Deutscher Bundestag **Drucksache 21/8275**

21. Wahlperiode 30.09.2026

Gesetzentwurf

der Bundesregierung

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

A. Problem und Ziel

Die Migrationsverwaltung sieht sich seit Jahren einem stetig steigenden Antragsaufkommen gegenüber. Die vorhandenen personellen und organisatorischen Kapazitäten reichen vielerorts nicht aus, 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. Ohne strukturelle Anpassungen ist angesichts begrenzter Ressourcen und weiter steigender Antragseingänge eine zusätzliche Belastung der Verfahren absehbar.

Ziel des Gesetzes ist es, einen rechtssicheren und datenschutzkonformen Rahmen zu schaffen, um durch den Einsatz digitaler Verfahren – insbesondere Künstlicher Intelligenz – die Effizienz, Einheitlichkeit, Qualität und Sicherheit der Migrations-, Visum- und Asylbearbeitung zu erhöhen. Die Digitalisierung soll Verwaltungsabläufe beschleunigen, Ressourcen zielgerichteter nutzbar machen und eine systematische Auswertung der Praxis ermöglichen.

B. Lösung

Der Gesetzentwurf soll die zuständigen Behörden dazu befähigen, personenbezogene Daten rechtssicher zu verarbeiten, um KI-Systeme oder andere automatisierte Anwendungen zur Datenverarbeitung zu entwickeln, insbesondere zu trainieren, zu validieren und zu testen. Zugleich werden die rechtlichen Grundlagen für den Einsatz spezifischer automatisierter Verfahren geschaffen. Dazu zählen das Verfahrensmonitoring, das der Beobachtung und Auswertung von Verfahren zur Gewinnung verallgemeinerungsfähiger Erkenntnisse über Abläufe und Entscheidungsmuster dient, sowie der automatisierte Abgleich öffentlich zugänglicher Internetdaten zur Verifizierung entscheidungserheblicher Antragsangaben.

Die individuelle Prüfung und Entscheidung bleiben dabei vollständig in der Verantwortung der zuständigen Mitarbeitenden. Automatisierte Verfahren ersetzen weder die rechtliche Würdigung noch prägen sie Entscheidungen verbindlich vor. Die automatisierte Anwendung zur Datenverarbeitung dient vielmehr dazu, Sachbearbeitende gezielt zu unterstützen – etwa indem sie mit Hilfe der Anwendung

widersprüchliche, unvollständige oder ungewöhnliche Angaben überprüfen können. Gleichzeitig ermöglicht das Verfahrensmonitoring, strukturelle Muster, Beschleunigungspotenziale und Optimierungsbedarfe zu erkennen und gezielt zu fördern. Dadurch können Effizienz, Einheitlichkeit und Qualität der Verfahren nachhaltig gesteigert werden.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Es entstehen keine Ausgaben ohne Erfüllungsaufwand.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht kein Erfüllungsaufwand.

E.3 Erfüllungsaufwand der Verwaltung

Für die Verwaltung entsteht kein Erfüllungsaufwand.

F. Weitere Kosten

Weitere Kosten entstehen nicht. Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

BUNDESREPUBLIK DEUTSCHLAND
DER BUNDESKANZLER

Berlin, 30. September 2026

An die
Präsidentin des
Deutschen Bundestages
Frau Julia Klöckner
Platz der Republik 1
11011 Berlin

Sehr geehrte Frau Bundestagspräsidentin,

hiermit übersende ich den von der Bundesregierung beschlossenen

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

mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium des Innern.

Der Bundesrat hat in seiner 1068. Sitzung am 25. September 2026 gemäß Artikel 76 Absatz 2 des Grundgesetzes beschlossen, zu dem Gesetzentwurf wie aus Anlage 2 ersichtlich Stellung zu nehmen.

Die Auffassung der Bundesregierung zu der Stellungnahme des Bundesrates ist in der als Anlage 3 beigefügten Gegenäußerung dargelegt.

Mit freundlichen Grüßen

Friedrich Merz

Anlage 1

Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung

(KI-Migrationsverwaltungsgesetz – KIMVG)

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Asylgesetzes

Das Asylgesetz in der Fassung der Bekanntmachung vom 2. September 2008 (BGBl. I S. 1798), das zuletzt durch Artikel 7 des Gesetzes vom 3. Juli 2026 (BGBl. 2026 I Nr. 199) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 7 durch die folgende Angabe ersetzt:

   „§ 7 Verarbeitung personenbezogener Daten

   § 7a Automatisiertes Verfahrensmonitoring in Asylverfahren

   § 7b Automatisierter Abgleich mit öffentlich zugänglichen Daten aus dem Internet“.

2. § 7 wird wie folgt geändert:

   a) In der Überschrift wird die Angabe „Erhebung personenbezogener Daten“ durch die Angabe „Verarbeitung personenbezogener Daten“ ersetzt.

   b) Absatz 1 wird durch den folgenden Absatz 1 ersetzt:

   „(1) Die mit der Ausführung dieses Gesetzes betrauten Behörden dürfen zum Zwecke der Ausführung dieses Gesetzes personenbezogene Daten verarbeiten, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Personenbezogene Daten, deren Verarbeitung nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) untersagt ist, dürfen verarbeitet werden, soweit dies im Einzelfall zur Aufgabenerfüllung erforderlich ist; § 22 Absatz 2 des Bundesdatenschutzgesetzes gilt entsprechend.“

   c) Nach Absatz 2 wird der folgende Absatz 2a eingefügt:

