im Betreff genannten Gesetzentwurf trotz der engen vom Bundesinnenministerium gesetzten Frist fristgerecht Stellung zu beziehen.

1 Einführung

Der Referentenentwurf des Bundesministeriums des Innern (BMI) verfolgt das Ziel die datenschutzrechtlichen Regelungen im Asylgesetz (AsylG) und im Aufenthaltsgesetz (AufenthG) so zu ändern, dass künftig zwecks Modernisierung von Verwaltungsabläufen und effizienterem Ressourceneinsatz in ausländerrechtlichen Verfahren automatisierte Verfahren und insbesondere sog. Künstliche Intelligenz (KI) unter Wahrung der europa- und verfassungsrechtlichen Vorgaben zum Einsatz kommen kann.

Das Anliegen einer verbesserten Digitalisierung im ausländerrechtlichen Bereich wird von der DVD im Grundsatz unterstützt.

Wenn im folgenden Text Seitenangaben gemacht werden, beziehen diese sich auf den Referentenentwurf und dessen Begründung.

Hintergrund der Gesetzesinitiative ist, dass die vorhandenen personellen und organisatorischen Kapazitäten nicht ausreichen, um die Verfahren innerhalb angemessener Fristen zu bearbeiten: „Die Komplexität rechtlicher Vorgaben, unterschiedliche Verfahrensarten und individuelle Sachverhalte führen zu einer uneinheitlichen Verwaltungspraxis und erschweren eine einheitliche Rechtsanwendung. … Ziel des Gesetzes ist es, durch den Einsatz digitaler Verfahren – insbesondere Künstlicher Intelligenz – die Effizienz, Einheitlichkeit, Qualität und Sicherheit der Migrations-, Visum- und Asylbearbeitung zu erhöhen“ (S. 1, 10)

Die Lösung des Problems soll darin bestehen, dass Rechtsgrundlagen zur personenbezogenen Datenverarbeitung geschaffen werden für „automatisierte Anwendungen der Datenverarbeitung – insbesondere KI-Systeme und KI-Modelle – zu entwickeln, zu trainieren, zu validieren und zu testen“ und diese in der Praxis eingesetzt werden sollen. Die individuelle Prüfung verbleibe „vollständig in der Verantwortung der zuständigen Mitarbeitenden“. Die Digitalisierung solle die Sachbearbeitenden gezielt unterstützen, wodurch „Effizienz, Einheitlichkeit und Qualität der Verfahren nachhaltig gesteigert werden“ können (S. 1).

Hierfür sollen im AsylG und im AufenthG jeweils weitgehend gleichlautende Regelungen aufgenommen werden mit den Überschriften

- Verarbeitung personenbezogener Daten (§ 7 AsylG, § 86 AufenthG),
- Automatisiertes Verfahrensmonitoring (§ 7a AsylG, 90d AufenthG),
- Automatisierter Abgleich mit öffentlich zugänglichen Daten aus dem Internet (§ 7b AsylG, § 90e AufenthG).

2 Generalklauseln zur Datenverarbeitung (§ 7 Abs. 1 AsylG, § 86 Abs. 1 AufenthG)

Bisher ist in den Regelungen § 7 AsylG und § 86 AufenthG in Abs. 1 nur die Erhebung personenbezogener Daten legitimiert. Künftig soll **jede Verarbeitung** erlaubt sein. Es wird in der Begründung fälschlich behauptet, der bisher verwendete Begriff der Erhebung sei ein „Oberbegriff für den Umgang mit personenbezogenen Daten" (S. 14, 15). Tatsächlich beschränkt sich die bisherige Befugnis auf das Beschaffen von Daten.[1] Die Weiterverarbeitung wurde über die Generalklauseln des allgemeinen Datenschutzrechts (vgl. Art. 6 Abs. 1 lit. e DSGVO, z. B. § 3 Abs. 1 HDSIG) erfasst. Der Begriff der „Verarbeitung" ist umfassend (Art. 4 Nr. 2 DSGVO). Die Änderung hat im Ergebnis keine materiell-rechtliche Änderung zur Folge.

Die **berechtigten Stellen** werden beschrieben als „mit der Ausführung dieses Gesetzes betraute Behörden". Dies ist äußerst weit und umfasst „insbesondere die Ausländerbehörden der Länder, das Bundesamt für Migration und Flüchtlinge, das Auswärtige Amt mit den Auslandsvertretungen und dem Bundesamt für Auswärtige Angelegenheiten sowie weitere Behörden, soweit ihnen durch das Aufenthaltsgesetz (bzw. das AsylG) Aufgaben übertragen werden". Die Aufzählung ist nicht abschließend und soll z. B. auch das Bundesverwaltungsamt, die Bundespolizei sowie die Polizeibehörden der Länder (vgl. § 71 AufenthG) einschließen (S. 15).

Die Regelung erlaubt die Verarbeitung von **besonderen Kategorien personenbezogener Daten**, also sensibler bzw. sensitiver Daten. Solche Daten fallen in ausländerrechtlichen und insbesondere in Asyl-Verfahren in großem Umfang an: „Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie … biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person" (Art. 9 Abs. 1 DSGVO).

In Abs. 1 S. 3 wird ein Verweis auf § 22 Abs. 2 BDSG eingefügt. Die Behauptung, dass durch die klarstellende Erwähnung des § 22 Abs. 2 BDSG zum **Schutz der sensitiven Daten** „ein hohes Datenschutzniveau gewahrt bleibt" (S. 15), ist nicht zutreffend. § 22 Abs. 2 BDSG kann allenfalls einen Grundschutz sensibler bzw. sensitiver Daten gewährleisten, der kaum über das Schutzniveau für Personendaten generell hinausgeht.[2] Die Regelung sowie deren Begründung vermitteln den falschen Eindruck, dass damit abschließend der Schutz sensitiver Daten geregelt sei. Dies trifft nicht zu. So gilt für Patientengeheimnisse (§ 203 Abs. 1 Nr. 1 StGB) eine Sonderregelung (§ 88 Abs. 1-3 AufenthG, § 8 Abs. 3 S. 4 AsylG). Sollte bei Flüchtlingen eine besondere Vulnerabilität bestehen, kommen zusätzliche gesetzliche Schutznormen und -pflichten hinzu.[3]

---

[1] Weichert in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, Art. 4 DSGVO Rn. 38.
[2] Weichert DuD 2017, 542 f.
[3] Dazu ausführlich Weichert, Vulnerabilitäts-Screening von Flüchtlingen und Datenschutz, 22.06.2026, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2026_fluchtlings-screening_final.pdf.

