21. Wahlperiode

Deutscher Bundestag
Innenausschuss

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

Schriftliche Stellungnahme

von Eric Töpfer, Deutsches Institut für Menschenrechte vom 23. November 2026

zu dem

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

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

Deutsches Institut
für Menschenrechte

Stellungnahme zum

Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (BT-Drs. 21/8275)

Öffentliche Anhörung des Innenausschusses
des Deutschen Bundestags am 23. November 2026

November 2026

Inhalt

1	**Vorbemerkung**	**3**
2	**Zusammenfassung**	**3**
3	**Einleitung**	**3**
4	**Unbestimmte und unverhältnismäßige Pläne zur Datenverarbeitung**	**5**
5	**Rechtssicheren KI-Einsatz ermöglichen**	**8**
6	**Transparenz und Kontrolle sicherstellen**	**9**

1 Vorbemerkung

Das Deutsche Institut für Menschenrechte (im Folgenden: das Institut) ist die unabhängige Nationale Menschenrechtsinstitution Deutschlands (§ 1 DIMR-Gesetz). Es ist gemäß den Pariser Prinzipien der Vereinten Nationen akkreditiert (A-Status). Zu den Aufgaben des Instituts gehören Politikberatung, Menschenrechtsbildung, Information und Dokumentation, anwendungsorientierte Forschung zu menschenrechtlichen Themen sowie die Zusammenarbeit mit internationalen Organisationen. Es wird vom Deutschen Bundestag finanziert. Das Institut ist mit dem Monitoring der Umsetzung der UN-Behindertenrechtskonvention (UN-BRK) und der UN-Kinderrechtskonvention (UN-KRK) sowie der Berichterstattung zur Umsetzung des Übereinkommens des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (Istanbul-Konvention), der Europaratskonvention gegen Menschenhandel sowie der EU-Richtlinie 2011/36/EU betraut und hat entsprechende Monitoring- und Berichterstattungsstellen eingerichtet. Das Institut ist deutscher Forschungspartner für die Berichterstattung an die Europäische Grundrechteagentur (FRA). Am 12. Juni 2026 wurde dem Institut zudem die Funktion übertragen, als Teil des unabhängigen Monitoring-Mechanismus gemäß Art. 10 Abs. 2 der Verordnung (EU) 2024/1356 und Art. 43 Abs. 4 der Verordnung (EU) 2024/1348 die Einhaltung von Grund- und Menschenrechten beim Screening und den Grenzverfahren im Rahmen des Gemeinsamen Europäischen Asylsystems zu überwachen.

2 Zusammenfassung

Das Institut begrüßt das Ziel des Gesetzentwurfs, migrationsrechtliche Verfahren effizienter, einheitlicher und qualitativ besser zu gestalten. Der vorgeschlagene Weg wird den grund- und menschenrechtlichen Anforderungen jedoch nicht gerecht. Die Befugnisse zur Entwicklung von KI-Systemen und anderen automatisierten Anwendungen sowie zum Verfahrensmonitoring sind nicht hinreichend bestimmt und unverhältnismäßig: Der Kreis der berechtigten Behörden ist unklar, nahezu alle in den Verfahren anfallenden Daten einschließlich besonderer Kategorien personenbezogener Daten dürfen verarbeitet werden, und die zulässigen Anwendungszwecke sind kaum begrenzt, ohne dass ein wirksamer Schutz der Rechte Betroffener gewährleistet wird.

Das Institut empfiehlt daher, die Befugnisse zu präzisieren, insbesondere die Rolle des Verfahrensmonitorings zu klären, und den KI-Einsatz bei der Einzelfallprüfung gesetzlich zu regeln. Außerdem sollten Metriken zur Bias-Erkennung und die Grundrechte-Folgenabschätzung per Rechtsverordnung konkretisiert und eine unabhängige wissenschaftliche Evaluierung gesetzlich verankert werden.

3 Einleitung

Mit dem vorliegenden Gesetzentwurf sollen neben einer Neufassung der Generalklauseln zur Datenverarbeitung in § 7 Abs. 1 AsylG-E und § 86 Abs. 1 AufenthG-E neue Befugnisse zur Weiterverarbeitung personenbezogener Daten, die in asyl- oder aufenthaltsrechtlichen Verfahren erhoben wurden, geschaffen werden. Dabei sind die Befugnisnormen für beide Gesetze nahezu wortgleich formuliert. Im Einzelnen geht es um die Weiterverarbeitung von Daten für

- die Entwicklung von KI-Systemen oder anderen automatisierten Anwendungen zur Datenverarbeitung (§ 7 Abs. 2a AsylG-E und § 86 Abs. 2 AufenthG-E),
- ein automatisiertes Verfahrensmonitoring (§ 7a AsylG-E und § 90d AufenthG-E),
- einen automatisierten Abgleich mit öffentlich zugänglichen Internetdaten (§ 7b AsylG-E und § 90e AufenthG-E).