   „(2a) Die mit der Ausführung dieses Gesetzes betrauten Behörden dürfen die von ihnen zum Zwecke der Ausführung dieses Gesetzes erhobenen personenbezogenen Daten auch zum Entwickeln, insbesondere zum Trainieren, Validieren und Testen von KI-Systemen im Sinne des Artikels 3 Nummer 1 der Verordnung (EU) 2024/1689 (Verordnung über künstliche Intelligenz) oder anderen automatisierten Anwendungen zur Datenverarbeitung verarbeiten. Die Verarbeitung nach Satz 1 ist nur zulässig, soweit die Anwendungen der Aufgabenerfüllung der zuständigen Stelle dienen und die Verarbeitung der Daten für die Entwicklung erforderlich ist. Die Behörden nach Satz 1 haben 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 festzule-

gen. Soweit Daten nach Artikel 9 Absatz 1 der Datenschutz-Grundverordnung verarbeitet werden, gilt § 22 Absatz 2 des Bundesdatenschutzgesetzes entsprechend.“

3. Nach § 7 werden die folgenden §§ 7a und 7b eingefügt:

„§ 7a

Automatisiertes Verfahrensmonitoring in Asylverfahren

(1) Die mit der Ausführung dieses Gesetzes betrauten Behörden können die von ihnen erhobenen personenbezogenen Daten nach Maßgabe der folgenden Absätze mittels einer automatisierten Anwendung zur Datenverarbeitung zum Zwecke der Analyse des Ablaufs abgeschlossener Asylverfahren und der bisherigen Praxis der Entscheidungen über Asylanträge (Verfahrensmonitoring) weiterverarbeiten. Die Weiterverarbeitung nach Satz 1 ist nur zulässig, soweit die Daten hierfür erforderlich sind. Biometrische Daten sind von der Weiterverarbeitung ausgeschlossen. Abweichend von Satz 3 ist eine Weiterverarbeitung zulässig, soweit eine vorherige Aussonderung technisch unmöglich ist oder unverhältnismäßig hohen technischen Aufwand erfordert.

(2) Das Verfahrensmonitoring dient ausschließlich der Gewinnung verallgemeinerungsfähiger Erkenntnisse, um die Verfahren weiterzuentwickeln, zu beschleunigen und die Qualität künftiger Entscheidungen zu verbessern. Im Rahmen des Verfahrensmonitorings können

1. 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,
2. die eingehenden bedeutenden Erkenntnisse relevanten Sachverhalten zugeordnet sowie unbedeutende Informationen und Erkenntnisse ausgeschlossen werden,
3. Suchkriterien gewichtet werden, insbesondere nach Sachnähe, Aktualität und Erheblichkeit der Verknüpfung mit anderen Informationen bezogen auf den Zweck des Verfahrensmonitorings nach Absatz 1, gewichtet werden, sowie
4. gespeicherte Daten statistisch ausgewertet werden.

Die Ergebnisse aus dem Verfahrensmonitoring dürfen nicht für ein Profiling im Sinne von Artikel 4 Nummer 4 der Datenschutz-Grundverordnung verwendet werden.

(3) Die mit der Ausführung dieses Gesetzes betrauten Behörden haben bei der Weiterverarbeitung nach Absatz 1 sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden.

(4) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Weiterverarbeitung nach Absatz 1 ausschließlich Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, so ist die Weiterverarbeitung unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch die Weiterverarbeitung erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.

(5) Die mit der Ausführung dieses Gesetzes betrauten Behörden haben bei der Weiterverarbeitung nach Absatz 1 sicherzustellen, dass das für die Durchführung des Verfahrensmonitorings eingesetzte Personal besonders geschult wird. Sie haben die erforderlichen technischen und organisatorischen Vorkehrungen, insbesondere zum Schutz der Daten gegen unbefugte Kenntnisnahme zu treffen. Sofern Daten im Sinne des Artikels 9 Absatz 1 der Datenschutz-Grundverordnung verarbeitet werden, gilt § 22 Absatz 2 des Bundesdatenschutzgesetzes entsprechend.

(6) Soweit zum Einsatz der automatisierten Anwendung zur Datenverarbeitung Dritte im Wege der Auftragsverarbeitung für die zuständigen Behörden tätig werden, so müssen sie ihren Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten an diese Dritten ist nur innerhalb der Europäischen Union, zuzüglich der Schengen-assoziierten Staaten, zuläs-

sig. Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 1 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Die Weiterverarbeitung von personenbezogenen Daten durch diese Dritten ist unzulässig.

§ 7b

Automatisierter Abgleich mit öffentlich zugänglichen Daten aus dem Internet

(1) Das Bundesamt kann im Einzelfall öffentlich zugängliche personenbezogene Daten aus dem Internet mit entscheidungserheblichen Angaben aus dem Asylantrag mittels einer automatisierten Anwendung zur Datenverarbeitung abgleichen, soweit bei diesen einzelnen entscheidungserheblichen Angaben auf Grund tatsächlicher Anhaltspunkte begründete Zweifel an der Richtigkeit bestehen und der Abgleich zur Aufklärung dieser Zweifel erforderlich ist. Biometrische Daten sind von dem Abgleich ausgeschlossen. Die Ergebnisse des Abgleichs müssen stets durch das Bundesamt manuell bewertet, eingeordnet und gegebenenfalls verifiziert werden.

(2) Das Bundesamt hat bei dem Abgleich nach Absatz 1 sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden.