3 Entwickeln von automatisierten Anwendungen (KI-Systemen, § 7 Abs. 2 AsylG, § 86 Abs. 2 AufenthG)

Die Gesetzesbegründung geht davon aus, dass der bloße Einsatz von KI-Systemen als solcher keiner eigenständigen gesetzlichen Ermächtigung bedürfe (S. 10). Diese Grundannahme ist für **hoheitliche KI-Einsätze** nicht zutreffend. Das Bundesverfassungsgericht (BVerfG) hat festgestellt, dass die automatisierte Datenanalyse und -auswertung wegen spezifischer Belastungseffekte ein Eigengewicht haben kann, das über das Übliche hinausgeht, weshalb sich aus dem Verhältnismäßigkeitsgrundsatz weitergehende Rechtfertigungsanforderungen ergeben.[4] Das ist hier der Fall. Wesentliche Aspekte bei der Verhältnismäßigkeitsprüfung sind die Eingriffsqualität, die Qualität der Zweckänderung sowie die Belastungseffekte bei der Nutzung der Ergebnisse.[5] Hinsichtlich der Zwecke ist größtmögliche Präzision nötig.[6] Je umfangreicher die eingeführten Datensätze, desto höher ist die Eingriffsintensität.[7] Es ist darauf zu achten, dass es nicht zu diskriminierenden Ergebnissen kommt, deren Nutzung gegen Art. 21 GRCh, Art. 3 Abs. 3 GG verstößt.[8] Es bedarf daher der Fixierung von Garantien, mit denen die Betroffenenrechte gewahrt werden. Dies wird auch im Entwurf zugestanden, der den Anspruch hat, einen verbindlichen datenschutzrechtlichen Rahmen mit Zweckbindung, Transparenz, Verantwortlichkeiten und Schutzmechanismen festzulegen (S. 10).

3.1 Entwicklung von KI-Systemen – Allgemeines

§ 86 Abs. 2 AufenthG sowie § 7 Abs. Abs. 2 AsylG legitimieren die Verarbeitung von Personendaten „zum Entwickeln, insbesondere zum Trainieren, Validieren und Testen von automatisierten Anwendungen zur Datenverarbeitung, wie KI-Systemen im Sinne des Artikel 3 Nummer 1 der Verordnung (EU) 2024/1689 (Verordnung über künstliche Intelligenz)“. Gemäß Art. 3 Abs. 1 der genannten KI-Verordnung (KI-VO) bezeichnet „`System der künstlichen Intelligenz´ (KI-System) eine Software, die mit einer oder mehreren der im Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die von Menschen festgelegt werden, Ergebnisse wie Inhalt, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren“.

Absolut verboten ist gemäß Art. 5 Abs. 1 lit. b KI-VO „das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das eine **Vulnerabilität** oder Schutzbedürftigkeit einer natürlichen Person oder einer bestimmten Gruppe von Personen aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation mit dem Ziel oder der Wirkung **ausnutzt**, das Verhalten dieser Person oder einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu

[4] BVerfG16.02.2023 – 1 BvR 1547/19 u. 1 BvR 2624/20, NJW 2023, 1196, Rn. 54.
[5] BVerfG 16.02.2024 (Fn. 4), Rn. 67.
[6] BVerfG 16.02.2024 (Fn. 4), Rn. 65.
[7] BVerfG 16.02.2024 (Fn. 4), Rn. 78.
[8] BVerfG 16.02.2024 (Fn. 4), Rn. 77.

verändern, die dieser Person oder einer anderen Person erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird“. Diese Grenze ist beim Einsatz von KI im Ausländerbereich, wo es oft um vulnerable Personen geht, in jedem Fall zu beachten.

Der Begriff „**Entwickeln von KI-Systemen**“ erfasst das Trainieren, Validieren und Testen. Als Beispiele führt die Begründung aus, dass dem KI-System u. a. beigebracht werden soll, „unter welchen Voraussetzungen eine aufenthaltsrechtliche Entscheidung (z. B Erteilung eines Aufenthaltstitels) zu treffen ist, welche Angaben die Voraussetzungen erfüllen, wie die Antragstellenden diese Angaben belegen können und wie man diese Belege überprüfen kann. Dabei muss das KI-System auch systemübergreifende Beziehungen oder Zusammenhänge zwischen länderspezifischen Besonderheiten, Personen, Institutionen, Organisationen, Reisezwecken und Erteilungs- bzw. Versagungspraxen verstehen und unbedeutende Informationen und Erkenntnisse ausschließen können“.

Die **Nutzung der Erkenntnisse** aus automatisierten Anwendungen ist in § 90d AufenthG bzw. § 7a AsylG geregelt (s. u. 4).

3.2 Datengrundlage

Datengrundlage für das Entwickeln der KI-Systeme sind die von den jeweiligen Behörden „zum Zweck der Ausführung dieses Gesetzes und ausländerrechtlicher Bestimmungen in anderen Gesetzen erhobenen Daten“. D. h. die Behörden dürfen zum Entwickeln der eigenen KI-Systeme unbegrenzt eigene Daten verwenden. Dies bewegt sich quantitativ bei einzelnen kommunalen Ausländerbehörden in einem noch überschaubaren Rahmen. Bei Landesämtern für Migration ist dies schon anders. Ebenso bei dem Auswärtigen Amt, der Bundespolizei und insbesondere dem Bundesamt für Migration und Flüchtlinge (BAMF). Im BAMF wird § 7 Abs. 2 AsylG wohl zunächst vorrangig zur Anwendung kommen. Einbezogen werden dürfen gemäß der Regelung sämtliche individuellen Asylakten. Dem Erforderlichkeitsgrundsatz (Satz 2) kommt gemäß dem erkennbaren Willen der Entwurfsverfasser nur eine nachgeordnete Bedeutung zu.

