

**Stellungnahme der Deutschen Vereinigung für Datenschutz (DVD e. V) und des
Netzwerks Datenschutzexpertise zum
Gesetzentwurf der Bundesregierung**

**Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der
Migrationsverwaltung (KIMVG)**

BR-Drs. 452/26 v. 14.08.2026

Stand 23.09.2026

Thilo Weichert

weichert@netzwerk-datenschutzexpertise.de

weichert@datenschutzverein.de

Waisenhofstraße 41, 24103 Kiel

www.netzwerk-datenschutzexpertise.de

www.datenschutzverein.de

Inhalt

1	Allgemeines	3
2	Generalklausel zur Verarbeitung personenbezogener Daten	4
3	Entwicklung automatisierter Anwendungen	5
4	Automatisiertes Verfahrensmonitoring	10
5	Abgleich mit Internetdaten	14
6	Evaluierung	15
7	Blick ins Ausland	15
8	Ergebnis	17
	Abkürzungen	19

Wenn im folgenden Text Seitenangaben gemacht werden, beziehen diese sich auf den Regierungsentwurf und dessen Begründung in der Bundesratsdrucksache 452/26. In einigen Fällen wird zudem auf die Begründung im Referentenentwurf des Bundesinnenministeriums¹ verwiesen.

Die Deutsche Vereinigung für Datenschutz e. V. (DVD) und das Netzwerk Datenschutzexpertise nehmen zu dem Entwurf der Bundesregierung eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (KIMVG) wie folgt Stellung:

1 Allgemeines

Der Entwurf verfolgt das Ziel, im Asylgesetz (AsylG) und im Aufenthaltsgesetz (AufenthG) datenschutzrechtliche Regelungen so zu ändern, dass künftig zwecks **Modernisierung von Verwaltungsabläufen** und effizienterem Ressourceneinsatz im Ausländerrecht automatisierte Verfahren und insbesondere sog. Künstliche Intelligenz (KI) unter Wahrung der europa- und verfassungsrechtlichen Vorgaben zum Einsatz kommen kann.

Dieses Anliegen ist zu begrüßen.

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. 8).

Die Lösung des Problems soll darin bestehen, dass eine **Rechtsgrundlage zur personenbezogenen Datenverarbeitung** geschaffen wird 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 einzusetzen. 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“ könne (S. 2, 12).

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).

¹ Referentenentwurf des Bundesministeriums des Innern v. 25.06.2026, <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/MI6/kimvg.html>; dazu DVD, Stellungnahme v. 02.07.2026, <https://www.datenschutzverein.de/2026/07/dvd-pm-stellungnahme-zum-referentenentwurf-des-kimvg/>.

Der Entwurf ist nur ein Teil von umfassenderen Bestrebungen zur **Digitalisierung der Migrationsverwaltung** in Deutschland. Erste rechtliche Grundlagen für die Automatisierung und Zentralisierung wurden schon mit dem Ausländerzentralregistergesetz im Jahr 1994 gesetzt. Dieses Gesetz und die damit legitimierte Datenverarbeitung im Ausländerzentralregister (AZR) wurden seitdem weiterentwickelt.² Im Rahmen der GEAS-Gesetzgebung wurden jüngst weitere Regelungen zur verstärkten Digitalisierung von Entscheidungsprozessen im Migrationsbereich in Kraft gesetzt.³ Insbesondere zum Zweck der Identifizierung und zum Abgleich mit Sicherheitsdatenbanken bestehen auf nationaler wie auf europäischer Ebene normativ abgesicherte digitale Prozesse, deren Ergebnisse in die vorliegend im KIMVG geregelten Prozesse einfließen können.⁴ Das Bundesamt für Migration und Flüchtlinge (BAMF) setzt schon heute spezifische automatisierte Anwendungen ein, etwa bei der automatisierten Dialekterkennung, der Inhaltsanalyse von Asylanträgen oder dem Auslesen von Handydaten.⁵

2 Generalklausel zur Verarbeitung personenbezogener Daten

Die geplanten § 7 Abs. 1 AsylG und § 86 Abs. 1 AufenthG sind im Wortlaut weitgehend identisch. Bisher wird in diesen Regelungen die Erhebung personenbezogener Daten durch die Migrationsverwaltung legitimiert. Künftig soll nicht nur die Erhebung, sondern danach jede Form der **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. 11, 21 f.). Tatsächlich beschränkt sich die bisherige Befugnis auf das Beschaffen von Daten.⁶ Die Weiterverarbeitung wurde über die allgemeinen Datenschutzregelungen (Generalklauseln, 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 jedoch keine materiell-rechtlichen Folgen.

Die **berechtigten Stellen** werden beschrieben als „mit der Ausführung dieses Gesetzes betraute Behörden“. Diese Regelung 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 Aufgaben übertragen werden“ (entsprechend im AsylG-E). Die Aufzählung ist nicht abschließend und soll z. B. auch das Bundesverwaltungsamt, die Bundespolizei sowie die Polizeibehörden der Länder (vgl. § 71 AufenthG) einschließen (S. 21).

² Dazu ausführlich Weichert in Berlitz (Hrsg.), Gemeinschaftskommentar zum Aufenthaltsgesetz (GK-AufenthG), Mai 2022, IX (AZR-Gesetz).

³ GEAS-Anpassungsgesetz v. 28.04.2026, BGBl. 2026 I Nr. 111; GEAS-Anpassungsfolgesgesetz v. 28.04.2026, BGBl. 2026 I Nr. 112.

⁴ S. Antworten der Parlamentarischen Staatssekretärin Ludwig v. 07.08.2026, BT-Drs. 21/7509, 13 (Frage 22) sowie v. 05.01.2026, BT-Drs. 21/3520, 18 (Frage 25); Weichert, Flüchtlinge, Datenverarbeitung und Datenschutz, Asylmagazin 9/2025, 288 ff.

⁵ Mrkaja, KI-Einsatz beim BAMF: Teuer, fehleranfällig und selten hilfreich, 16.01.2025, <https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/ki-einsatz-beim-bamf-teuer-fehleranfaellig-und-selten-hilfreich>; Amnesty International, KI und Migration, <https://amnesty-digital.de/ki-und-migration/>.

⁶ Weichert in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 3. Aufl. 2024, Art. 4 DSGVO Rn. 38.