(3) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch einen Abgleich nach Absatz 1 ausschließlich Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, so ist der Abgleich unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch den Abgleich erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen. Das Bundesamt hat, soweit möglich, technisch sicherzustellen, dass bei Abgleichen nach Absatz 1 Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.

(4) Die im Rahmen des Abgleichs nach Absatz 1 erhobenen Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, sobald sie nicht mehr erforderlich sind. Die Weiterverarbeitung der beim Abgleich erhobenen Daten zu anderen Zwecken ist unzulässig. Der Abgleich, das Ergebnis des Abgleichs und das Löschen der Daten sind zu dokumentieren.

(5) Im Übrigen gilt § 7a Absatz 5 und 6 entsprechend.“

Artikel 2

Änderung des Aufenthaltsgesetzes

Das Aufenthaltsgesetz in der Fassung der Bekanntmachung vom 25. Februar 2008 (BGBl. I S. 162), das zuletzt durch Artikel 2 des Gesetzes vom 23. April 2026 (BGBl. 2026 I Nr. 111) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:
   a) Die Angabe zu § 86 wird durch die folgende Angabe ersetzt:
      „§ 86 Verarbeitung personenbezogener Daten“.
   b) Nach der Angabe zu § 90c wird die folgende Angabe eingefügt:
      „§ 90d Automatisiertes Verfahrensmonitoring in aufenthaltsrechtlichen Verfahren
      § 90e Automatisierter Abgleich mit öffentlich zugänglichen Daten aus dem Internet“.
2. § 71 wird wie folgt geändert:
   a) In Absatz 2 Satz 3 wird die Angabe „90c, 91d“ durch die Angabe „90c bis 90e, 91d“ ersetzt.

b) In Absatz 3 Nummer 6 wird die Angabe „Bundesministerium des Innern, für Bau und Heimat“ durch die Angabe „Bundesministerium des Innern“ ersetzt.

3. § 86 wird durch den folgenden § 86 ersetzt:

„§ 86

Verarbeitung personenbezogener Daten

(1) Die mit der Ausführung dieses Gesetzes betrauten Behörden dürfen zum Zweck der Ausführung dieses Gesetzes und ausländerrechtlicher Bestimmungen in anderen Gesetzen personenbezogene Daten verarbeiten, soweit dies zur Erfüllung ihrer Aufgaben nach diesem Gesetz und nach ausländerrechtlichen Bestimmungen in anderen Gesetzen erforderlich ist. Personenbezogene Daten, deren Verarbeitung nach Artikel 9 Absatz 1 der Datenschutz-Grundverordnung untersagt ist, dürfen verarbeitet werden, soweit dies im Einzelfall zur Aufgabenerfüllung erforderlich ist; § 22 Absatz 2 des Bundesdatenschutzgesetzes gilt entsprechend.

(2) Die mit der Ausführung dieses Gesetzes betrauten Behörden dürfen die von ihnen zum Zweck der Ausführung dieses Gesetzes und ausländerrechtlicher Bestimmungen in anderen Gesetzen erhobenen personenbezogenen Daten auch zum Entwickeln, insbesondere zum Trainieren, Validieren und Testen von KI-Systemen im Sinne des Artikels 3 Nummer 1 der Verordnung (EU) 2024/1689 (Verordnung über künstliche Intelligenz) oder anderen automatisierten Anwendungen zur Datenverarbeitung verarbeiten. Die Verarbeitung nach Satz 1 ist nur zulässig, soweit die Anwendungen der Aufgabenerfüllung der zuständigen Stelle dienen und die Verarbeitung der Daten hierfür erforderlich ist. Die Behörden nach Satz 1 haben 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. Soweit Daten nach Artikel 9 Absatz 1 der Datenschutz-Grundverordnung verarbeitet werden, gilt § 22 Absatz 2 des Bundesdatenschutzgesetzes entsprechend.“

4. In § 87 Absatz 1 Satz 1 wird die Angabe „§ 86 Satz 1“ durch die Angabe „§ 86 Absatz 1 Satz 1“ ersetzt.

5. Nach § 90c werden die folgenden §§ 90d und 90e eingefügt:

„§ 90d

Automatisiertes Verfahrensmonitoring in aufenthaltsrechtlichen Verfahren

(1) Die mit der Ausführung dieses Gesetzes betrauten Behörden können die von ihnen erhobenen personenbezogenen Daten nach Maßgabe der folgenden Absätze mittels einer automatisierten Anwendung zur Datenverarbeitung zum Zweck der Analyse des Ablaufs abgeschlossener Verfahren und der bisherigen Praxis der Erteilung von Aufenthaltstiteln (Verfahrensmonitoring) weiterverarbeiten. Die Weiterverarbeitung nach Satz 1 ist nur zulässig, soweit die Daten hierfür erforderlich sind. Biometrische Daten sind von der Weiterverarbeitung ausgeschlossen. Abweichend von Satz 3 ist eine Weiterverarbeitung zulässig, soweit eine vorherige Aussonderung technisch unmöglich ist oder unverhältnismäßig hohen technischen Aufwand erfordert.

(2) Das Verfahrensmonitoring dient ausschließlich der Gewinnung verallgemeinerungsfähiger Erkenntnisse, um die Verfahren weiterzuentwickeln, zu beschleunigen und die Qualität künftiger Entscheidungen zu verbessern. Im Rahmen des Verfahrensmonitorings können

1. 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,

2. die eingehenden bedeutenden Erkenntnisse relevanten Sachverhalten zugeordnet sowie unbedeutende Informationen und Erkenntnisse ausgeschlossen werden,
3. Suchkriterien gewichtet werden, insbesondere nach Sachnähe, Aktualität und Erheblichkeit der Verknüpfung mit anderen Informationen bezogen auf den Zweck des Verfahrensmonitorings sowie
4. gespeicherte Daten statistisch ausgewertet werden.