Der Fokus dieser Stellungnahme sind die Normen für die Entwicklung von KI- und anderen Systemen sowie für das automatisierte Verfahrensmonitoring.

Die Ziele des Entwurfs, die Effizienz, Einheitlichkeit und Qualität migrationsrechtlicher Verfahren zu verbessern, sind zu begrüßen. Sie sind auch im Interesse der Betroffenen. Allerdings ist zu bezweifeln, dass der vorgeschlagene Weg tatsächlich zielführend ist und die Rechte der Betroffenen angemessen geschützt sind.

Die Entwicklung und Nutzung automatisierter Anwendungen zur Datenverarbeitung in der Migrationsverwaltung bedeuten nicht nur Eingriffe in das Grundrecht auf informationelle Selbstbestimmung und Datenschutz. Darüber hinaus betreffen die Entwicklung und Nutzung solcher Anwendungen Menschen, die sich als Schutzsuchende häufig in besonders vulnerablen Situationen befinden (oder die im Ausland erschwerten Zugang zum Recht haben), und sie können erhebliche Auswirkungen auch auf weitere Grund- und Menschenrechte wie das Recht auf Asyl, das Refoulement-Verbot und das Diskriminierungsverbot haben. Angesichts der häufig dokumentierten Fehleranfälligkeit „intelligenter“ Systeme und der bekannten Probleme bei ihrer menschlichen Anwendung (Stichwort „automation bias“)[1] bestehen durch die geplante Ausweitung von Entwicklung und Einsatz solcher Systeme erhebliche Risiken für den Schutz der genannten Rechte.[2] Diese adressiert der Entwurf nicht in angemessener Weise.

Obwohl der Gesetzentwurf den Begriff „künstliche Intelligenz“ (KI) im Titel trägt, ist er bewusst technikoffen gehalten und will neben KI im Sinne von Art. 3 Nr. 1 der Verordnung (EU) 2024/1689 (KI-Verordnung, KI-VO) auch die Datenverarbeitung für andere automatisierte Anwendungen normieren. Die angestrebte Datenverarbeitung fällt zwar grundsätzlich in den Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO). Nicht in jedem Fall sichergestellt ist hingegen, dass die grundrechtsschützenden Vorgaben der KI-Verordnung zur Anwendung kommen, auch wenn sie im Gesetzentwurf mehrfach genannt werden.

Zwar gelten KI-Systeme für den Bereich Migration, Asyl und Grenzkontrolle gemäß Art. 6 Abs. 2 i.V.m. Anhang III Nr. 7 KI-VO in der Regel als Hochrisiko-KI-Systeme. Dies gilt jedoch nicht für herkömmliche regelbasierte Verfahren,[3] die der Gesetzentwurf laut Begründung ausdrücklich mit einschließt.[4] Denn die KI-Verordnung erfasst nur Systeme, die für einen in unterschiedlichem Grad autonomen Betrieb ausgelegt

---

1 Die KI-Verordnung beschreibt den „Automatisierungsbias“ als mögliche Neigung zu einem automatischen oder übermäßigen Vertrauen in die von einem [Hochrisiko-]KI-System hervorgebrachte Ausgabe (Art. 14 Abs. 4 lit. b KI-VO).

2 Siehe etwa UN, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance (10.11.2020): Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement, UN Doc. A/75/590; EU, European Union Agency for Fundamental Rights (2022): Bias in algorithms – artificial intelligence and discrimination. Luxemburg.

3 Laut KI-Verordnung sollte der Begriff „KI-System“ sich „nicht auf Systeme beziehen, die auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen“ (Erwägungsgrund 12 KI-VO).

4 Deutscher Bundestag (30.09.2026): Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung (KI-Migrationsverwaltungsgesetz – KIMVG). Drucksache 21/8275, S. 14 und 23.

sind und aus den erhaltenen Eingaben ableiten, wie Ausgaben erstellt werden.[5] Zudem legt die Begründung zum Entwurf nahe, dass nicht alle vom Gesetz normierten Systeme als „hochriskant“ eingestuft werden sollen. So wird mit Blick auf das automatisierte Verfahrensmonitoring argumentiert, dass dies „nicht dazu bestimmt [sei], eine zuvor abgeschlossene menschliche Bewertung ohne angemessene menschliche Überprüfung zu ersetzen oder zu beeinflussen“, und dazu auf die Ausnahme vom Hochrisiko-Status nach Art. 6 Abs. 3 KI-VO verwiesen.[6]