Eine Beschränkung der einfließenden Daten ist im Entwurf nicht vorgesehen. Vielmehr wird betont, dass es nicht möglich ist „den **Datenkranz/Gegenstand der Analyse** auf bestimmte Daten zu beschränken“. In der Begründung werden Datenbeispiele genannt, die analysiert, kombiniert und automatisiert bewertet werden sollen: „Daten verschiedener Antragsteller auf Beziehungen untereinander, zu Personengruppierungen wie beispielsweise den Familien der Antragsteller, Institutionen wie Universitäten, von denen Antragsteller möglicherweise Abschlüsse vorlegen, Organisationen wie beispielsweise Unternehmen, von denen Beschäftigungsangebote vorgelegt werden, und Sachen wie zum Beispiel Grundeigentum, das von Antragstellern angeführt werden kann, um die Verwurzelung in einem Herkunftsstaat darzulegen“ (S. 19). Die Notwendigkeit, selbst die Namen der Antragstellenden aufzunehmen wird damit begründet, dass „in vielen ausländischen Staaten … gerade die Namen der Antragsteller aufgrund der aus ihnen erkennbaren Informationen über den soziokulturellen

Kontext wesentliche Informationen (enthalten), die für die genannten Untersuchungsaspekte relevant sind“ (S. 19).

Der Entwurf geht offenbar davon aus, dass regelmäßig die **gesamten verfügbaren Dokumente** aus dem Asyl- bzw. Aufenthaltsverfahren in die KI unverändert eingepflegt werden, wie sich aus folgender Begründungspassage (S. 17) ergibt:

Bestimmte Angabe, wie etwa Namen oder Geburtsdaten, sind nicht lediglich identifizierende Merkmale, sondern enthalten zugleich kontextrelevante Informationen, die für die Plausibilitätsprüfung, die Bewertung der Kohärenz von Angaben und die Einordnung vorgelegter Unterlagen von Bedeutung sein können. So können Vor- und Nachname Auskunft über regionale oder soziale Herkunft und Religionszugehörigkeit geben. Ebenso lässt sich aus dem Geburtsdatum plausibilisieren, ob eine Person das angegebene Alter hat, der angegebene Lebenslauf stimmig ist oder Lichtbilder der antragstellenden Person zugewiesen werden können. Ihre Entfernung oder Entfremdung kann dazu führen, dass typische Muster, Abweichungen oder Unstimmigkeiten nicht mehr zuverlässig erkannt werden. Gleiches gilt für die Verknüpfung verschiedener Angaben innerhalb eines Datensatzes sowie mit begleitenden Dokumenten.

Damit eine automatisierte Anwendung die beabsichtigte Unterstützungsleistung im Einzelfall erbringen kann, muss sie unter Umständen mit solchen Daten entwickelt und trainiert werden, die die tatsächlichen Prüfungsbedingungen realitätsnah abbilden. Eine Entwicklung ausschließlich auf Grundlage stark abstrahierter oder veränderter Daten würde zwar ein im Gegensatz zur Verarbeitung von Echtdaten milderes Mittel darstellen, kann allerdings dazu führen, dass die Anwendung im praktischen Einsatz keine hinreichend belastbaren oder verwertbaren Ergebnisse liefert. In diesen Fällen wäre der mit der Entwicklung verfolgte Zweck nicht erreichbar und die entsprechenden Daten damit nicht gleich geeignet.

Satz 4 stellt klar, dass bei der Entwicklung von KI auch sensitive Daten gemäß Art. 9 Abs. 1 DSGVO verarbeitet werden dürfen. Solche Daten fallen im Rahmen von ausländerrechtlichen und insbesondere von Asyl-Verfahren in großem Umfang an. Davon erfasst sind auch **Patientengeheimnisse**, insbesondere wenn es sich um Daten aus dem Vulnerabilitäts-Screening handelt (s. o. 2).[9] Die Patientengeheimnisse lassen sich bisher in der Praxis in den digitalen Datenbeständen kaum von sonstigen Daten trennen. Das Verhältnis von den § 86 Abs. 2 AufenthG und § 7 Abs. 2 AsylG zu Patientengeheimnissen wird im Entwurf nicht angesprochen. Da § 88 AufenthG, der Patientengeheimnisse schützen soll, nur für Datenübermittlungen gilt und KI-Systeme innerhalb der Behörde entwickelt werden sollen, legitimiert der Entwurf uneingeschränkt die Nutzung von Patientengeheimnissen für die KI-Entwicklung und Nutzung.

Mit der Entwicklung von KI-Systemen ist, wie der Entwurf richtig erkennt (S. 16), eine **Zweckänderung** der personenbezogenen Daten verbunden. Diese sei gerechtfertigt als eine „notwendige und verhältnismäßige Maßnahme zum Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses des Mitgliedstaates“ (S. 16).

[9] Weichert, Vulnerabilitäts-Screening von Flüchtlingen und Datenschutz (Fn. XX), Kap. 5.3 (S. 14 ff.)

Art. 6 Abs. 4 S. 1 i. V. m. Art. 23 Abs. 1 lit. e DSGVO legitimiert diese Zweckänderung, die Verarbeitung sensitiver Daten und die möglichen Folgen der beabsichtigten Weiterverarbeitung aber nur bei einem „Vorhandensein geeigneter Garantien, wozu Verschlüsselung und Pseudonymisierung gehören kann“ (Art. 6 Abs. 4 lit. e DSGVO).

3.3 Technisch-organisatorische Vorkehrungen

Die Behörden haben gemäß S. 3 „die **technischen und organisatorischen Vorkehrungen** zu treffen, die erforderlich sind, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten, insbesondere sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden, sowie eine angemessene Löschfrist festzulegen“.