Die Regelung erlaubt die Verarbeitung von **besonderen Kategorien personenbezogener Daten**, also sensibler bzw. sensibler Daten. Solche Daten fallen in ausländerrechtlichen und insbesondere 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 jeweils ein Verweis auf § 22 Abs. 2 BDSG eingefügt. Die Behauptung, dass durch die klarstellende Erwähnung des § 22 Abs. 2 BDSG zum **Schutz der sensiblen Daten** „ein hohes Datenschutzniveau gewahrt bleibt“ (S. 12, 22), ist nicht zutreffend. § 22 Abs. 2 BDSG kann allenfalls einen Grundschutz sensibler bzw. sensibler Daten gewährleisten, dessen Schutzniveau kaum über das sonstiger Personendaten hinausgeht.⁷ Die Regelung sowie deren Begründung vermitteln zudem den falschen Eindruck, dass damit abschließend der Schutz sensibler 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.⁸

3 Entwicklung automatisierter Anwendungen

Die Begründung des Referentenentwurfs ging davon aus, dass der bloße Einsatz von KI-Systemen als solcher keiner **eigenständigen gesetzlichen Ermächtigung** bedürfe (dort S. 10). Diese Grundannahme ist bei einem hoheitlichen Einsatz unzutreffend. Das 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“.⁹ Wesentliche Aspekte bei der Verhältnismäßigkeitsprüfung sind die Eingriffsqualität, die Qualität der Zweckänderung sowie die Belastungseffekte bei der Nutzung der Ergebnisse.¹⁰ Hinsichtlich der Zwecke ist eine größtmögliche Präzision nötig.¹¹ Je umfangreicher die eingeführten Datensätze, desto höher ist die Eingriffsintensität.¹² Es ist darauf zu achten, dass es nicht zu diskriminierenden Ergebnissen kommt, deren Nutzung gegen Art. 21 GRCh bzw. Art. 3 Abs. 3 GG verstößt.¹³ Es bedarf daher der rechtlichen Fixierung von Garantien, mit denen die Betroffenenrechte gewahrt werden. Dies wird auch im Entwurf zugestanden, der den Anspruch hat, „hohe Anforderungen an Datenschutz, Transparenz, Nichtdiskriminierung und den Schutz des Kernbereichs privater Lebensgestaltung“ zu gewährleisten (S. 8).

§ 86 Abs. 2 AufenthG-E sowie § 7 Abs. 2a AsylG-E legitimieren die Verarbeitung von Personendaten „zum Entwickeln, insbesondere zum **Trainieren, Validieren und Testen von automatisierten**

⁷ Weichert DuD 2017, 542 f.

⁸ 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.

⁹ BVerfG 16.02.2023 – 1 BvR 1547/19 u. 1 BvR 2624/20, NJW 2023, 1196, Rn. 54.

¹⁰ BVerfG 16.02.2023 (Fn. 9), Rn. 67.

¹¹ BVerfG 16.02.2023 (Fn. 9), Rn. 65.

¹² BVerfG 16.02.2023 (Fn. 9), Rn. 78.

¹³ BVerfG 16.02.2023 (Fn. 9), Rn. 77.

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“.

Die KI-VO ist seit dem 02.08.2026 **in Kraft** (Art. 113 KI-VO). Die Pflichten für Betreiber und Anbieter von Hochrisiko-KI-Systemen gemäß Art. 6 Abs. 1 KI-VO (s. u. 4) sind vom 02.08.2027 wirksam (Art. 113 lit. c KI-VO). Schon zuvor sind die Maßnahmen zu ergreifen, die für die künftige Geltung der Regelungen nötig sind.

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 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 Migrationsbereich, wo es oft um vulnerable Personen geht, in jedem Fall zu beachten. Der Gesetzentwurf lässt nicht erkennen, dass diese Anforderung der KI-Verordnung bekannt ist, geschweige denn, wie ein Verstoß gegen Art. 5 Abs. 1 lit. b KI-VO verhindert werden soll.

Erfasst von dem Regelungsvorschlag ist das **Entwickeln von KI-Systemen**. Mit dem Begriff mit erfasst sein soll 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“ (S. 22 f., ähnlich S. 12).

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

Datengrundlage für das Entwickeln der KI-Systeme sind die von den jeweiligen Behörden „zum Zwecke der Ausführung dieses Gesetzes“ erfassten Daten (§ 7 Abs. 1 S. 1 AsylG-E, weiter § 86 Abs. 1 S. 1 AufenthG-E, der alle nach „ausländerrechtlichen Bestimmungen“ erfassten Daten einbezieht). D. h. die Behörde darf zum Entwickeln des eigenen KI-Systems nur eigene Daten verwenden. Dies bewegt sich quantitativ bei einzelnen kommunalen Ausländerbehörden in einem noch überschaubaren Rahmen. Bei Landesämtern für Migration ist dies schon anders. Dies gilt erst recht für das Auswärtige Amt, die Bundespolizei und insbesondere das BAMF, bei dem der § 7 Abs. 2 AsylG wohl zunächst vorrangig zur Anwendung kommen wird. Einbezogen werden dürfen gemäß der Regelung auch sämtliche individuellen Asylakten. So ist vorstellbar, dass mit der Regelung alle beim BAMF digital vorhandenen Dokumente mit einem mächtigen Verfahren wie z. B. von Palantir erfasst und einer Auswertung zugeführt werden. Dem Erforderlichkeitsgrundsatz (Abs. 2 bzw. 2a jeweils S. 2) kommt offenbar gemäß Netzwerk Datenschutzexpertise und Deutsche Vereinigung für Datenschutz zum Entwurf eines Gesetzes zum Einsatz Künstlicher Intelligenz in der Migrationsverwaltung

dem Willen der Entwurfsverfasser nur eine nachgeordnete Bedeutung zu. Es werden keine Prüfkriterien für die Erforderlichkeit vorgegeben.

Eine Beschränkung der zum KI-Training genutzten Daten ist im Entwurf nicht vorgesehen. Vielmehr wird betont, dass es nicht möglich ist, „den **Datenkranz/Gegenstand der Analyse** auf bestimmte Daten zu beschränken“ (S. 16, 26). 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. 26, ähnlich S. 16). Die Notwendigkeit, selbst die Namen der Antragsteller 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. 16, 26).