Zudem gelten die Pflichten für Hochrisiko-KI-Systeme nach Anhang III KI-VO aufgrund der Änderung durch den „Digital Omnibus KI“ erst ab dem 2. Dezember 2027,[7] für Hochrisiko-KI-Systeme von Behörden, die vor diesem Zeitpunkt in Verkehr gebracht oder in Betrieb genommen wurden, sogar erst ab dem 2. August 2030.[8] Damit bestehen sowohl in materiell-rechtlicher als auch in zeitlicher Hinsicht Schutzlücken. Darüber hinaus bedürfen die Vorgaben der KI-Verordnung in vielerlei Hinsicht einer konkreten Operationalisierung, die im vorliegenden Gesetzentwurf nicht enthalten ist.

4 Unbestimmte und unverhältnismäßige Pläne zur Datenverarbeitung

Rechtsvorschriften, mit denen Mitgliedstaaten der EU im öffentlichen Interesse von der Öffnungsklausel nach Art. 6 Abs. 3 DSGVO Gebrauch machen, müssen hinreichend bestimmt geregelt sein und in einem angemessenen Verhältnis zum verfolgten legitimen Zweck stehen.[9] An die Verhältnismäßigkeit einer Befugnis sind umso strengere Anforderungen zu stellen, je intensiver der Grundrechtseingriff ist. Diesen Anforderungen wird der Gesetzentwurf nicht gerecht.

Sowohl die Befugnisse zur Entwicklung von KI-Systemen und anderen automatisierten Anwendungen als auch jene zum Verfahrensmonitoring sollen grundsätzlich für alle Behörden gelten, die mit der Ausführung des Asyl- bzw. Aufenthaltsgesetzes betraut sind.[10] Die Begründung nennt mit Blick auf die aufenthaltsrechtlichen Befugnisse „insbesondere die Ausländerbehörden der Länder, das Bundesamt für Migration und Flüchtlinge, das Auswärtige Amt mit den Auslandsvertretungen und dem Bundesamt für Auswärtige Angelegenheiten“ sowie das Bundesverwaltungsamt, die Bundespolizei und die Polizeibehörden der Länder.[11] Dabei bleibt offen, ob auch die Verfahrensbeteiligung von weiteren Behörden wie dem Bundeskriminalamt[12] und den Nachrichtendiensten von Bund und Ländern[13] eine Aufgabenzuweisung im Sinne einer „funktionale[n] Zuständigkeit“ darstellt, wie sie die Begründung fordert.[14] Zumindest für das Bundesverwaltungsamt, das eine zentrale Rolle bei Datenübermittlungen unter

---

5 Art. 3 Nr. 1 KI-VO.
6 Deutscher Bundestag (30.09.2026), a.a.O., S. 17 und 25.
7 Art. 113 lit. c Ziff. i KI-VO in der Fassung der Verordnung (EU) 2026/1744 vom 08.07.2026.
8 Art. 111 Abs. 2 Satz 2 KI-VO.
9 Vgl. Art. 6 Abs. 3 Satz 4 DSGVO und Art. 52 Abs. 1 Satz 2 der Charta der Grundrechte der Europäischen Union.
10 Im Fall der geplanten Befugnisse im Aufenthaltsgesetz gilt dies auch für die Durchführung ausländerrechtlicher Befugnisse in anderen Gesetzen.
11 Deutscher Bundestag (30.09.2026), a.a.O., S. 22.
12 § 16 AsylG und § 89 AufenthG.
13 § 73 AufenthG.
14 Deutscher Bundestag (30.09.2026), a.a.O., S. 21.

anderem zu Sicherheitszwecken spielt,[15] ohne dass § 71 AufenthG eine „Zuständigkeit“ zuweist, wird davon ausweislich der Begründung offensichtlich ausgegangen.

Der Gesetzentwurf beschränkt die Datenverarbeitung zwar auf Daten, welche die Behörden selbst erhoben haben. Mindestens im Fall größerer Behörden wie dem Bundesamt für Migration und Flüchtlinge (BAMF) oder der Bundespolizei dürfte es dabei um erhebliche Datenmengen gehen, zumal das BAMF als Registerbehörde zuständig für das Führen des Ausländerzentralregisters mit mehreren Millionen Datensätzen ist.[16] Unklar ist zudem, ob Daten, die etwa – siehe oben – für Zwecke der Identitätsfeststellung an das Bundeskriminalamt oder im Rahmen des Sicherheitsabgleichs an Sicherheitsbehörden übermittelt werden und dort zur Erfüllung der gesetzlichen Aufgaben weiterverarbeitet werden dürfen, als „erhoben“ zu werten sind.