Die Ergebnisse aus dem Verfahrensmonitoring dürfen nicht für ein Profiling im Sinne von Artikel 4 Nummer 4 der Datenschutz-Grundverordnung verwendet werden.

(3) Die mit der Ausführung dieses Gesetzes betrauten Behörden haben bei der Weiterverarbeitung nach Absatz 1 sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden.

(4) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Weiterverarbeitung nach Absatz 1 ausschließlich Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, so ist die Weiterverarbeitung unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch die Weiterverarbeitung erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.

(5) Die mit der Ausführung dieses Gesetzes betrauten Behörden haben bei der Weiterverarbeitung nach Absatz 1 sicherzustellen, dass das für die Durchführung des Verfahrensmonitorings eingesetzte Personal besonders geschult wird. Sie haben die erforderlichen technischen und organisatorischen Vorkehrungen, insbesondere zum Schutz der Daten gegen unbefugte Kenntnisnahme zu treffen. Sofern Daten im Sinne des Artikels 9 Absatz 1 der Datenschutz-Grundverordnung verarbeitet werden, gilt § 22 Absatz 2 des Bundesdatenschutzgesetzes entsprechend.

(6) Soweit zum Einsatz der automatisierten Anwendung zur Datenverarbeitung Dritte im Wege der Auftragsverarbeitung für die zuständigen Behörden tätig werden, so müssen sie ihren Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten an diese Dritten ist nur innerhalb der Europäischen Union, zuzüglich der Schengen-assoziierten Staaten, zulässig. Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 1 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Die Weiterverarbeitung von personenbezogenen Daten durch diese Dritten ist unzulässig.

§ 90e

Automatisierter Abgleich mit öffentlich zugänglichen Daten aus dem Internet

(1) Die mit der Ausführung dieses Gesetzes betrauten Behörden können im Einzelfall öffentlich zugängliche personenbezogene Daten aus dem Internet mit entscheidungserheblichen Angaben aus dem Antrag auf Erteilung eines Aufenthaltstitels mittels einer automatisierten Anwendung zur Datenverarbeitung abgleichen, soweit bei diesen einzelnen entscheidungserheblichen Angaben auf Grund tatsächlicher Anhaltspunkte begründete Zweifel an deren Richtigkeit bestehen und der Abgleich zur Aufklärung dieser Zweifel erforderlich ist. Biometrische Daten sind von dem Abgleich ausgeschlossen. Die Ergebnisse des Abgleichs müssen stets durch die Behörden nach Satz 1 manuell bewertet, eingeordnet und gegebenenfalls verifiziert werden.

(2) Die mit der Ausführung dieses Gesetzes betrauten Behörden haben bei dem Abgleich nach Absatz 1 sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden.

(3) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch einen Abgleich nach Absatz 1 ausschließlich Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, so ist der Abgleich unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch den Abgleich erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen. Die Behörden nach Absatz 1 Satz 1

haben, soweit möglich, technisch sicherzustellen, dass bei Abgleichen nach Absatz 1 Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.

(4) Die im Rahmen des Abgleichs nach Absatz 1 erhobenen Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, sobald sie nicht mehr erforderlich sind. Die Weiterverarbeitung der beim Abgleich erhobenen Daten zu anderen Zwecken ist unzulässig. Der Abgleich, das Ergebnis des Abgleichs und das Löschen der Daten sind zu dokumentieren.

(5) Im Übrigen gilt § 90d Absatz 5 und 6 entsprechend.“

Artikel 3

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

EU-Rechtsakte:

1. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35)
2. 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 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024; 2025/90802, 9.10.2025)

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Die Migrationsverwaltung sieht sich seit Jahren einem stetig steigenden Antragsaufkommen gegenüber. Die vorhandenen personellen und organisatorischen Kapazitäten reichen vielerorts nicht aus, 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. Ohne strukturelle Anpassungen ist angesichts begrenzter Ressourcen und weiter steigender Antragseingänge eine zusätzliche Belastung der Verfahren absehbar.

Ziel des Gesetzes ist es, einen rechtssicheren und datenschutzkonformen Rahmen zu schaffen, um durch den Einsatz digitaler Verfahren insbesondere Künstlicher Intelligenz – die Effizienz, Einheitlichkeit, Qualität und Sicherheit der Migrations-, Visum- und Asylbearbeitung zu erhöhen. Die Digitalisierung soll Verwaltungsabläufe beschleunigen, Ressourcen zielgerichteter nutzbar machen und eine systematische Auswertung der Praxis ermöglichen.

II. Wesentlicher Inhalt des Entwurfs

Der Gesetzentwurf schafft die rechtlichen Voraussetzungen dafür, dass die zuständigen Behörden in der Migrationsverwaltung personenbezogene Daten verarbeiten dürfen, um KI-Systeme oder andere automatisierte Anwendungen der Datenverarbeitung zu entwickeln, insbesondere zu trainieren, zu validieren und zu testen. Damit wird ein rechtssicherer Rahmen für die technische Weiterentwicklung solcher Systeme geschaffen.