Satz 4 stellt indirekt klar, dass bei der Entwicklung von KI auch sensitive Daten gemäß Art. 9 Abs. 1 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).¹⁴ Die Patientengeheimnisse lassen sich in der Praxis in 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 aber § 88 AufenthG nur für Datenübermittlungen gelten soll und KI-Systeme innerhalb der Behörde entwickelt werden (sollen), legitimiert der Entwurf zunächst uneingeschränkt die Nutzung von Patientengeheimnissen für die KI-Entwicklung.

Gemäß der Begründung ist der Begriff der „**automatisierten Anwendung zur Datenverarbeitung**“ technik- und produktneutral ausgestaltet (S. 14, 24). Der Gesetzgeber geht offenbar davon aus, dass alle regelbasiert oder statistisch arbeitenden datenanalytische Anwendungen erlaubt sein können. So ist es vorstellbar, dass die Migrationsverwaltung Systeme wie die des US-Anbieters Palantir zum Einsatz bringt, so wie dies schon bei der deutschen Polizei teilweise der Fall ist.¹⁵

Mit der Entwicklung von KI-Systemen ist, wie der Entwurf richtig erkennt (S. 13), eine **Zweckänderung** der personenbezogenen Daten verbunden. Er sieht in der Regelung eine „notwendige und verhältnismäßige Maßnahme zum Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses des Mitgliedstaates“ (S. 13). Art. 6 Abs. 4 S. 1 i. V. m. Art. 23 Abs. 1 lit. e DSGVO legitimiert diese Zweckänderung, die Verarbeitung sensibler 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). Diese fehlen (s. u.).

¹⁴ Weichert, Vulnerabilitäts-Screening von Flüchtlingen und Datenschutz (Fn. 8), Kap. 5.3 (S. 14 ff.)

¹⁵ Neuß, Wirklich alternativlos? So setzt die Polizei Palantir ein, 16.01.2026,

<https://www.zdfheute.de/politik/deutschland/palantir-einsatz-polizei-deutschland-alternative-100.html>.

Die Behörden haben gemäß § 7 Abs. 2a AsylG-E sowie § 86 Abs. 2 AufenthG-E, jeweils 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. 2a/2 S. 3 der **Verhinderung diskriminierender Algorithmen**. Wie der Effekt der Diskriminierung sicher auszuschließen ist, wie die Begründung fordert (S. 14, 24), ist nicht erkennbar. Der Verweis auf Art. 10 Abs. 2 lit. f KI-VO ist wenig hilfreich. Danach muss bei dem Training, der Validierung und den Tests der verwendeten Datensätze eine sorgfältige Prüfung auf mögliche Verzerrungen („Bias“) erfolgen, welche die Gesundheit und Sicherheit von Personen beeinträchtigen oder sich negativ auf die Grundrechte auswirken. Diskriminierungseffekte bei KI ergeben sich regelmäßig nicht durch eine bewusste Programmierung, sondern durch das Trainieren mit Daten, aus denen sich solche Effekte ergeben. Ein Verhindern solcher Effekte ist kaum möglich; ein Vermeiden kann nur dadurch erreicht werden, dass regelmäßig eine Prüfung der Trainingsergebnisse erfolgt.¹⁶

Hinsichtlich der Diskriminierungsrisiken erwartet der Entwurf insofern **positive Auswirkungen** „als insbesondere die systematische Untersuchung von möglichen Diskriminierungsmustern dazu dienen kann, gleichstellungspolitisch relevante Aspekte in Migrationsverfahren künftig noch besser zu adressieren“ (S. 10). Dass und wie solche Auswertungen geplant sind, ist dem Entwurf nicht zu entnehmen.

Weiterhin wird auf Art. 10 Abs. 3 S. 1 KI-VO verwiesen (S. 14, 24), wonach die Datensätze „relevant, hinreichend repräsentativ, fehlerfrei und vollständig“ sein müssen. Diese Anforderung an die **Datenrichtigkeit** bekräftigt den entsprechenden Grundsatz in Art. 5 Abs. 1 lit. d DSGVO. Das Problem von KI-Anwendungen besteht darin, dass sie fehleranfällig sind; sog. Halluzinationen sind nicht auszuschließen.¹⁷ Fehler sind im Migrationsbereich wegen den dabei erfolgenden existenziellen Entscheidungen für die Betroffenen unbedingt zu vermeiden.¹⁸

Als weitere technisch-organisatorische Vorkehrung nennt der Entwurf das Festlegen einer **angemessenen Löschfrist**. Auch diese Forderung wird durch die DSGVO mit dem Grundsatz der Speicherbegrenzung und dem Recht auf Datenlöschung (Art. 5 Abs. 1 lit. e, 17 DSGVO) normativ bestätigt. Dass die Angemessenheit der Frist von der verantwortlichen Stelle festzulegen ist und nicht gesetzlich festgelegt wird, eröffnet einen großen Ermessensspielraum, zumal auch nach langer Zeit eine „Erforderlichkeit“ der Datensätze begründet werden kann. Der Entwurf erläutert zur Löschung Folgendes: „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“ (S. 15, 25). Daraus ergibt sich, dass eine Löschung einzelner Datensätze während des Betriebs eines KI-Systems nicht beabsichtigt ist. Inwieweit überhaupt eine Löschung im Rahmen eines KI-Systems möglich ist, wird im Entwurf nicht thematisiert. Bisher sind hierfür keine funktionierenden

¹⁶ Schwartmann/Keber/Köhler/Nägele in Schwartmann/Keber/Zenner, KIVO, 2. Aufl. 2024, S. 122 f.

¹⁷ Wissenschaftliche Dienste, Deutscher Bundestag, Bias und Halluzinationen von KI-Systemen - Kategorien, Ursachen und Minimierungsstrategien, 19.11.2025, WD 5 - 3000 - 082/25.

¹⁸ Mrkaja (Fn. 5), S. 3.

Verfahren ersichtlich. In der KI-Blackbox werden die individuellen Datensätze regelmäßig so aufgelöst, dass keine sicheren Zuordnungen mehr möglich sind.