Es sollen nahezu alle Daten Betroffener verarbeitet werden dürfen, die in asyl- oder aufenthaltsrechtlichen Verfahren anfallen. Dies beinhaltet auch besondere Kategorien personenbezogener Daten etwa über Religionszugehörigkeit, politische Meinungen oder sexuelle Orientierung, wie sie insbesondere in Asylverfahren regelmäßig erhoben werden. Ausgeschlossen sind laut Begründung lediglich Sozialdaten,[17] und beim Verfahrensmonitoring soll die Verarbeitung biometrischer Daten nur dann zulässig sein, wenn ihre Aussonderung zu aufwändig wäre.[18] Hinzu kommt, dass auch Daten von Unbeteiligten wie Familienangehörigen betroffen sein können, was die Streubreite der Maßnahmen erhöht.[19]

Die **Befugnis zur Entwicklung automatisierter Anwendungen** zielt nach der Begründung vor allem auf Systeme zur Unterstützung von Entscheidungen in Asylverfahren oder bei der Erteilung von Aufenthaltstiteln.[20] Als Beispiele werden Systeme genannt, die trainiert werden zu erkennen, „unter welchen Voraussetzungen eine Entscheidung über einen Asylantrag zu treffen ist, welche Angaben die Voraussetzungen erfüllen, wie die Antragstellenden diese Angaben belegen können und wie man diese Belege überprüfen kann“.[21] Nicht ausgeschlossen scheinen aber auch völlig andere Anwendungsszenarien: etwa die Entwicklung von Systemen zur Prüfung des Risikos, dass Personen sich einer Abschiebung zu entziehen suchen,[22] oder die Weiterentwicklung von Algorithmen zur biometrischen Identifizierung. Begrenzt wird die Befugnis allein dadurch, dass die Anwendungen der Aufgabenerfüllung der zuständigen Stelle dienen müssen und die Datenverarbeitung hierfür erforderlich sein muss.[23]

Auch die **Vorschriften zum Verfahrensmonitoring** sind nicht hinreichend bestimmt. Das Monitoring bezweckt die Analyse von abgeschlossenen Verfahren und der bisherigen Entscheidungspraxis.[24] Dabei soll es ausschließlich der Gewinnung verallgemeinerungsfähiger Erkenntnisse zur Weiterentwicklung, Beschleunigung und

---

15 §§ 72a und 73 AufenthG.
16 § 1 Abs. 1 AZRG.
17 Deutscher Bundestag (30.09.2026), a.a.O., S. 15, 17, 23 und 26.
18 § 7a Abs. 1 Satz 3 und 4 AsylG-E und § 90d Abs. 1 Satz 3 und 4 AufenthG-E.
19 Die Begründung nennt ausdrücklich die Analyse von Beziehungen zu „Personengruppierungen wie beispielsweise den Familien der Antragsteller“; Deutscher Bundestag (30.09.2026), a.a.O., S. 18 und 26.
20 Deutscher Bundestag (30.09.2026), a.a.O., S. 15 und 23.
21 Deutscher Bundestag (30.09.2026), a.a.O., S. 15 und ähnlich für die aufenthaltsrechtliche Befugnis, S. 23.
22 Vgl. für ein solches Anwendungsszenario EU, European Commission (2020): Opportunities and challenges for the use of artificial intelligence in border control, migration and security. Volume 2: addendum. Unter Mitarbeit von Deloitte, S. 74–75. https://op.europa.eu/en/publication-detail/-/publication/69f33ff7-a156-11ea-9d2d-01aa75ed71a1/language-en/format-PDF/source-search (abgerufen am 20.11.2026).
23 § 7 Abs. 2a Satz 2 AsylG-E und § 86 Abs. 2 Satz 2 AufenthG-E.
24 § 7a Abs. 1 AsylG-E und § 90d Abs. 1 AufenthG-E.