Zugleich werden die gesetzlichen Grundlagen für den Einsatz spezifischer automatisierter Verfahren gelegt. Hierzu zählt das Verfahrensmonitoring, das der Beobachtung und Auswertung des Verfahrensablaufs im Zusammenhang mit der Prüfung von Anträgen und der Praxis der Erteilung von Aufenthaltstiteln dient, um verallgemeinerungsfähige Erkenntnisse über Abläufe und Entscheidungsmuster zu gewinnen. Dadurch können strukturelle Muster, Beschleunigungspotenziale und Optimierungsbedarfe identifiziert und gezielt adressiert werden. Ebenso wird unter engen Voraussetzungen der automatisierte Abgleich öffentlich zugänglicher Internetdaten mit entscheidungserheblichen Antragsangaben ermöglicht, um diese zu verifizieren, wenn begründete Zweifel an der Richtigkeit dieser Angaben bestehen.

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.

Die Befugnisse sind technik- und produktneutral ausgestaltet. Sie gewährleisten zugleich hohe Anforderungen an Datenschutz, Transparenz, Nichtdiskriminierung und den Schutz des Kernbereichs privater Lebensgestaltung.

III. Exekutiver Fußabdruck

Eine Beteiligung von Interessenvertreterinnen und -vertretern sowie von beauftragten Dritten im Rahmen des Gesetzentwurfes ist aufgrund einer fehlenden Außenwirkung dieser gesetzlichen Regelung nicht erforderlich.

IV. Alternativen

Praktisch tragfähige Alternativen zum Einsatz einer automatisierten Anwendung zur Datenverarbeitung bestehen nicht. Die Nutzung solcher Systeme bietet erhebliche organisatorische und inhaltliche Vorteile für Antragstellende wie auch für die beteiligten Behörden und ist angesichts des steigenden Antragsaufkommens unverzichtbar. Eine Ausweitung der personellen Kapazitäten scheidet aufgrund der Haushaltslage und des Fachkräftemangels aus. Ebenso ist eine systematische, umfassende Analyse und Optimierung der Verfahren ohne technische Unterstützung aus organisatorischen Gründen nicht leistbar.

Die nach dem Koalitionsvertrag für die 21. Legislaturperiode in den Zeilen 3086 f. festgelegte Absicht, das Aufenthaltsgesetz zu entbürokratisieren, um die Rechtsanwendung für alle zu vereinfachen, besteht weiterhin fort. Eine Reduktion oder Vereinfachung der rechtlichen Grundlagen würde die strukturellen Herausforderungen jedoch allein nicht lösen. Das automatisierte Verfahrensmonitoring dient der übergreifenden Analyse der Verwaltungspraxis – ein Nutzen, der unabhängig von der Zahl der Rechtsgrundlagen besteht und durch rein gesetzliche Vereinfachungen nicht erreicht werden kann. Gerade hier kann ein Verfahrensmonitoring, das mittels automatisierter Anwendungen durchgeführt wird, entlasten und durch seine Unterstützung die Qualität der Entscheidungen verbessern.

V. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes für die Änderung des Asylgesetzes (Artikel 1), des Aufenthaltsgesetzes (Artikel 2) ergibt sich aus Artikel 74 Absatz 1 Nummer 4 GG (Aufenthalts- und Niederlassungsrecht der Ausländer) und Artikel 72 Absatz 2 GG und Artikel 74 Absatz 1 Nummer 6 GG (Angelegenheiten der Flüchtlinge und Vertriebenen).

Eine bundesgesetzliche Regelung auf dem Gebiet des Artikels 74 Absatz 1 Nummer 4 GG (Aufenthalts- und Niederlassungsrecht der Ausländer) ist zur Wahrung der Rechtseinheit im gesamtstaatlichen Interesse erforderlich. Die Anpassung der bestehenden bundesgesetzlichen Aufenthaltsregelungen kann nur durch den Bundesgesetzgeber erfolgen, da ansonsten die Gefahr einer Rechtszersplitterung bestünde. Ohne eine bundeseinheitliche Regelung wären erhebliche Beeinträchtigungen des länderübergreifenden Rechtsverkehrs beim Aufenthalt von Ausländern zu erwarten.

VI. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen vereinbar.

VII. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Die Regelung dient der Verwaltungsvereinfachung: Indem Teilprozesse weitestgehend technisch unterstützt und einfache Teilprüfungen automatisiert werden können, vereinfacht sich die Bearbeitung von Anträgen und somit kann die Verwaltungspraxis vereinfacht, beschleunigt und optimiert werden.

2. Nachhaltigkeitsaspekte

Die Regelung steht im Einklang mit den Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Deutschen Nachhaltigkeitsstrategie, die der Umsetzung der Agenda 2030 für nachhaltige Entwicklung der Vereinten Nationen dient.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Es entstehen keine Ausgaben ohne Erfüllungsaufwand.

4. Erfüllungsaufwand

4.1. Erfüllungsaufwand für Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

4.2. Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht kein Erfüllungsaufwand.

4.3. Erfüllungsaufwand der Verwaltung

Für die Verwaltung entsteht kein Erfüllungsaufwand.

Änderungen des gewährleisteten und europarechtlich verbindlich vorgegebenen Umgangs mit personenbezogenen Daten, die Auswirkungen auf den Erfüllungsaufwand hätten, sind durch die vorgesehenen Rechtsänderungen nicht verbunden.