Als eine technisch-organisatorische Vorkehrung nennt Abs. 2 S. 3 die **Verhinderung diskriminierender Algorithmen**. Art. 21 Grundrechte-Charta (GRCh) verbietet Diskriminierungen insbesondere wegen des Geschlechts, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung. Derartige Merkmale sind in ausländerrechtlich relevanten Dokumenten umfangreich enthalten und finden Eingang in die KI-Analysen. Die Begründung des Entwurfs fordert Diskriminierungswirkungen sicher auszuschließen (S. 17). Mit welchen Maßnahmen dies erreicht werden soll, ist nicht erkennbar. Der Verweis auf Art. 10 Abs. 2 lit. f KI-VO ist wenig hilfreich. Danach sind die bei Training, Validierung und Tests verwendeten Datensätze sorgfältig auf mögliche Verzerrungen („Bias“) hin zu überprüfen. Dies gilt insbesondere für Verzerrungen, „die die Gesundheit und Sicherheit von Personen beeinträchtigen, sich negativ auf die Grundrechte auswirken“. Das Vermeiden von Diskriminierung bei KI-Systemen ist ein hochkomplexer Vorgang, zu dem es bisher nur begrenzte Erfahrungen gibt. Lösungsvorschläge laufen letztlich darauf hinaus im Rahmen von Akzeptanztests unter Einbeziehung außenstehender Einrichtungen regelmäßige Kontrollen durchzuführen.[10] Derartige notwendige Maßnahmen werden von den Entwurfsverfassern nicht erwähnt und sind offenbar auch nicht geplant.

Hinsichtlich der Diskriminierungsrisiken erwartet der Entwurf **positive Auswirkungen,** da „insbesondere die systematische Untersuchung von möglichen Diskriminierungsmustern dazu dienen kann, gleichstellungspolitisch relevante Aspekte in Migrationsverfahren künftig noch besser zu adressieren“ (S. 12 f.). Wer in welcher Form solche systematischen Untersuchungen durchführen soll und kann, wird nicht dargelegt.

Der Entwurf verweist auf Art. 10 Abs. 3 S. 1 KI-VO (S. 17), wonach die KI-Datensätze „relevant, hinreichend repräsentativ, fehlerfrei und vollständig“ sein müssen. Dies entspricht der Anforderung in Art. 5 Abs. 1 lit. d DSGVO an die **Datenrichtigkeit**. Im ausländerrechtlichen Kontext ist diese Anforderung höchst voraussetzungsvoll. So ist bekannt, dass die Richtigkeit

[10] Hilgendorf/Roth-Isigkeit, Die neue Verordnung der EU zur Künstlichen Intelligenz, 2. Aufl. 2025, § 5 Rn. 30 (S. 136).

im Ausländerzentralregister (AZR), die insbesondere auf Datenquellen der Ausländerbehörden basiert, große Defizite aufweist. Die ARZ-Datenquellen sind weitgehend identisch mit denjenigen, die für das Entwickeln der KI genutzt werden sollen. Bei den betroffenen Merkmalen handelt es sich zudem um solche, die oft schnellen Veränderungen unterworfen sind und deshalb nicht mehr aktuell sind.[11]

Als technisch-organisatorische Vorkehrung nennt der Entwurf das Festlegen einer **angemessenen Löschfrist** durch die verantwortliche Behörde. Diese Forderung entspricht dem Grundsatz der Speicherbegrenzung und korrespondiert mit dem datenschutzrechtlichen Anspruch auf Datenlöschung (Art. 5 Abs. 1 lit. e, 17 DSGVO). Der Entwurf erklärt hierzu: „Die Notwendigkeit für die weitere Speicherung der Daten entfällt zum Beispiel grundsätzlich, wenn die Entwicklung des KI-Systems oder KI-Modells abgeschlossen, keine Qualitätssicherung mehr erforderlich ist und keine anderen rechtlichen Verpflichtungen der Löschung entgegenstehen." Damit wird den verantwortlichen Stellen ein großer Ermessensspielraum eröffnet, zumal auch nach langer Zeit eine „Erforderlichkeit" der Datensätze begründet werden kann. Inwieweit überhaupt eine Löschung im Rahmen des Entwickelns von KI möglich ist, da in der KI-Blackbox die individuelle Datensätzen nicht mehr in der Ursprungsform vorliegen,[12] wird im Entwurf nicht thematisiert.

Die DSGVO nennt als eine wesentliche Schutzvorkehrung die Datenminimierung durch **Anonymisierung und Pseudonymisierung** (Art. 25 Abs. 1, 32 Abs. 1 lit. a DSGVO). Diese Maßnahmen werden in der Entwurfsbegründung in einem kursiv gedruckten Klammerzusatz tendenziell verworfen (S. 17):

Zur Prüfung der Notwendigkeit und Erforderlichkeit zählt auch die Prüfung, unter denen eine Verarbeitung von personenbezogenen Echtdaten zum Zwecke der Entwicklung zulässig ist. Demnach dürfen Echtdaten nur dann verwendet werden, wenn eine Anonymisierung oder Pseudonymisierung nicht möglich ist oder nur mit unverhältnismäßigem Aufwand erreicht werden kann und dies zugleich zu einer wesentlichen Beeinträchtigung der Ergebnisqualität führen würde.

Die Unentschiedenheit des Entwurfs hinsichtlich der **Datenminimierung** beim Trainieren von KI erklärt sich zum einen mit der ausdrücklichen Absicht möglichst viele individuellen Merkmale bis hin zu Namen in das System einzuführen (s. o. 3.2). Hinzu kommt der mit einer Datenminimierung verbundene Aufwand, für den keine Ressourcen bereitgestellt werden sollen. Der Entwurf zielt darauf ab selbst bei sensiblen Vorgängen auf eine Anonymisierung zu verzichten.

Diese Annahme wird durch folgende Ausführungen der Begründung bestätigt, die einen engen **Zusammenhang zwischen Entwicklung des KI-Systems und deren Nutzung** als Zielsetzung erklären:

---

[11] BT-Drs. 19/17380, 36.
[12] Zenner/Schwartmann/Hansen in Schwartmann/Keber/Zenner, KI-VO, 2. Aufl. 2024, S. 168 (Rn. 483).