Die DSGVO nennt als wesentliche Maßnahme zur Datenminimierung die **Anonymisierung und die Pseudonymisierung** (Art. 5 Abs. 1 lit. c i. V. m. Art. 25 Abs. 1, 32 Abs. 1 lit. c DSGVO). Im Referentenentwurf wird zu dieser Maßnahme in einem kursiv gedruckten Klammerzusatz Folgendes ausgeführt (dort 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.“*

Hinsichtlich der „Prüfung individueller Asylanträge“ oder der „**Prüfung individueller Anträge**, etwa auf Erteilung eines Aufenthaltstitels“ heißt es im Gesetzentwurf jetzt: „In solchen Konstellationen kann eine Anonymisierung oder Pseudonymisierung dazu führen, dass zentrale inhaltliche Zusammenhänge nicht mehr erkannt oder zutreffend bewertet werden können“, weshalb es dann nötig sei „auf nicht anonymisierte oder nicht pseudonymisierte Daten zurückzugreifen“ (S. 14, 24).

Die Beliebigkeit des Entwurfs hinsichtlich der Datenminimierung beim Trainieren von KI erklärt sich auch mit dem damit verbundenen **Aufwand**, der vermieden werden soll. Es ist davon auszugehen, dass in der Praxis auch bei sensiblen Vorgängen wegen des Aufwands auf eine Anonymisierung oder Pseudonymisierung verzichtet wird.

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

Bestimmte Angaben, 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 milderer 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 (S. 14, 24).

Als **weitere technisch-organisatorische Maßnahmen** nennt die Entwurfsbegründung „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 „unbemerktter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte“ (S. 14, 24). Bei diesen Maßnahmen handelt es sich um nach Art. 32 DSGVO selbstverständlich umzusetzende Maßnahmen. Die „technische Trennung von Datensätzen“ nach unterschiedlichen Zwecken steht im Widerspruch zum KI-Ansatz, Daten zweckübergreifend zusammenzuführen.

4 Automatisiertes Verfahrensmonitoring

§ 90d AufenthG-E und § 7a AsylG-E sollen eine gesetzliche Ermächtigungsgrundlage (S. 19) bzw. „eine **ausdrückliche Rechtsgrundlage** für den Einsatz automatisierter Anwendungen zur Datenverarbeitung zum Zwecke der Analyse“, d. h. für ein „Verfahrensmonitoring“ in den behördlichen Verfahren schaffen (S. 15, 25).

Der Begriff des Monitorings wird dabei sinnentstellend verwendet. Monitoring in seiner ursprünglichen Bedeutung ist „Beobachtung“, nicht „Lenkung“.¹⁹ In der Gesetzesbegründung 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. 8). Die Norm legitimiert die Nutzung der aus den entwickelten KI-Verfahren erlangten Ergebnisse in konkreten individuellen Verfahren. Der Referentenentwurf ging 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“ (dort S. 16). Diese nicht haltbare Behauptung stellt der Regierungsvorschlag nicht mehr auf. Wohl aber wird folgende Aussage gemacht: „Der nach diesem Gesetzentwurf vorgesehene Einsatz automatisierter Anwendungen ersetzt weder die individuelle Prüfung noch prägt er Entscheidungen verbindlich vor. 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. 8, ähnlich S. 1).

Diese gesetzgeberische Unterstellung entspricht der lange vertretenen Behauptung, durch Wirtschaftsauskunfteien berechnete Bonitätsscores seien nur automatisierte Hilfen, keine Entscheidungsvorgaben für Kreditvergaben. Es handele sich nicht einmal um personenbezogene, sondern um rein statistische 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 statistischen Durchschnitts- oder Wahrscheinlichkeitsdaten handelt.²⁰

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 wird. Das Verfahrensmonitoring soll, so explizit

¹⁹ Duden – Das Fremdwörterbuch, 1997, S. 528.

²⁰ 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.

der Referentenentwurf die „Prüfung und Bewertung der Angaben und Nachweise **im Einzelfall**“ erleichtern und damit die „Qualität der Entscheidungen verbessern“ (dort S. 11).

Gemäß der Begründung soll die **menschliche Entscheidungsverantwortung** durch die Absätze 3 und 4 sichergestellt werden (S. 15, 25). Demgemäß ist die Verwendung diskriminierender Algorithmen verboten und der Kernbereichsschutz soll gewährleistet werden (dazu im Detail weiter unten). Diese Behauptung trifft nicht zu: Die Verwendung bestimmter Algorithmen gewährleistet nicht, dass ein Mensch die Letztentscheidung vornimmt. Selbst, wenn Entscheidungen nach einer automatisierten Vorlage nochmals auf Diskriminierungen und Kernbereichsbezüge überprüft werden, ändert dies nichts daran, dass diese wesentlich automatisiert bestimmt werden.

Hier werden **automatisierte Entscheidungsverfahren** i. S. v. Art. 22 DSGVO geregelt. Der Entwurfsbegründung ist zu entnehmen, dass die KI-Ergebnisse zwar nicht alleinentscheidend, aber maßgeblich sein sollen für die ausländerrechtliche Entscheidungsfindung.²¹ 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“ (S. 15, 25). Tatsächlich ist die zentrale Aufgabe des KI-Einsatzs, dass die Entscheidungsfindung der Sachverarbeitenden „wesentlich beeinflusst“ wird und dieser „maßgeblich“ ist. Art. 22 Abs. 4 DSGVO verlangt in diesen Fällen, dass beim Einsatz von sensiblen Daten nach Art. 9 Abs. 1 DSGVO die einschränkende Regelung des Art. 9 Abs. 2 lit. g DSGVO anzuwenden ist (Verhältnismäßigkeit, Wahrung des Wesensgehalts des Datenschutzgrundrechts) und „angemessene **Maßnahmen zum Schutz der Rechte und Freiheiten** sowie der berechtigten Interessen der betroffenen Person getroffen“ werden müssen. Zudem ist nach Art. 15 Abs. 1 lit. h DSGVO erforderlich, dass den Betroffenen auf Nachfrage „die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der derartigen Verarbeitung für die betroffene Person“ transparent gemacht wird.²² Vorkehrungen hierzu sind dem Entwurf nicht zu entnehmen.