Ferner wird den zuständigen Behörden in beiden Rechtsgebieten die Möglichkeit eröffnet, KI-Systeme zu entwickeln, automatisiert die vorhandenen eigenen Daten zum Zwecke des Verfahrensmonitorings weiterzuverarbeiten oder die vorhandenen eigenen Daten im Einzelfall mit öffentlich zugänglichen Inhalten abzugleichen. Rechtlich unverbindlich kann somit jede einzelne Stelle für sich entscheiden, ob die erforderlichen Investitionen einen tatsächlichen Vorteil für die eigene behördliche Leistung bieten. Methodisch bleibt der Erfüllungsaufwand auch von dieser Gesetzesinitiative unberührt, da ihr die grundlegende Verbindlichkeit für ein solches Verfahren fehlt.

5. Weitere Kosten

Weitere Kosten entstehen nicht. Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

6. Weitere Gesetzesfolgen

Die Regelungen sind inhaltlich geschlechtsneutral. Auswirkungen von gleichstellungspolitischer Bedeutung sind nicht zu erwarten. Mittelbar sind positive Auswirkungen insofern zu erwarten, als insbesondere die systematische Untersuchung von möglichen Diskriminierungsmustern dazu dienen kann, gleichstellungspolitisch relevante Aspekte in Migrationsverfahren künftig noch besser zu adressieren.

Das Vorhaben führt nicht zu finanziellen Belastungen für künftige Generationen.

Auswirkungen auf die Wahrung und Förderung gleichwertiger Lebensverhältnisse sind nicht zu erwarten.

VIII. Befristung; Evaluierung

Eine Befristung des Gesetzes ist nicht vorgesehen.

Für das Gesetz ist gemäß Evaluierungskonzept der Bundesregierung eine Evaluierung vorgesehen. Ziel der Evaluierung ist es, das Erreichen der Zwecke der Nutzung der automatisierten Anwendungen zur Datenverarbeitung, den Schutz der personenbezogenen Daten und die effektive Vermeidung diskriminierender Algorithmen zu überprüfen. Kriterien der Zielerreichung sind unter anderem Effizienzsteigerungen bei der Titelerteilung und der Prüfung von Asylanträgen aufgrund des Verfahrensmonitoring, die Identifikation von Schwächen in der Praxis, die durch das Verfahrensmonitoring identifiziert und in der Folge adressiert werden konnten, sowie die effektive Umsetzung der Regelungen zum Schutz der personenbezogenen Daten von Antragstellern durch die Migrationsbehörden. Hierbei wären als Datengrundlage eine spezifische Untersuchung der vorgenannten Aspekte der Migrationsverfahren durch die Migrationsbehörden sowie Kontrollberichte der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit heranzuziehen. Die Evaluierung hat ab Inbetriebnahme der automatisierten Anwendungen zur Datenverarbeitung mindestens alle fünf Jahre zu erfolgen.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Asylgesetzes)

Zu Nummer 1

Es handelt sich um eine notwendige Folgeänderung zu Artikel 1 Nummer 2 Buchstabe a und Artikel 1 Nummer 3.

Zu Nummer 2

Zu Buchstabe a

Durch die Neufassung der Überschrift wird verdeutlicht, dass der bisherige Begriff „Erhebung“ als Oberbegriff für den Umgang mit personenbezogenen Daten im Asylgesetz durch den Begriff „Verarbeitung“ als unionsrechtlich harmonisierten Begriff ersetzt wird.

Zu Buchstabe b

Mit der Änderung in § 7 Absatz 1 AsylG wird der Wortlaut der Regelung an die Begrifflichkeiten der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) angepasst, indem das Wort „erheben“ durch das Wort „verarbeiten“ ersetzt wird. Die bisherige Fassung verwendet den Begriff „Erhebung“ als Oberbegriff für den Umgang mit personenbezogenen Daten im Asylrecht. Nach der Definition in Artikel 4 Nummer 2 der DSGVO umfasst der Begriff „Verarbeitung“ sämtliche Vorgänge im Zusammenhang mit personenbezogenen Daten, einschließlich der Erhebung, Speicherung, Organisation, Anpassung, Übermittlung, Löschung und Vernichtung solcher Daten. Die Änderung hat ausschließlich klarstellenden Charakter. Eine materielle Änderung der bestehenden Befugnisse oder Verpflichtungen der betroffenen Behörden ist mit der Anpassung nicht verbunden. Durch die Aufnahme des unionsrechtlich harmonisierten Begriffs „verarbeiten“ wird sichergestellt, dass die nationale Regelung mit der Systematik des europäischen Datenschutzrechts konsistent bleibt und stellt somit eine terminologische Präzisierung im Einklang mit der DSGVO dar.

Zum Schutz der besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 der DSGVO wurde im Vergleich zur bisherigen Version des § 7 Absatz 1 AsylG klarstellend auf die Schutzvorschriften des § 22 Absatz 2 des Bundesdatenschutzgesetzes Bezug genommen. Durch die unmittelbare Verweisung auf § 22 Absatz 2 des Bundesdatenschutzgesetzes wird sichergestellt, dass ein hohes Datenschutzniveau gewahrt bleibt. Die Regelung schafft einen Ausgleich zwischen den praktischen Erfordernissen der Verwaltung und dem Schutz besonders sensibler Daten.

Zu Buchstabe c

Mit der Regelung in § 7 Absatz 2a werden die datenschutzrechtlichen Befugnisse der Behörden erweitert und klar ausgestaltet. Die Regelung trägt den technischen Entwicklungen Rechnung und sorgt für Rechtssicherheit im Umgang mit innovativen automatisierten Anwendungen.

Satz 1 schafft für die genannten Behörden im Rahmen ihrer Aufgabenerfüllung eine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten zum Zwecke der Entwicklung von KI-Systemen oder anderen automatisierten Anwendungen zur Datenverarbeitung.