Für die Entwicklung automatisierter Anwendungen zur Unterstützung aufenthaltsrechtlicher Verfahren kann es erforderlich sein, auf nicht anonymisierte oder nicht pseudonymisierte Daten zurückzugreifen. Dies kann insbesondere für Anwendungen gelten, die auf Unterstützung der Prüfung individueller Anträge, etwa auf Erteilung eines Aufenthaltstitels oder eines Visums gerichtet sind. In solchen Konstellationen kann eine Anonymisierung oder Pseudonymisierung dazu führen, dass zentrale inhaltliche Zusammenhänge nicht mehr erkannt oder zutreffend bewertet werden können (S. 17).

Die Entwurfsbegründung zählt **weitere technisch-organisatorische Maßnahmen** auf: „die technische Zugriffsbeschränkung auf eine begrenzte Anzahl von Mitarbeitenden und die besondere Qualifizierung dieser, die technische Trennung von Datenbeständen nach ihren unterschiedlichen Verarbeitungszwecken sowie die Verschleierung von sensiblen Inhalten und die Verhinderung von unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte“ (S. 17 f). Bei diesen Maßnahmen handelt es sich um nach Art. 32 DSGVO selbstverständlich umzusetzende Maßnahmen. Die erwähnte „technische Trennung von Datensätzen“ nach unterschiedlichen Zwecken steht im Widerspruch zum KI-Ansatz Daten zweckübergreifend zusammenzuführen.

4 Automatisiertes Verfahrensmonitoring (Art. 7a AsylG, § 90 AufenthG)

§ 90d AufenthG-E und § 7a AsylG-E sollen jeweils eine gesetzliche Ermächtigungsgrundlage (S. 19) bzw. „eine **ausdrückliche Rechtsgrundlage** für den Einsatz automatisierter Anwendungen zur Datenverarbeitung zum Zwecke der Analyse“ für ein „Verfahrensmonitoring“ in den ausländerbehördlichen Verfahren schaffen (S. 18).

4.1 Personenbezogene Datennutzung

Der Begriff des Monitorings wird dabei sinnentstellend verwendet. Monitoring in seiner ursprünglichen Bedeutung ist „Beobachtung“, nicht „Lenkung“.[13] In der Entwurfsbegründung heißt es: „Die Systeme dienen ausschließlich der Erkenntnisgewinnung für zukünftige Verfahren sowie der **Unterstützung der Sachbearbeitung**. Die rechtliche Würdigung und die abschließende Entscheidung verbleiben uneingeschränkt bei den zuständigen Mitarbeitenden“ (S. 10). Die Norm legitimiert die Nutzung der aus den entwickelten KI-Verfahren erlangten Ergebnisse in konkreten individuellen Verfahren. Der Entwurf geht dabei davon aus, dass es sich bei der Ergebnisnutzung nicht um einen datenschutzrechtlich sensiblen Vorgang handele: „Durch die Entwicklung werden weder Entscheidungen, Empfehlungen oder Prognosen zu individuellen Sachverhalten getroffen, noch Erkenntnisse über einzelne Personen erzeugt, auf deren Grundlage oder unter deren Zuhilfenahme (nachteilige) Auswirkungen für die Betroffenen entstehen können“ (S. 16).

Diese gesetzgeberische Unterstellung entspricht der lange vertretenen Behauptung, es handele sich bei durch Auskunfteien berechneten Bonitätsscores nicht um (sensible)

[13] Duden – Das Fremdwörterbuch, 1997, S. 528.

personenbezogene Daten. Diese Ansicht wird inzwischen nicht mehr vertreten. Ein **Personenbezug** ist gegeben, wenn es sich bei den Angaben zur Beschreibung der Person als Mitglied einer Gruppe um statistische Durchschnitts- oder Wahrscheinlichkeitsdaten handelt.[14] Die entwickelten und von den Sachbearbeitenden verwendeten KI-Systeme sollen auf Basis der Daten des betroffenen Ausländers Empfehlungen erstellen, die der aufenthalts- oder sonstigen ausländerrechtlichen Entscheidung zugrunde gelegt werden. Das Verfahrensmonitoring soll die „Prüfung und Bewertung der Angaben und Nachweise im Einzelfall" erleichtern und damit die „Qualität der Entscheidungen verbessern" (S. 11).

Gemäß Abs. 2 S. 1 ist für das Verfahrensmonitoring vorgesehen, dass „datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Verfahren, Vorgängen, Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen identifiziert und hergestellt werden, sowohl qualitativ als auch quantitativ klassifiziert, strukturell analysiert und visualisiert werden" (Nr. 1) und eine Zuordnung erfolgt (Nr. 2). Damit stellt der Entwurf klar, dass im KI-System der **Personenbeziehbarkeit** eine zentrale Bedeutung beigemessen wird.

In Abs. 2 S. 2 heißt es: „Die Ergebnisse aus dem Verfahrensmonitoring dürfen nicht zur Bewertung oder Prognose des Verhaltens, der Zuverlässigkeit oder sonstiger Eigenschaften einzelner Personen verwendet werden." Diese Regelung steht in einem logischen Widerspruch zur weiter oben zitierten Regelung. Ausländerrechtliche Entscheidungen sind eine **Bewertung des Verhaltens und der Eigenschaft** einer konkreten Person.

4.2 Vorrang der menschlichen Entscheidung?

Gemäß der Begründung wird die **menschliche Entscheidungsverantwortung** in ausländerrechtlichen Verfahren durch die Absätze 3 und 4 sichergestellt (S. 18). Danach wird die Verwendung diskriminierender Algorithmen verboten; der Kernbereichsschutz soll gewährleistet werden (dazu im Detail 4.3). Die Begründung hält einer Überprüfung nicht stand: Die Verwendung bestimmter Algorithmen kann nicht gewährleisten, dass ein Mensch die Letztentscheidung vornimmt. Selbst wenn die Entscheidung nach einer automatisierten Vorlage nochmals auf Kernbereichsbezüge überprüft wird, würde dies nichts daran ändern, dass diese wesentlich automatisiert bestimmt wird.

Es ist erklärtes Ziel des Entwurfes, die Quantität und Qualität der ausländerrechtlichen Entscheidungen **ohne mehr Personal** zu erreichen: „Eine Ausweitung der personellen Kapazitäten scheidet aufgrund der Haushaltslage und des Fachkräftemangels aus" (S. 11).