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

Beim Einsatz von Hochrisiko-KI-Systemen muss ein **Risikomanagementsystem** „eingerrichtet, angewandt, dokumentiert und aufrechterhalten“ werden (Art. 9 KI-VO). Die aktuellen Diskussionen über Sicherheitsrisiken beim KI-Einsatz offenbaren einen immer größer werdenden Strauß von durch solche Verfahren möglichen Gefahren. Bei den geregelten Systemen im Bereich der Migrationsverwaltung handelt es sich insbesondere um Gefahren für die individuellen Grundrechte der Migranten, insbesondere deren Rechte auf Privatsphäre, auf Datenschutz, auf Asyl, auf Nichtdiskriminierung und auf Schutz von Familie und Gesundheit (Art. 7, 8, 18, 21, 33 u. 35 GRCh). Die

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

²² EuGH 12.09.2024 – C-203/22, NJW 2025, 1441; dazu Weichert NJW 2025, 1917.

Risiken für diese Grundrechte beim Einsatz der KI werden im Gesetzentwurf überhaupt nicht thematisiert.

Weitere **Pflichten von Betreibern** von Hochrisiko-KI-Systemen sind in Art. 26 KI-VO aufgeführt. Danach sind die „technisch-organisatorischen Maßnahmen“ zu ergreifen, um einen regelkonformen Betrieb zu gewährleisten, wozu gehört: Einsatz von Personen mit erforderlicher „Kompetenz, Ausbildung und Befugnis“ (Abs. 2), Eingabekontrolle, Überwachung und Protokollierung (Abs. 3-6) sowie Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO (Abs. 9).

Als Hochrisiko-KI-Systeme bedürfen die in diesen Verfahren **eingesetzten Produkte** einer **Konformitätsbewertung** (Art. 6 Abs. 1 lit. b KI-VO). Eine solche Konformitätsbewertung (Art 3 Nr. 20 KI-VO) gemäß Art. 40 ff. KI-VO setzt das Durchlaufen eines umfangreichen Verfahrens voraus (Art. 43 Abs. 1 KI-VO). Die Funktion der notifizierten Stelle zur Durchführung der Konformitätsbewertung übernimmt bei Hochrisiko-KI-Systemen von Einwanderungs- und Asylbehörden die zuständige Aufsichts- oder Marktüberwachungsbehörde (Art. 43 Abs 1 UAbs. 3 i. V. m. Art. 74 Abs. 8 KI-VO). Vor einer Inbetriebnahme der geplanten KI-Systeme bedarf es daher einer Bewertung durch die jeweils zuständige Datenschutzaufsicht und nach einer erfolgreichen Bewertung einer CE-Kennzeichnung (Art. 47 f. KI-VO). Voraussetzung für eine erfolgreiche Bewertung ist die umfassende Beachtung der Vorgaben der DSGVO.

Gemäß § 90d AufenthG bzw. § 7a AsylG, jeweils Abs.2 Nr. 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 eine **Personenbeziehbarkeit** relevant bleiben soll.

In Abs. 2 S. 2 heißt es: „Die Ergebnisse aus dem Verfahrensmonitoring dürfen nicht für ein Profiling im Sinne von Artikel 4 Nummer 4 der Datenschutz-Grundverordnung verwendet werden“. Gemäß Art. 4 Nr. 4 DSGVO ist Profiling die automatisierte Bewertung einer Person. § 7a AsylG-E und § 90d AufenthG-E enthalten somit in sich einen logischen Widerspruch: Das geregelte Monitoring zielt auf ausländerrechtliche Entscheidungen ab, bei denen es um eine „**Bewertung**“ des **Verhaltens und der Eigenschaft** einer konkreten Person, also um ein „Profiling“ geht.

Abs. 3 regelt für die Behörden jeweils „grundrechtsschützende Schranken“ (S. 17, 27), konkret dass beim Verhaltensmonitoring keine „**diskriminierenden Algorithmen**“ verwendet werden dürfen. Damit soll offenbar Art. 21 Abs. 1 GRCh und Art. 10 Abs. 2 lit. f KI-VO genügt werden. Art. 21 GRCh verbietet Diskriminierungen „insbesondere wegen des Geschlechts, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung“. Die in dieser Regelung genannten Diskriminierungsmerkmale sind zentrale Aspekte, die im Rahmen ausländerrechtlicher Entscheidungen relevant sind und daher zwangsläufig in die KI-Systeme einfließen. Der Entwurf erläutert nicht, wie vermieden werden soll, dass der Algorithmus diese Merkmale nur nichtdiskriminierend auswertet. Art. 10 KI-VO verpflichtet beim Trainieren, Validieren und Testen von Hochrisiko-KI-Systemen zu Untersuchungen im Hinblick auf verbotene Diskriminierungen. Die Umsetzung dieser Vorgaben durch entsprechende Vorkehrungen ist im Entwurf nicht vorgesehen.

Netzwerk Datenschutzexpertise und Deutsche Vereinigung für Datenschutz zum Entwurf eines Gesetzes zum Einsatz Künstlicher Intelligenz in der Migrationsverwaltung

Gemäß Abs. 4 soll durch „weitere grundrechtsschützende Schranken“ (S. 17, 27) sichergestellt werden, dass „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 diese einen höchstpersönlichen Charakter haben und in geringerem Maße die Sphäre anderer oder die Belange der Gemeinschaft berühren.²³ Er umfasst innere Vorgänge wie Empfindungen, Gefühle, Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art.²⁴ 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.²⁵ Aus der Regelung und der Entwurfsbegründung ist nicht erkennbar, wie der Kernbereichsschutz umgesetzt werden soll.

Durch die Hinzuziehung von KI bei der Entscheidungsfindung in Asyl- und Aufenthaltsverfahren ergibt sich die Notwendigkeit einer nachvollziehbaren und **überprüfbaren Entscheidungsbegründung**. Das Problem von KI-basierten Entscheidungen besteht darin, dass einem Entscheider nicht nachvollziehbar ist, wie die KI zu ihrem Entscheidungsvorschlag gekommen ist. Dies aber muss bei der Entscheidung offengelegt werden, was letztlich nötig ist, damit im Fall eines Rechtsbehelfs das angerufene Gericht in seiner Rechtmäßigkeitsprüfung die Erwägungsgründe nachvollziehen und bewerten kann. Um diesen Anforderungen zu genügen, bedarf es einer Festlegung der Prüfkriterien und einer verständlichen Beschreibung der Funktionsweise des automatisierten Verfahrens.²⁶ Diese Festlegungen sind auch unabdingbar, um datenschutzrechtliche Überprüfungen durch die zuständige Aufsichtsbehörde zu ermöglichen.²⁷

Der Entwurf unterstellt, dass es **keine Alternative** zum „Einsatz einer automatisierten Anwendung“ in der Migrationsverwaltung gäbe: „Eine Ausweitung der personellen Kapazitäten scheidet aufgrund der Haushaltslage und des Fachkräftemangels aus“ (S. 9). Diese pauschale Aussage ersetzt keine ernsthafte Verhältnismäßigkeitsprüfung.