Qualitätsverbesserung zukünftiger Verfahren dienen.[25] Zugleich aber sollen diese Erkenntnisse ausweislich der Begründung dann in die „zukünftige Prüfungsintensität der Einzelfallentscheidungen“[26] einfließen. Das setzt jedoch voraus, dass Daten aus laufenden Verfahren mit den Ergebnissen der Analyse abgeschlossener Verfahren in Beziehung gesetzt werden. Würden dabei persönliche Merkmale der Antragstellenden ausgewertet, um die Prüfungsintensität im Einzelfall zu bestimmen, würde es sich um ein Profiling im Sinne von Art. 4 Nr. 4 DSGVO handeln. Gerade dies soll jedoch laut § 7a Abs. 2 Satz 3 AsylG-E und § 90d Abs. 2 Satz 3 AufenthG-E ausgeschlossen sein. Die Begründung ist insoweit widersprüchlich: Denn an anderer Stelle heißt es, dass das Verfahrensmonitoring „nicht unmittelbar der Einzelfallentscheidung dient“.[27] Es bleibt somit unklar, ob es sich beim Verfahrensmonitoring tatsächlich um ein Instrument zur Entwicklung von Analysetools für ein künftiges „Scoring“, um ein Instrument zum „Scoring“ oder gar um selbstlernende Systeme handelt, welche die gewonnenen „Erkenntnisse“ permanent an die Ergebnisse laufender Verfahren anpassen. Unklar ist damit zum einen, ob das Verfahrensmonitoring nicht eigentlich der Entwicklung von automatisierten Anwendungen dient, die durch § 7 Abs. 2a AsylG-E und § 86 Abs. 2 AufenthG-E normiert werden sollen. Zum anderen bleibt offen, auf welcher Rechtsgrundlage eine Datenverarbeitung stattfinden würde, die „Erkenntnisse“ des Verfahrensmonitorings mit künftigen Verfahren in Bezug setzt. Die neuen Generalklauseln für die Datenverarbeitung in § 7 Abs. 1 AsylG-E und § 86 Abs. 1 AufenthG-E tragen dafür jedenfalls nicht.

Sowohl die geplanten Befugnisse zur Entwicklung von KI-Systemen und anderen automatisierten Anwendungen als auch jene zum Verfahrensmonitoring normieren aufgrund des Umfangs und der Komplexität der Datenverarbeitung intensive Grundrechtseingriffe. Hinweise dazu liefert die Rechtsprechung des Bundesverfassungsgerichts zur automatisierten Datenanalyse, in der das Gericht Kriterien für die Bestimmung der Eingriffsintensität entwickelt hat (Art und Umfang der Daten, Einbeziehung Unbeteiligter, Analysemethoden).[28] Alle drei Faktoren sprechen hier für eine hohe Eingriffsintensität: Einbezogen werden nahezu alle Daten aus asyl- und aufenthaltsrechtlichen Verfahren einschließlich besonderer Kategorien personenbezogener Daten, wie sie insbesondere in Asylverfahren regelmäßig anfallen; betroffen sein können auch zahlreiche Menschen, die keinen Anlass für die Verarbeitung gegeben haben; und die Methoden sind nicht begrenzt, sodass auch lernfähige Systeme eingesetzt werden können, bei denen die Verhinderung diskriminierender Algorithmen eine besondere Herausforderung ist.

Aus der Begründung des Gesetzentwurfs wird jedoch nicht ersichtlich, ob die geplanten Befugnisse geeignet und erforderlich sind, um ihren Zweck – eine Beschleunigung und Verbesserung der Qualität von Migrationsverfahren – zu erfüllen. Weder werden die bisherigen Erfahrungen mit Systemen reflektiert noch werden Annahmen über Effizienzgewinne ausgewiesen. Vielmehr heißt es, dass jede Stelle selbst entscheiden könne, ob sich die erforderlichen Investitionen lohnen.[29] Zweifel an der Eignung, die sich daraus ergeben, dass Anwendungen, die aus abgeschlossenen Verfahren lernen, die dort enthaltenen Fehler und Ungleichbehandlungen fortschreiben können („algorithmic bias“), wird lediglich mit der knappen Vorgabe begegnet, dass keine

---

25 § 7a Abs. 2 AsylG-E und § 90d Abs. 2 AufenthG-E.
26 Deutscher Bundestag (30.09.2026), a.a.O., S. 18 und 26.
27 Ebd.
28 Bundesverfassungsgericht (2023), Urteil vom 16.02.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20.
29 Deutscher Bundestag (30.09.2026), a.a.O., S. 13.

diskriminierenden Algorithmen entwickelt oder genutzt werden dürfen. Alternativen zu den neuen Befugnissen hält die Begründung pauschal für nicht tragfähig, insbesondere weil eine Ausweitung der personellen Kapazitäten aus Haushaltsgründen und wegen des Fachkräftemangels ausscheide.[30] Mildere Mittel werden kaum geprüft. So räumt die Begründung zwar ein, dass eine Entwicklung auf Grundlage abstrahierter oder veränderter Daten ein milderes Mittel wäre, verwirft dies aber mit der bloßen Möglichkeit, dass die Ergebnisse dann weniger belastbar sein könnten,[31] ohne diese Annahme für den jeweiligen Anwendungsfall zu belegen.