Der Begriff des „KI-Systems“ richtet sich nach der Begriffsbestimmung des Artikels 3 Nummer 1 der Verordnung (EU) 2024/1689 (Verordnung über künstliche Intelligenz).

Der Begriff der „automatisierten Anwendung zur Datenverarbeitung“ ist demgegenüber technik- und produktneutral ausgestaltet. Er erfasst nicht nur KI-Technologie, sondern auch herkömmliche datenanalytische Anwendungen, die regelbasiert oder statistisch arbeiten und im Rahmen der behördlichen Aufgaben entsprechend zu entwickeln sind. Damit wird sichergestellt, dass die Norm auch gegenüber zukünftigen technologischen Entwicklungen offen bleibt.

Die Verwendung beider Begriffe stellt sicher, dass die Vorschrift sowohl KI-Systeme im unionsrechtlichen Sinne als auch andere bestehende und künftige Formen automatisierter Datenverarbeitung erfasst und damit gegenüber technologischen Entwicklungen offen ausgestaltet ist.

Der Begriff „Entwicklung“ umfasst insbesondere das Trainieren, Validieren und Testen. Die Begriffe gewährleisten ein weites Verständnis hinsichtlich der Entwicklung von KI-Systemen insbesondere aufgrund divergierender Begrifflichkeiten in der Verordnung über künstliche Intelligenz. Unter Training wird die Anwendung von Verfahren beziehungsweise Methoden des maschinellen Lernens oder vergleichbarer Techniken auf einen Datensatz verstanden. Bei dem Validieren und Testen wird unter anderem die Leistungsfähigkeit, Robustheit und Generalisierungsfähigkeit geprüft. Zudem sollten potenzielle Verzerrungen geprüft werden. Der Begriff der Entwicklung schließt auch die wesentliche Veränderung eines bereits bestehenden KI-Systems oder KI-Modells ein, das von einem externen Anbieter zur Verfügung gestellt und durch die Veränderung der Parameter im Zuge eines weiteren Trainings mit den gespeicherten Daten weiterentwickelt wurde. Bei der Entwicklung soll dem KI-System u. a. beigebracht werden, 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. Dabei muss das KI-System auch systemübergreifende Beziehungen oder Zusammenhänge zwischen herkunftslandspezifischen Besonderheiten, Personen, Institutionen, Organisationen, Reisezwecken und Erteilungs- bzw. Versagungspraxen verstehen und unbedeutende Informationen und Erkenntnisse ausschließen können.

Die Schaffung einer ausdrücklichen gesetzlichen Grundlage ist erforderlich, da die Verarbeitung personenbezogener Daten zu Entwicklungszwecken regelmäßig eine Zweckänderung darstellt. Die Daten wurden ursprünglich im Rahmen asylrechtlicher Verwaltungsverfahren zur Einzelfallbearbeitung erhoben und verarbeitet. Die Nutzung dieser Daten für die Entwicklung von automatisierten Anwendungen zur Datenverarbeitung ist von diesem Zweck nicht umfasst und stellt daher eine rechtfertigungsbedürftige Verarbeitung für einen anderen Zweck im Sinne des Artikels 5 Absatz 1 Buchstabe b der DSGVO dar.

Soweit jedoch – wie hier – eine Zweckänderung im öffentlichen Bereich erfolgt, kann der Gesetzgeber gemäß Artikel 6 Absatz 3 Satz 1 DSGVO eine Rechtsgrundlage schaffen, die eine notwendige und verhältnismäßige Maßnahme zum Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses des Mitgliedstaates darstellt. Mit der Vorschrift in Absatz 2a Satz 1 wird von dieser Öffnungsklausel Gebrauch gemacht und eine Ermächtigung zur zweckändernden Verarbeitung normativ abgesichert.

Die Regelung gilt nicht für Sozialdaten, die den genannten Behörden nach § 71 Absatz 2 Satz 1 Nummer 6 des Zehnten Buches Sozialgesetzbuch (SGB X) in Verbindung mit den § 8 Absatz 1c AsylG übermittelt wurden. Sozialdaten sind personenbezogene Daten (Artikel 4 Nummer 1 der Verordnung (EU) 2016/679), die von einer in § 35 des Ersten Buches Sozialgesetzbuch genannten Stelle im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch verarbeitet werden, § 67 Absatz 2 Satz 1 SGB X. Gemäß § 78 Absatz 1 Satz 1 und Satz 3 SGB X dürfen Sozialdaten nur zu dem Zweck verarbeitet werden, zu dem sie befugt übermittelt worden sind. Zweckänderungen über den Übermittlungszweck des § 71 Absatz 2 Satz 1 Nummer 6 SGB X in Verbindung mit den § 8 Absatz 1c AsylG hinaus sind unzulässig.

Satz 2 begrenzt die Zulässigkeit dieser Verarbeitung auf automatisierte Anwendungen, die der Aufgabenerfüllung der zuständigen Stelle dienen. Dies setzt einen hinreichenden funktionalen Zusammenhang zwischen der Entwicklung der automatisierten Anwendung und den gesetzlichen Aufgaben der zuständigen Stellen voraus und stellt sicher, dass eine Nutzung zu sachfremden Zwecken ausgeschlossen ist.

Die Nutzung personenbezogener Daten für die Entwicklung, insbesondere dem Trainieren, Validieren und Testen einer automatisierten Anwendung zur Datenverarbeitung wird gestattet, wenn dies der Erfüllung einer gesetzlichen Aufgabe dient, etwa wenn die Entwicklung der Beschleunigung und der Erhöhung der Entscheidungsqualität in asylrechtlichen Verfahren dient und damit zur Effizienzsteigerung und Qualitätssicherung beiträgt.