Irritierend ist, dass die Gesetzesbegründung davon ausgeht, dass für die Verwaltung „**kein Erfüllungsaufwand**“ entstünde (S. 2). Mit dem Verfahrensmonitoring könne „jede Stelle für sich entscheiden, ob die erforderlichen Investitionen einen tatsächlichen Vorteil für die eigene behördliche Leistung bietet“ (S. 10). Der Entwurf geht von der weit verbreiteten, aber falschen Annahme aus, dass der verstärkte Einsatz von digitalen Auswertungen und KI keine Kosten verursachen würde. Tatsächlich sind mit deren Entwicklung und Einsatz hohe Investitions- und Pflegekosten verbunden. Es bedarf des Einkaufs lizenzierter Software, der Beschäftigung hochqualifizierter und teurer Spezialisten und der Beschaffung und des Betriebs leistungsfähiger Rechenanlagen. Der Einsatz von KI führt zudem zu einem großen ökologischen Fußabdruck,²⁸ der vom Entwurf geleugnet wird (S. 10).

23 BVerfG 14.09.1989 – 2 BvR 1062/87 (Tagebuch), Rn. 29 ff., NJW 1990, 563 ff.

24 BVerfG 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99 (akustische Wohnraumüberwachung), Rn. 120, NJW 2004, 999 ff.

25 Baldus, JZ 2008, 218 ff.

26 EuGH 21.06.2022 – C-817/19 (PNR), Rn. 211.

27 EuGH 21.06.2022 – C-817/19 Rn. 212.

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

In Abs. 5 werden **europarechtliche Pflichten** aus der DSGVO (Art. 9 DSGVO i. V. m. § 22 BDSG, dazu s. o.) und der KI-VO, die beide direkt gelten, bekräftigt (S. 17 f., 27 f.). Dazu gehört das Risikomanagement gemäß Art. 9 KI-VO, das vor dem Inverkehrbringen und während des gesamten Lebenszyklus des KI-Systems sicherstellen 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).²⁹

Die o. g. Verpflichtungen werden den **verantwortlichen Behörden** auferlegt (S. 17, 27). Abgesehen von den Bundesbehörden und evtl. den obersten Landesausländerbehörden sind die gemäß dem Entwurf berechtigten Stellen (z. B. Landespolizei, kommunale Ausländerbehörden) nicht ansatzweise mit den Ressourcen ausgestattet, um diesen Anforderungen zu genügen. Die Verpflichtungen an Auftragsverarbeiter auszulagern (Abs. 6) genügt nicht für die Wahrnehmung der Verantwortlichkeit und setzt zumindest eine gleichwertige Kontrollqualifikation voraus.

5 Abgleich mit Internetdaten

In den § 90e AufenthG-E und § 7b AsylG-E erlaubt der Entwurf den **automatisierten Abgleich mit öffentlich zugänglichen Internet-Daten**, soweit bei Angaben, die entscheidungserheblich für aufenthaltsrechtliche oder Asyl-Entscheidungen sind, „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 Art. 12-14 DSGVO verlangen, dass die Verarbeitung von personenbezogenen Daten den Betroffenen transparent gemacht wird und zwar in „präziser, transparenter, verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache“ (Art. 12 Abs. 1 S. 1), auch wenn Daten bei Dritten, etwa aus dem Internet, erhoben werden (Art. 14). Dies hat zur Folge, dass für die Betroffenen insofern **Transparenz** hergestellt werden muss, bevor entsprechend erhobene Daten im weiteren Verfahren verwendet werden. Die bisher vorgesehene behördeninterne Verifikation, wie sie in § 7b AsylG-E bzw. § 90e AufenthG-E jeweils in Abs. 1 S. 3 vorgesehen ist, genügt für die gesetzlich geforderte Transparenz nicht. Nur mit ihr kann verhindert werden, dass aus dem Internet erlangte Falschinformationen für ausländerrechtliche Entscheidungen bestimmend werden, die sich für die Betroffenen negativ auswirken.

²⁹ Zu allem genauer s. o.

Die Regelung erlaubt den Abruf aus sog. sozialen Medien (S. 19, 29). 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 sensibler Art (Art. 9 DSGVO) erhoben, abgeglichen und evtl. gespeichert. Es fallen auch bei den Internet-Plattformen **personenbezogene Metadaten** und möglicherweise sogar Inhaltsdaten an, aus denen zu erkennen ist, dass es sich bei den gesuchten Personen um Asylsuchende oder sonstige in Deutschland ausländerrechtlich relevante Personen handelt. Derartige Informationen können in den USA oder in Heimatstaaten 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. Abs. 3 verbietet die Nutzung von Erkenntnissen aus dem **Kernbereich privater Lebensgestaltung** und verpflichtet zur dokumentierten Löschung. Die Behörden sollen soweit möglich, technisch sogar 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**. Ob und wie diesen Anforderungen genügt werden kann, wird im Entwurf nicht thematisiert. Die obigen Ausführungen zu **technisch-organisatorischen Maßnahmen**, zum Diskriminierungsschutz sowie zum Schutz des Kernbereichs privater Lebensgestaltung (unter 3 und 4) sind auf die hier geregelte behördliche Internetrecherche übertragbar.

6 Evaluierung

Eine gesetzliche **Befristung oder Evaluierung** ist nicht vorgesehen. Die Entwurfsbegründung verweist vielmehr auf das „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. 11). Die erwähnte Evaluierung ist zumindest im Hinblick auf den Betroffenenenschutz unglaublich: Selbst gesetzlich geregelte Evaluierungen³⁰ sind insofern schon bisher rechtlich geboten, ohne dass sie sich im Ergebnis auf den Betroffenenenschutz bezogen haben.³¹ Es sind keine Gründe zu erkennen, weshalb sich angesichts der Unverbindlichkeit der Evaluierungsvorgaben in Zukunft hieran etwas ändern sollte.