Obwohl mit der Schwere des Grundrechtseingriffs die Anforderungen steigen, die an die gesetzlichen Schutzvorkehrungen zu stellen sind,[32] setzt der Entwurf auf nicht näher bestimmte technische und organisatorische Vorkehrungen, mit denen insbesondere sichergestellt werden soll, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Besonders problematisch ist dies mit Blick auf die ausdrücklich erwünschte Verarbeitung von besonderen Kategorien personenbezogener Daten und die algorithmische Konstruktion von Gruppen im Rahmen des Verfahrensmonitorings. Das Verbot diskriminierender Algorithmen ist als Ziel zu begrüßen. Der Entwurf regelt aber weder, an welchen Maßstäben Diskriminierung zu messen ist, noch mit welchen Verfahren und durch wen dies überprüft werden soll. Der Verweis darauf, dass für die Verarbeitung besonderer Kategorien personenbezogener Daten § 22 Abs. 2 BDSG gilt, garantiert kein über die allgemeinen Vorgaben hinausgehendes Schutzniveau, da der dortige Katalog mit Maßnahmen zum Schutz Betroffener beispielhaft und nicht abschließend ist, so dass die Entscheidung, welche konkreten Maßnahmen getroffen werden, der Verwaltung überlassen bleibt.

5 Rechtssicheren KI-Einsatz ermöglichen

Ein rechtssicherer Einsatz von automatisierten Anwendungen zur Datenverarbeitung muss normenklar, hinreichend bestimmt und verhältnismäßig geregelt sein. Ziel und Zweck müssen für die Verwaltung und die Betroffenen verständlich sein, die Art der zu verarbeitenden Daten ist zu begrenzen, die Methoden der Datenverarbeitung müssen nachvollziehbar sein und die Maßnahmen zum Schutz der Rechte Betroffener müssen konkret geregelt sein.

Für den vorliegenden Gesetzentwurf ist das Institut der Ansicht,

- dass es einer Präzisierung der Befugnisse zur Entwicklung von automatisierten Anwendungen bedarf, insbesondere mit Blick auf den Kreis befugter Behörden, die zu verarbeitenden Daten – mit Vorrang für anonymisierte oder pseudonymisierte Daten – und den Zweck der Anwendungen,
- dass für das Verfahrensmonitoring geklärt werden muss, in welchem Verhältnis die Verarbeitung von Daten aus abgeschlossenen Verfahren zu ihrer Nutzung für zukünftige Verfahren steht,
- dass es einer eigenen Rechtsgrundlage für den Einsatz von KI oder anderen automatisierten Anwendungen in asyl- und aufenthaltsrechtlichen Verfahren bedarf, soweit deren Ergebnisse in Einzelfallentscheidungen einfließen sollen,

---

30 Deutscher Bundestag (30.09.2026), a.a.O., S. 12.
31 Deutscher Bundestag (30.09.2026), a.a.O., S. 16 und 24.
32 Bundesverfassungsgericht (2023), a.a.O., Rn. 112–113.

- dass wirksame Maßnahmen zum Schutz der Rechte Betroffener definiert werden müssen, etwa angemessene Löschfristen und das Recht, informiert zu werden.

Da eine Anwendbarkeit der KI-Verordnung nicht in jedem Fall gegeben ist, ihre Hochrisiko-Pflichten erst ab dem 2. Dezember 2027 (für Bestandssysteme von Behörden erst ab dem 2. August 2030) gelten und selbst deren Vorgaben der Konkretisierung bedürfen, sollte der Gesetzgeber außerdem bestimmen, dass folgende Punkte in einer Rechtsverordnung zu regeln sind:

- Metriken und Verfahren zur Bestimmung von Verzerrungen (*bias*) bei der Entwicklung und Nutzung von Algorithmen,
- Details für die Durchführung der gemäß Art. 27 KI-VO durchzuführenden Grundrechte-Folgenabschätzung, insbesondere die zwingende Einbeziehung von Expertise im Bereich Diskriminierungsschutz.