Es gibt keinen Grund, weshalb im Ausländerbereich bei automatisierten Verfahren eine andere Praxis eintreten wird als im Kreditwesen, wo Bonitätsprüfungen regelmäßig durch digitale Analysen vorgegeben werden. Die Nutzung von KI soll die ausländerrechtlichen

[14] Kamp/Weichert (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein), Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, 2005, S. 66 m. w. N. auch für die damals vertretene Gegenansicht.

Verfahren beschleunigen und die **Sachbearbeitenden entlasten**. Dieser Effekt könnte nicht erreicht werden, wenn die Sachbearbeitenden die KI-Ergebnisse kritisch hinterfragen würden.

Beim automatisierten Verfahrensmonitoring handelt es sich um ein **automatisiertes Entscheidungsverfahren** i. S. v. Art. 22 DSGVO. Der Entwurfsbegründung ist zu entnehmen, dass die KI-Ergebnisse zwar nicht alleinentscheidend, aber maßgeblich sein sollen für die ausländerrechtliche Entscheidungsfindung.[15] Zwar versucht die Entwurfsbegründung dies unter Verweis auf Art. 6 Abs. 3 KI-VO zu relativieren: „Die hierbei eingesetzte automatisierte Anwendung zur Datenverarbeitung ist dazu bestimmt, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen; sie ist nicht dazu bestimmt, eine zuvor abgeschlossene menschliche Bewertung ohne angemessene menschliche Überprüfung zu ersetzen oder zu beeinflussen." Tatsächlich ist die zentrale Aufgabe des KI-Einsatz, dass die Entscheidungsfindung der Sachverarbeitenden „wesentlich beeinflusst" wird und dieser Einsatz „maßgeblich" ist. Art. 22 Abs. 4 DSGVO verlangt in diesen Fällen, dass beim Einsatz von sensitiven Daten (nach Art. 9 Abs. 1 DSGVO) Art. 9 Abs. 2 lit. g DSGVO anzuwenden ist (Verhältnismäßigkeitsprüfung, Wahrung des Wesensgehalts des Datenschutzgrundrechts) und dass „angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen" werden müssen.

Die im Entwurf vorgesehenen KI-Systeme sind „**Hochrisiko-KI-Systeme**" i. S. v. Art. 6 KI-VO. In Anhang III Nr. 7 KI-VO werden solche Systeme, die nach nationalem Recht in den Bereichen „Migration, Asyl und Grenzkontrolle" eingesetzt werden, ausdrücklich aufgeführt. Der Gesetzentwurf enthält keine Regelung, die sicherstellt, dass darüber lediglich ein „Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit" verbessert wird (Art. 6 Abs. 3 lit. b u. c KI-VO).

4.3 Schutzmaßnahmen

Abs. 3 verpflichtet die Behörden zu „grundrechtsschützenden Schranken" (S. 20), konkret dass beim Verhaltensmonitoring keine „**diskriminierenden Algorithmen**" verwendet werden. Damit soll offenbar Art. 21 Abs. 1 GRCh genügt werden (s. o. 3.3). Die in dieser Regelung genannten Diskriminierungsmerkmale sind zentrale Aspekte, die im Rahmen ausländerrechtlicher Entscheidungen relevant sind und daher zwangsläufig in die KI-Systeme einfließen und ausgewertet werden können. Der Entwurf erläutert nicht, wie vermieden werden soll, dass der Algorithmus diese Merkmale nur nichtdiskriminierend auswertet.

Gemäß Abs. 4 soll durch „weitere grundrechtsschützende Schranken" (S. 20) sichergestellt werden, dass keine „Erkenntnisse aus dem **Kernbereich privater Lebensgestaltung**" erlangt und weiterverarbeitet werden. Aufzeichnungen hierzu sollen unverzüglich aktenkundig gelöscht werden. Nach der Rechtsprechung des Bundesverfassungsgerichts werden Sachverhalte dem Kernbereich persönlicher Lebensgestaltung dann zugeordnet, wenn der

[15] EuGH 07.12.2023 – C-634/21, Rn. 48 ff., 73, NJW 2024, 413

Sachverhalt einen höchstpersönlichen Charakter hat und in geringerem Maße die Sphäre anderer oder die Belange der Gemeinschaft berührt.[16] Der Kernbereich umfasst innere Vorgänge wie Empfindungen, Gefühle, Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art.[17] Wenn ein Sachverhalt dem Kernbereich privater Lebensgestaltung angehört, so dürfen der Staat und seine Organe in diesen Bereich unter keinen Umständen eingreifen. Trotz vielfältiger Verwendung des Begriffs ist bis heute unklar, wie dieser einigermaßen zuverlässig zu definieren ist.[18] So unklar es ist, wie im Rahmen der KI-Nutzung ein Kernbereichsschutz umgesetzt werden kann, so ungenügend wäre dieser für die Wahrung des umfassenderen allgemeinen Persönlichkeitsrechts der Betroffenen.

In Abs. 5 werden **europarechtliche Pflichten** aus der DSGVO (Art. 9 DSGVO i. V. m. § 22 BDSG) bzw. der KI-VO bekräftigt (S. 20 f.). Dazu gehört das Risikomanagement gemäß Art. 9 KI-VO, mit dem vor Inverkehrbringen und während des gesamten Lebenszyklus des KI-Systems sichergestellt werden soll, dass etwaige Risiken für Grundrechte, Gesundheit oder Sicherheit – einschließlich solcher durch diskriminierende Ergebnisse – frühzeitig erkannt, minimiert und überwacht werden. Art. 9 Abs. 2 lit. c KI-VO verpflichtet zur fortlaufenden Überwachung der KI-Leistung und zum Umgang mit Abweichungen und Fehlverhalten. Art. 10 Abs. 2 lit. f KI-VO sieht vor, dass bei den für Training, Validierung und Tests verwendeten Datensätzen eine sorgfältige Prüfung auf mögliche Verzerrungen („Bias“) erfolgen muss, die sich negativ auf Grundrechte oder gesetzlich geschützte Merkmale auswirken könnten. Gemäß Art. 10 Abs. 3 S. 1 KI-VO müssen die Datensätze „relevant, hinreichend repräsentativ, fehlerfrei und vollständig“ sein. Art. 13 KI-VO verlangt Maßnahmen zur Transparenz: Hochrisiko-KI-Systeme müssen so gestaltet sein, dass ihre Ausgaben für den Nutzer verständlich sind und dieser die Ergebnisse sachgerecht bewerten kann. Nach Art. 14 KI-VO muss eine menschliche Aufsicht gewährleistet werden, u. a. um diskriminierende Entscheidungen erkennen und korrigieren zu können. Die Aufsichtspersonen müssen angemessen geschult und befugt sein (Art. 14 Abs. 4 KI-VO).