7 Blick ins Ausland

In **Großbritannien** kommen schon seit vielen Jahren in der Migrationsverwaltung Künstliche Intelligenz und automatisierte Entscheidungsprozesse zur Anwendung.³² Im August 2020 musste das britische Innenministerium nach einer Intervention des Joint Council for Welfare of Immigration (JCWI) den Einsatz eines algorithmisch getriebenen Visaverfahrens zurückziehen, nachdem bekannt wurde, dass das System in diskriminierender Weise die Nationalität von Antragstellenden als Hauptfaktor

30 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.

31 Weichert in Berlitz (Hrsg.), GK-AufenthG (Fn. 2), 3 Evaluierung.

32 Zum Folgenden ausführlich Kapadia, Immigration AI in 2025: What's Actually Changed Since the Streaming Algorithm?, 08.08.2025, <https://www.ein.org.uk/blog/immigration-ai-2025-whats-actually-changed-streaming-algorithm>.

einsetzte.³³ Dies hinderte die Innenverwaltung nicht, automatisierte Entscheidungsfindung weiter voranzutreiben und ein IPIC-System (**Identity and Prioritise Immigration Cases**) einzuführen, das dazu dient, „die Abschiebbarkeit und das Ausmaß der von Einwanderungsdelinquenten ausgehenden Gefahr zu bewerten, die Identifizierung und Priorisierung von Fällen zu automatisieren und Informationen darüber bereitzustellen, wie lange ein Hindernis für die Abschiebung bereits besteht“. IPIC arbeitet mit einer Vielzahl von sensiblen Personendaten, u. a. Angaben zur Biometrie, zur Ethnie, zur Gesundheit, zu Strafverfahren, selbst mit Daten aus GPS-Tracking.³⁴ Digitales Rückgrat der britischen Migrationsdigitalisierung ist das Atlas-Fallbearbeitungssystem, das von um die 30.000 Behördenmitarbeitenden (Stand 2022) genutzt wird. Das System wurde wegen seiner Fehleranfälligkeit, etwa auf Grund von falschen Zuordnungen, Systemmängeln und Falschangaben, kritisiert.³⁵ Dessen ungeachtet ist Atlas die zentrale Datenbasis für IPIC. IPIC schlägt den Sachbearbeitenden Entscheidungen vor. Gemäß öffentlich gewordenen Schulungsunterlagen müssen Entscheider, die von einem IPIC-Vorschlag abweichen wollen, dies schriftlich begründen; soll dem automatisiert erstellten Vorschlag zugestimmt werden, bedarf es keiner weiteren Erklärung. Die Betroffenen werden nicht darüber informiert, dass ihre Daten mit KI verarbeitet werden und eine Entscheidung auf KI basiert. Gemäß Jonah Mendelson der Nichtregierungsorganisation Privacy International besteht keine Möglichkeit, die Funktionsweise und die Bewertungskriterien von IPIC nachzuvollziehen. Fizza Qureshi vom Migrants' Rights Network äußerte Bedenken wegen der rassistischen Voreingenommenheit von IPIC, der Verarbeitung von Gesundheitsdaten und der Überwachungswirkung des Systems. Für Anwälte und Berater erweisen sich die KI-basierten Migrationsentscheidungen als eine große Herausforderung und schwer hinterfragbar.

Auch **in anderen Staaten** werden KI-Anwendungen zur Prüfung von Visums- und Asylanträgen eingesetzt. Einige Länder wie Kanada verwenden Algorithmen zum automatisierten Vorsortieren von Visumanträgen, während die Vereinigten Staaten Risikobewertungsalgorithmen einsetzen, die die Daten der Antragstellenden analysieren, um potenzielle Betrugs- oder Sicherheitsrisiken vorherzusagen. Dabei werden auch Daten verwendet, die aus sozialen Medien stammen. Diese Systeme versprechen zwar Effizienz, werfen jedoch Bedenken hinsichtlich algorithmischer Verzerrungen, ordnungsgemäßer Verfahren und des Rechts auf individuelle Beurteilung auf. Fragen hinsichtlich der Genauigkeit und möglichen Auswirkungen auf Asylentscheidungen sind bisher offengeblieben.³⁶

³³ Home Office says it will abandon its racist visa algorithm – after we sued them, 04.08.2020, <https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them/>.

³⁴ 'AI' tool could influence Home Office immigration decisions, critics say, 11.11.2024, <https://www.theguardian.com/uk-news/2024/nov/11/ai-tool-could-influence-home-office-immigration-decisions-critics-say>.

³⁵ Home Office immigration database errors hit more than 76,000 people, <https://www.theguardian.com/uk-news/2024/mar/14/home-office-immigration-database-errors-hit-more-than-76000-people>.

³⁶ Molnar, Künstliche Intelligenz im Migrationsmanagement, 04.09.2025, <https://www.bpb.de/themen/migration-integration/kurzdossiers/migration-und-sicherheit/570377/kuenstliche-intelligenz-im-migrationsmanagement/>; Mrkaja (Fn. 5) m. w. N.

8 Ergebnis

Der Gesetzentwurf postuliert, ohne in eine nähere Prüfung einzutreten, dass er „mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen vereinbar“ sei (S. 9). Diese Behauptung trifft nicht zu.