6 Transparenz und Kontrolle sicherstellen

Fraglich ist zudem, ob die Aufsicht über die Entwicklung und den Betrieb von Systemen, die als Hochrisiko-KI-Systeme klassifiziert werden, über die erforderliche Expertise verfügt, um auf die besonderen Grundrechtsrisiken zu reagieren, die sich im Feld der Migrationsverwaltung stellen. Eine zentrale Rolle dabei spielen die Marktüberwachungsbehörden, die für die Beobachtung von Hochrisiko-KI-Systemen zuständig sind, nachdem diese in Verkehr gebracht wurden. Die Aufsicht über Hochrisiko-KI-Systeme im Bereich Migration, Asyl und Grenzkontrolle wurde, soweit Bundesbehörden betroffen sind, durch § 2 Abs. 5 i.V.m. § 4 des am 29. Juli 2026 in Kraft getretenen KI-Marktüberwachungs- und Innovationsförderungsgesetzes (KI-MIG) zur Durchführung der KI-Verordnung primär einem neuen Aufsichtsgremium übertragen: der Unabhängigen KI-Marktüberwachungskammer (im Folgenden: UKIM), bestehend aus der Präsidentin oder dem Präsidenten der Bundesnetzagentur und den Vizepräsident*innen, die von einer Geschäftsstelle mit abgeordnetem Personal der Bundesnetzagentur unterstützt werden. Die Marktüberwachung über KI-Systeme von Landesbehörden (hier insbesondere die Ausländerbehörden) obliegt gemäß § 2 Abs. 6 KI-MIG Behörden, die nach Landesrecht zu bestimmen sind, was eine Fragmentierung der Aufsicht zur Folge haben wird.

Die Einrichtung der UKIM weicht vom Regelmodell der KI-VO ab. Denn nach Art. 74 Abs. 8 KI-VO benennen die Mitgliedstaaten für Hochrisiko-KI-Systeme in besonders grundrechtssensiblen Bereichen wie Strafverfolgung und Migrationsverwaltung als Marktüberwachungsbehörden entweder die nach der DSGVO oder der Richtlinie (EU) 2016/680 (JI-Richtlinie) zuständigen Datenschutzaufsichtsbehörden oder eine andere Behörde, die unter den Bedingungen der Art. 41 bis 44 JI-Richtlinie benannt wurde. Die Entscheidung für die neue Struktur der UKIM wurde damit begründet, dass den auf Grundrechtsschutz fokussierenden Datenschutzaufsichtsbehörden die Erfahrung für die Produktregulierung fehle.[33] Insbesondere für den Bereich

[33] Deutscher Bundestag (09.03.2026): Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828. Drucksache 21/4594, S. 24.

Diskriminierungsschutz kann jedoch davon ausgegangen werden, dass die UKIM entsprechende Expertise erst noch aufbauen muss.

Die Datenschutzaufsichtsbehörden sind mit Blick auf neue KI-Systeme der Migrationsverwaltung zuständig für die Prüfung der Rechtmäßigkeit der Datenverarbeitung. Daneben haben sie als für „den Schutz der Grundrechte zuständige Behörden“ gemäß Art. 77 KI-VO das Recht, unter bestimmten Umständen die nach der KI-VO erstellte Dokumentation von Hochrisiko-KI-Systemen von den zuständigen Marktüberwachungsbehörden anzufordern und einzusehen, sofern der Zugang dazu „für die wirksame Ausübung ihrer Aufträge im Rahmen ihrer Befugnisse innerhalb der Grenzen ihrer Hoheitsgewalt notwendig ist“.[34] Sie können außerdem die Durchführung technischer Tests bei der Marktüberwachungsbehörde beantragen (Art. 77 Abs. 1 und 3 KI-VO). Im Vergleich zur Marktaufsicht handelt es sich dabei um schwächere Befugnisse, die sich nicht auf Trainings-, Validierungs- und Testdaten oder gar den Quellcode der Systeme beziehen.[35] Zusätzlich ist die Antidiskriminierungsstelle des Bundes als Stelle nach Art. 77 KI-VO benannt. Aufgrund ihres im Wesentlichen auf den Anwendungsbereich des Allgemeinen Gleichbehandlungsgesetzes begrenzten Mandats hat sie jedoch keine Befugnisse gegenüber der Migrationsverwaltung.

Ferner ist das Institut Teil der Aufsichtsarchitektur zum Schutz der Grundrechte in der Migrationsverwaltung: Als Teil des unabhängigen Monitoring-Mechanismus nach Art. 10 Abs. 2 der Verordnung (EU) 2024/1356 und Art. 43 Abs. 4 der Verordnung (EU) 2024/1348 hat es seit dem 12. Juni 2026 die Funktion, die Einhaltung der Grund- und Menschenrechte im Screening und im Asylgrenzverfahren zu überwachen. Dafür hat es Besuchsrechte in den Einrichtungen für das Screening und die Asylgrenzverfahren und kann Dokumente von den zuständigen Behörden anfordern und einsehen.