Die o. g. Verpflichtungen werden den **verantwortlichen Behörden** auferlegt (S. 21). Abgesehen von den Bundesbehörden und evtl. den oberen Landesmigrationsbehörden sind die gemäß dem Entwurf berechtigten Stellen (z. B. Polizei, kommunale Ausländerbehörden) nicht ansatzweise mit den Ressourcen ausgestattet, um diesen Anforderungen zu genügen. Diese Verpflichtungen an Auftragsverarbeiter auszulagern (Abs. 6) genügt nicht für die Wahrnehmung der Verantwortlichkeit und setzt zumindest eine gleichwertige Kontrollqualifikation voraus.

Irritierend ist, dass die Gesetzesbegründung davon ausgeht, dass für die Verwaltung „**kein Erfüllungsaufwand**“ entstünde. Mit dem Verfahrensmonitoring könne jede „Stelle für sich entscheiden, ob die erforderlichen Investitionen einen tatsächlichen Vorteil für die eigene behördliche Leistung bietet“ (S. 12). Der Entwurf geht von der weit verbreiteten, aber falschen

[16] BVerfG 14.09.1989 – 2 BvR 1062/87 (Tagebuch), Rn. 29 ff., NJW 1990, 563 ff.
[17] BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99 (akustische Wohnraumüberwachung), Rn. 120, NJW 2004, 999 ff.
[18] Baldus, JZ 2008, 218 ff.

Annahme aus, dass der verstärkte Einsatz von digitaler Technik und KI keine Kosten verursachen würde. Tatsächlich sind mit deren Einsatz hohe Investitions- und Pflegekosten verbunden. Der Einsatz von KI verursacht zudem einen großen ökologischen Fußabdruck,[19] der vom Entwurf geleugnet wird (S. 12).

5 Automatisierter Abgleich mit Internetdaten (§ 7b AsylG, § 90e AufenthG)

Der Entwurf erlaubt in den § 90e AufenthG und § 7b AsylG den **automatisierten Abgleich mit öffentlich zugänglichen Internet-Daten**, soweit bei entscheidungserheblichen Angaben „begründete Zweifel an der Richtigkeit bestehen und der Abgleich zur Aufklärung dieser Zweifel erforderlich ist“. Nach dem Abgleich bedarf es stets einer manuellen Bewertung, Einordnung und gegebenenfalls Verifizierung.

Die Regelung erlaubt den Abruf aus sog. sozialen Medien (S. 22). Von der Begründung nicht erwähnt, aber von der Regelung erfasst ist auch der Einsatz von Internet-Suchmaschinen sowie von dort verfügbaren Chatbots. Bei deren Nutzung werden nicht nur personenbezogene Daten, evtl. auch sensitiver Art (Art. 9 DSGVO) erhoben, abgeglichen und evtl. gespeichert. Vielmehr fallen bei den Internet-Plattformen bzw. -Diensten **personenbezogene Metadaten** an, aus denen diese erkennen können, dass es sich bei den gesuchten Personen um Asylsuchende oder sonstige in Deutschland ausländerrechtlich relevante Personen handelt. Diese Daten landen regelmäßig bei US-Unternehmen, denen ein weitgehendes Monopol bei Social Media, Suchmaschinen und Chatbots zukommt. Für eine solche indirekte Datenübermittlung insbesondere in die USA besteht keine Rechtsgrundlage. Derartige Informationen können im Drittausland aus sicherheitsbehördlicher Sicht hoch relevant sein und zugleich ein gewaltiges Risiko für die Betroffenen darstellen. Schutzvorkehrungen sind insofern nicht vorgesehen.

Gemäß Abs. 2 dürfen bei dem Abgleich keine diskriminierenden Algorithmen verwendet werden. Die Behörden sollen, soweit möglich, technisch sicherstellen, dass bei Abgleichen „Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden“ (Abs. 3 S. 4). Nicht mehr erforderliche Abgleichsergebnisse sind gemäß Abs. 4 unverzüglich zu löschen. Die Ausführungen zu **technisch-organisatorischen Maßnahmen**, zum Diskriminierungsschutz sowie zum Schutz des Kernbereichsprivater Lebensgestaltung beim Entwickeln und Nutzen von KI (s. o. 3.3 u. 4.3) gelten auch für die behördliche Internetrecherche.

6 Betroffenentransparenz

Der Gesetzentwurf weist zwar beiläufig darauf hin, dass die neu geregelten Verfahren transparent sein müssen (S. 11). Er sieht aber **keine einzige Transparenzmaßnahme** vor. Es

[19] Dazu von Brackel, Wie viel Strom frisst die KI? Süddeutsche Zeitung v. 17.06.2026, 14.

handelt sich bei dem Einsatz der Verfahren praktisch umfassend um solche, die für die Betroffenen intransparent deren Daten verarbeiten.

Datenverarbeitung muss „in einer für die betroffene Person **nachvollziehbaren Weise**“ erfolgen (Art. 5 Abs. 1 lit. a DSGVO). Zu diesem Zweck enthalten die Art. 12-15 DSGVO detaillierte Transparenzvorschriften. Wie diese umgesetzt werden sollen, ist im Entwurf nicht ersichtlich. Beabsichtigt eine Behörde, wie beim KI-Einsatz, die im ausländerrechtlichen Verfahren erlangten Daten für einen anderen Zweck weiterzuverarbeiten so hat sie den Betroffenen zu informieren (Art. 13 Abs. 3 DSGVO). Entsprechendes gilt, wenn Daten aus dem Internet – also von Dritten – erhoben werden (Art. 14 DSGVO). Dies gilt nicht, wenn die Betroffenen über die Information verfügen (Art. 13 Abs. 4, 14 Abs. 5 lit. a DSGVO). Hiervon kann nicht ausgegangen werden. Verzichtet werden könnte auf eine direkte Information, wenn Rechtsvorschriften die Verarbeitung vorsehen „und geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person§ ausdrücklich geregelt sind“ (Art. 14 Abs. 5 lit. c DSGVO). Auch dies ist nicht der Fall.