- Die Erlaubnisse zur Verarbeitung sensibler Daten gemäß Art. 9 DSGVO in den asyl- und aufenthaltsrechtlichen Generalklauseln in § 7 AsylG und § 86 AufenthG genügen nicht den hohen Schutzanforderungen dieser Daten und stehen im Konflikt mit dem Schutz von Berufsgeheimnissen sowie weiterer spezialgesetzlicher Regelungen.
- Die Zweckbeschreibungen für den Einsatz von Künstlicher Intelligenz (KI) genügen nicht den verfassungsrechtlichen Bestimmtheitsanforderungen.
- Die Einbeziehung sensibler Daten für das Trainieren bzw. Entwickeln von KI ohne konkrete, spezifisch geregelte Schutzvorkehrungen ist unverhältnismäßig.
- Die Einbeziehung sämtlicher in ausländerrechtlichen Verfahren anfallenden Daten ohne Differenzierung nach Relevanz, Sensibilität und Richtigkeit für das Trainieren bzw. Entwickeln von KI und ohne spezifische Vorkehrungen ist unverhältnismäßig.
- Die Regelung zu technisch-organisatorischen Maßnahmen beim Einsatz von KI sind zu unbestimmt.
- Den Zielbestimmungen des Schutzes der Grundrechte, vor Diskriminierung und des Kernbereichs privater Lebensgestaltung fehlt jegliche Operationalisierung.
- Bei der Nutzung der Ergebnisse aus KI-Verfahren werden die Anforderungen an automatisierte Entscheidungen in Art. 22 DSGVO missachtet.
- Es wird nicht gewährleistet, dass automatisierte Entscheidungsvorschläge nicht übernommen werden, ohne dass zuvor eine individuelle menschliche Prüfung erfolgt ist.
- Den Dokumentations- und Transparenzpflichten gegenüber den Betroffenen gemäß der DSGVO wie der KI-VO wird nicht genügt.
- Den Anforderungen an das KI-Management gemäß der KI-VO, wonach eine laufende Risikobewertung und -beobachtung nötig ist, werden nicht operationalisiert.
- Die Nutzung von Daten aus dem Internet und insbesondere aus Social Media ohne Gewährleistung der Transparenz für die Betroffenen und der Richtigkeit und ohne Berücksichtigung der Sensitivität von Daten gemäß Art. 9 DSGVO ist unverhältnismäßig und verstößt gegen die Art. 12-14 DSGVO.
- Durch die Abfrage von Internetdaten durch Ausländer- oder Asylbehörden zu Migranten fallen bei Internetplattformen Metadaten und möglicherweise Inhaltsdaten mit einer hohen Aussagekraft über die Betroffenen an, die sich für diese als äußerst gefährlich erweisen können, wenn sie z. B. in die Hände von Sicherheitsbehörden des Heimatstaates gelangen.

Es besteht der Eindruck, dass der Entwurf eine formale rechtliche Hülle schaffen soll, um den KI-Einsatz in der Migrationsverwaltung zu legitimieren, ohne dass ernsthafte und realistische Bemühungen verfolgt werden, dies grundrechtskonform zu gestalten.

Zudem geht der Entwurf von faktisch falschen Voraussetzungen aus:

- Der Entwurf unterstellt fälschlich, dass das Gesetz keine finanziellen Belastungen für die verantwortlichen Behörden hat.

- Der Entwurf unterstellt fälschlich, dass die tätigen Behörden die nötigen personellen, finanziellen, technischen und kognitiven Ressourcen verfügbar hätten, um ihrer Verantwortung für die Nutzung der neuen Befugnisse gerecht zu werden.
- Der Entwurf unterstellt fälschlich, dass Datensätze in KI-Systemen gemäß den Vorgaben der DSGVO gelöscht bzw. gezielt verändert werden könnten.
- Der Entwurf unterstellt, dass die Umsetzung des Gesetzes ausschließlich positive Wirkungen habe und erwähnt und untersucht nicht ansatzweise, welche negativen Konsequenzen sich für die Betroffenen ergeben können.

Folgende Änderungen im Entwurf sind notwendig:

- Zur Sicherstellung eines datenschutzkonformen Umgangs mit sensiblen Daten (Art. 9 DSGVO) bedarf es einer technisch-organisatorischen und operativen Trennung von Verfahrens- und Strukturdaten einerseits und besonders gesicherten sensiblen Daten, insbesondere solche mit Aussagekraft über die Vulnerabilität der Betroffenen, andererseits.
- Die Befugnis zur Entwicklung von KI-Systemen darf nicht allen gemäß dem AufenthG bzw. AsylG zuständigen Behörden erteilt werden, sondern ausschließlich solchen Stellen, die sich hierfür nach einem festzulegenden Verfahren als qualifiziert erweisen.
- Es ist eine unabhängige hoheitliche Stelle einzurichten, die mit der Prüfung von asyl- und ausländerrechtlichen KI-Verfahren beauftragt wird.
- Vor einem Einsatz von KI-Verfahren müssen diese einer unabhängigen Prüfung durch die Datenschutzaufsicht unterworfen werden, die deren Grundrechtskonformität bescheinigt.³⁷
- Sowohl beim personenbezogenen Einsatz von KI-Verfahren wie auch bei der Nutzung von aus dem Internet erlangten Daten sind die Betroffenen vor einer Entscheidung über die Entscheidungsgrundlagen zu informieren und anzuhören.
- Bei KI-basierten Entscheidungen sind den Betroffenen die wesentlichen Entscheidungskriterien mitzuteilen.³⁸
- Eine regelmäßige Evaluierung der gesetzlichen Regelungen im Hinblick auf ihre Grundrechtsverträglichkeit und Wirksamkeit ist gesetzlich vorzusehen.

³⁷ Nachweise für „Genauigkeit, Robustheit und Cybersicherheit“ gem. Art. 15 KI-VO sind noch im Entwicklungsstadium, dazu Nägele/Steinbrück in Schwartmann/Keber/Zenner (Fn. 16), S. 138 ff.

³⁸ EuGH 12.09.2024 – C-203/22 Rn. 59-62.

Abkürzungen

Abs.	Absatz
Art.	Artikel
AsylG	Asylgesetz
AufenthG	Aufenthaltsgesetz
AZR/G	Ausländerzentralregister/-gesetz
BAMF	Bundesamt für Migration und Flüchtlinge
BDSG	Bundesdatenschutzgesetz
BGBI.	Bundesgesetzblatt
BMI	Bundesministerium des Innern
BR-Drs.	Bundesratsdrucksache
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
d. h.	das heißt
DSGVO	Europäische Datenschutz-Grundverordnung
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVD	Deutsche Vereinigung für Datenschutz
-E	-Entwurf
EuGH	Europäischer Gerichtshof
f/f.	fort-/folgende
Fn.	Fußnote
GEAS	Gemeinsames Europäisches Asylsystem
GG	Grundgesetz
GK-	Gemeinschaftskommentar
GRCh	Europäische Grundrechte-Charta
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
IPIC	Identity and Prioritise Immigration Cases
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
JZ	Juristenzeitung
KIMVG	Gesetz zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung
KI	Künstliche Intelligenz
KI-VO	EU-Gesetz über Künstliche Intelligenz
lit.	Buchstabe
m. w. N.	mit weiteren Nachweisen
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
Rn.	Randnummer
S.	Satz/Seite
s.	siehe
s.o.	siehe oben
StGB	Strafgesetzbuch
s.u.	siehe unten
v.	von
vgl.	vergleiche
z. B.	zum Beispiel