Die Aufsicht über den Betrieb von Hochrisiko-KI-Systemen in der Migrationsverwaltung liegt somit, soweit Bundesbehörden betroffen sind, primär in den Händen der UKIM, die Expertise für die grundrechtlichen Risiken des KI-Einsatzes in der Migrationsverwaltung erst aufbauen muss; für die Ausländerbehörden der Länder sind die nach Landesrecht bestimmten Behörden zuständig.[36] Die Datenschutzaufsichtsbehörden könnten Diskriminierungsrisiken im Rahmen der vorherigen Konsultation nach einer Datenschutz-Folgenabschätzung (Art. 36 DSGVO) oder bei der Aufsicht über automatisierte Entscheidungen im Einzelfall (Art. 22 DSGVO) adressieren. Art. 22 DSGVO erfasst jedoch grundsätzlich nur Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung beruhen, und damit nicht ohne Weiteres Systeme, die menschliche Entscheidungen unterstützen.[37]

Zur Verstärkung der Kontrolle von KI-Systemen in der Migrationsverwaltung empfiehlt das Institut, folgende Punkte gesetzlich zu regeln:

- regelmäßige parlamentarische Berichtspflichten über die Umsetzung des Gesetzes, die quantitativ und qualitativ Auskunft über die Entwicklung und Nutzung von

---

34 Art. 77 Abs. 1 Satz 1 KI-VO.
35 Vgl. Art. 74 Abs. 12 und 13 KI-VO.
36 § 2 Abs. 6 KI-MIG.
37 Nach der Rechtsprechung des Europäischen Gerichtshofs kann allerdings bereits ein automatisiert ermittelter Wahrscheinlichkeitswert eine Entscheidung im Sinne von Art. 22 Abs. 1 DSGVO sein, wenn er für die nachfolgende Entscheidung maßgeblich ist; siehe Europäischer Gerichtshof (2023): SCHUFA Holding, Urteil vom 07.12.2023, Rs. C-634/21.

automatisierten Anwendungen zur Datenverarbeitung in der Migrationsverwaltung von Bund und Ländern geben,
- die Durchführung einer unabhängigen Evaluierung nach wissenschaftlichen Standards sowie deren Veröffentlichung.[38]

Darüber hinaus könnte es sich anbieten, das Deutsche Institut für Menschenrechte, dem zum 12. Juni 2026 gemeinsam mit der Nationalen Stelle zur Verhütung von Folter die Funktion des unabhängigen Mechanismus zum Monitoring der Grundrechtssituation in den Screening- und Außengrenzverfahren übertragen wurde, als Stelle nach Art. 77 KI-VO durch die Bundesregierung zu benennen. Damit würde das Institut zusätzlich die Möglichkeit erhalten, technische Tests bei der Marktüberwachung anzuregen und wäre von dieser bei Grundrechtsrisiken und schwerwiegenden Vorfällen zu informieren.

Impressum

Deutsches Institut für Menschenrechte
Zimmerstraße 26/27
10969 Berlin
Tel.: 030 25 93 59-0
info@institut-fuer-menschenrechte.de
www.institut-fuer-menschenrechte.de

Das Institut auf Social Media:
www.institut-fuer-menschenrechte.de/socialmedia

KONTAKT: Eric Töpfer

LIZENZ: Creative Commons (CC BY-NC-ND 4.0)
https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de

November 2026

Deutsches Institut für Menschenrechte

Das Deutsche Institut für Menschenrechte ist die unabhängige Nationale Menschenrechtsinstitution Deutschlands (§ 1 DIMR-Gesetz). Es ist gemäß den Pariser Prinzipien der Vereinten Nationen akkreditiert (A-Status). Zu den Aufgaben des Instituts gehören Politikberatung, Menschenrechtsbildung, Information und Dokumentation, anwendungsorientierte Forschung zu Menschenrechten und deren Umsetzung in und durch Deutschland sowie die Zusammenarbeit mit internationalen Organisationen. Es wird vom Deutschen Bundestag finanziert. Das Institut ist darüber hinaus mit dem Monitoring der Umsetzung der UN-Behindertenrechtskonvention und der UN-Kinderrechtskonvention betraut worden sowie mit der Berichterstattung zu den Konventionen des Europarats zu Menschenhandel und zu Gewalt gegen Frauen und häuslicher Gewalt. Seit 2026 erfüllt das Institut zudem das Mandat des Monitoring-Mechanismus im Rahmen des Gemeinsamen Europäischen Asylsystems (GEAS) in Deutschland, gemeinsam mit der Nationalen Stelle zur Verhütung von Folter.

[38] Die Begründung sieht lediglich eine Evaluierung nach dem Evaluierungskonzept der Bundesregierung vor, die sich auf eine Untersuchung durch die Migrationsbehörden selbst und auf Kontrollberichte der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit stützen soll; Deutscher Bundestag (30.09.2026), a.a.O., S. 13. Eine gesetzliche Verankerung fehlt.