Diese datenschutzrechtlichen Transparenzerfordernisse gelten auch im Rahmen des Entwickelns und Nutzens personenbeziehbarer **KI-Systeme** gemäß der KI-VO. Die KI-Anbieter müssen die Betroffenen über den Betrieb des Systems in einem zugänglichen Format informieren und die Informationspflichten nach den Art. 13, 14 DSGVO umsetzen (ErwGr. 132 S. 3-6 KI-VO).

Für die Betroffenen können Entscheidungen, die auf Grundlage der neuen Regelungen erfolgen, existenzielle Konsequenzen haben. Um sich hiergegen zur Wehr setzen oder zumindest Falschinformationen richtig stellen zu können, benötigen die Ausländer Kenntnis über die Hintergründe dieser Entscheidungen. Allein das Risiko von KI-Halluzinationen macht es unabdingbar, dass die Betroffenen über die Art und Weise der Informationsbeschaffung informiert werden. Durch die Einbindung der Betroffenen können zudem behördliche **Fehlentscheidungen vermieden** werden, die für die Behörden zu einem Arbeitsmehraufwand führen können.

7 Evaluierung?

Eine gesetzliche **Befristung und Evaluierung** ist nicht vorgesehen. Der Entwurf verweist auf ein nicht näher beschriebenes „Evaluierungskonzept der Bundesregierung“ bei dem „das Erreichen der Zwecke der Nutzung der automatisierten Anwendungen, der Schutz der personenbezogenen Daten und die effektive Vermeidung diskriminierender Algorithmen zu überprüfen“ sei. Die Evaluierung habe ab Inbetriebnahme „mindestens alle fünf Jahre zu erfolgen“ (S. 13). Diese in der Begründung aufgeführte Evaluierung ist zumindest im Hinblick auf den Betroffenenschutz unglaubwürdig. Selbst ausländergesetzlich geregelte

Evaluierungen[20] haben bisher die Wahrung der Betroffenenrechte nicht in den Blick genommen, obwohl dies angesichts der Verarbeitungspraxis dringend geboten wäre.[21]

8 Ergebnis

Der Entwurf postuliert, ohne in eine nähere Prüfung einzutreten, dass er „mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen vereinbar“ sei (S. 11). Diesen Anforderungen wird der Entwurf nicht gerecht. Vorgaben der DSGVO wie der KI-VO werden missachtet.

- Die Befugnis zum Einsatz ausländerrechtlicher KI-Systeme wird Stellen erlaubt, die hierfür nicht die rechtlichen Anforderungen erfüllen können.
- Ein spezifischer Schutz sensitiver Daten und insbesondere von Patientengeheimnissen ist entgegen den Vorgaben von Art. 9 DSGVO nicht vorgesehen.
- Das Entwickeln automatisierter Anwendungen wird mit sämtlichen im Ausländerrecht anfallenden personenbezogenen Informationen erlaubt und vorgesehen, wodurch eine Verletzung des Zweckbindungsgrundsatzes und des Verhältnismäßigkeits-grundsatzes vorprogrammiert ist.
- Die Anforderungen der KI-VO an Hochrisikosysteme und der DSGVO an automatisierte Entscheidungen werden ignoriert.
- Es fehlt an wirksamen Vorkehrungen zur Vermeidung von Diskriminierungen, etwa durch verpflichtende externe unabhängige Kontrollverfahren.
- Eine wirksame menschliche Kontrolle von automatisiert generierten Ergebnissen ist nicht gewährleistet.
- Bei der Datenbeschaffung über das Internet werden ohne Schutzmaßnahmen in unzulässiger Weise Betroffenendaten an US-Internetdienste übermittelt.
- Den rechtsstaatlichen Anforderungen an die Datentransparenz und an die Beteiligungsrechte der Betroffenen wird nicht genügt.
- Damit werden auch die vom BVerfG formulierten verfassungsrechtlichen Anforderungen an hoheitliche KI-Systeme ignoriert.

Der Einsatz von Digitalisierung allgemein und von KI speziell im Ausländerrecht bedarf – anders als vom Entwurf vorgesehen – des zusätzlichen Einsatzes von personellen, technischen und letztlich finanziellen Ressourcen. Der Entwurf weigert sich diese Notwendigkeit anzuerkennen.

Dem im Anschreiben genannten Wunsch, Änderungs- und Ergänzungswünsche als konkrete Formulierungsvorschläge zu präsentieren, kann leider nicht entsprochen werden. Das Konzept, das dem Entwurf zugrunde liegt, missachtet grundlegende rechtsstaatliche

[20] Art. 13 Datenaustauschverbesserungsgesetz (DVAG) v. 02.02.2016, BGBl. I S 130; Art. 11 Zweites Datenaustauschverbesserungsgesetz (2. DVAG) v. 04.08.2019, BGBl. I S. 1131.
[21] Weichert in Berlit (Hrsg.), Gemeinschaftskommentar zum Aufenthaltsgesetz (GK-AufenthG), Mai 2022, IX (AZR-Gesetz) – 3 Evaluierung.

Prinzipien. Daher empfiehlt die DVD dringend den Referentenentwurf zurückzuziehen und nicht der Bundesregierung zur Beschlussfassung vorzulegen. Der Entwurf bedarf einer umfassenden Überarbeitung.

Dessen ungeachtet wird nochmals betont, dass das Anliegen einer Beschleunigung und Qualifizierung von ausländerrechtlichen Verfahren durch Digitalisierung von der DVD ausdrücklich geteilt wird. Daher stehen wir für eine konstruktive Beratung gerne zur Verfügung.

Thilo Weichert

Vorstandsmitglied der Deutschen Vereinigung für Datenschutz e. V. (DVD)