Darüber hinaus stellt Satz 2 klar, dass die Verarbeitung personenbezogener Daten nur zulässig ist, soweit sie zur Entwicklung, insbesondere dem Trainieren, Validieren und Testen einer automatisierten Anwendung zur Datenverarbeitung erforderlich ist. Die Erforderlichkeit der Verarbeitung personenbezogener Daten ist unter Beachtung des Grundsatzes der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c in Verbindung mit Artikel 25 der Datenschutz-Grundverordnung zu beurteilen. Hierbei ist zu prüfen, ob die Verarbeitung in Bezug auf den jeweiligen Entwicklungszweck angemessen, erheblich und auf das notwendige Maß beschränkt ist. Die Rechtsgrundlage benennt hierbei bewusst keine konkreten technischen oder organisatorischen Maßnahmen in diesem Sinne.

Nach der DSGVO kommen als technische oder organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik neben der Anonymisierung oder Pseudonymisierung eine Vielzahl anderer Maßnahmen in Betracht.

Eine Anonymisierung oder Pseudonymisierung der Daten ist nicht erforderlich, wenn eine solche Verarbeitung nicht technisch möglich ist oder nur mit unverhältnismäßigem Aufwand erreicht werden kann oder hierdurch die Qualität oder Aussagekraft der Entwicklungsergebnisse wesentlich beeinträchtigt würde. Bei der Auswahl der geeigneten Trainingsdaten ist nach der Verordnung über künstliche Intelligenz dabei unter anderem zu berücksichtigen, ob und inwieweit die Trainings-, Validierungs- und Testdaten im Hinblick auf die Zweckbestimmung relevant, hinreichend repräsentativ, fehlerfrei und vollständig sind, die Verarbeitung für die Erkennung und Korrektur von Verzerrungen (Bias) erforderlich ist. Hieraus kann sich beispielsweise auch eine Verpflichtung zur Nutzung von Echtdaten ergeben.

Für die Entwicklung automatisierter Anwendungen zur Unterstützung asylrechtlicher Verfahren kann es notwendig sein, auf nicht anonymisierte oder nicht pseudonymisierte Daten zurückzugreifen. Dies kann insbesondere für Anwendungen gelten, die auf Unterstützung der Prüfung individueller Asylanträge gerichtet sind. In solchen Konstellationen kann eine Anonymisierung oder Pseudonymisierung dazu führen, dass zentrale inhaltliche Zusammenhänge nicht mehr erkannt oder zutreffend bewertet werden können.

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 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.

Des Weiteren werden mit den Sätzen 3 und 4 Schutzmaßnahmen angeordnet. Bei der Entwicklung der Anwendung zur automatisierten Datenverarbeitung hat die zu entwickelnde Stelle die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen, um Missbrauch zu verhindern und die Daten vor unbefugter Kenntnisnahme zu schützen. Zu beachten sind die unmittelbar anwendbaren Regelungen sowohl für die Verarbeitung personenbezogener Daten nach der DSGVO als auch für die Gewährung ausreichenden Schutzes nach der KI-VO. Insbesondere ergreift die entwickelnde Behörde die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Interessen der betroffenen Personen. Durch die technische Ausgestaltung und ein Kontrollsystem ist sicherzustellen, dass eine Diskriminierung der Antragstellenden durch das KI-System ausgeschlossen ist. Artikel 10 Absatz 2 Buchstabe f der Verordnung über künstliche Intelligenz schreibt insoweit 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. Nach Artikel 10 Absatz 3 Satz 1 der Verordnung über künstliche Intelligenz müssen die Datensätze ferner „relevant, hinreichend repräsentativ, fehlerfrei und vollständig“ sein – dies ist besonders wichtig zur Vermeidung strukturell benachteiligender Trainingsgrundlagen. Als geeignete Vorkehrungen kommen des Weiteren in Betracht: 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. Der Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte ist durch geeignete technische und organisatorische Maßnahmen entgegenzuwirken.

Die besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 der DSGVO sind besonders schutzwürdig. Über die entsprechende Anwendung des § 22 Absatz 2 des Bundesdatenschutzgesetzes sind diese Daten auch bei der Verarbeitung zu anderen Zwecken durch geeignete Maßnahmen besonders zu schützen. Im Einklang mit Artikel 5 Absatz 1 Buchstabe f der DSGVO ist die Integrität und Vertraulichkeit der Verarbeitung der perso-

nenbezogenen Daten sicherzustellen, indem sie nur an bestimmte Personen übermittelt werden dürfen. Die Entwicklung der Anwendungen zur automatisierten Datenverarbeitung bzw. des KI-Systems erfordert den Einsatz hochspezialisierter Experten, der die Hinzuziehung von spezialisierten Unternehmen bei der Umsetzung notwendig macht. Sofern Dritte im Wege der Auftragsverarbeitung tätig werden, ist sicherzustellen, dass dies nur unter Einhaltung der engen Voraussetzungen der DSGVO erfolgt. Es ist sicherzustellen, dass Unbefugte die Daten nicht verarbeiten und das hohe Schutzniveau der DSGVO über alle Schritte der Entwicklung und des Trainings auch dann sichergestellt ist, wenn hierzu auf Dritte zurückgegriffen werden muss. Aus Artikel 5 und Artikel 17 der DSGVO ergibt sich ergänzend die allgemeine Löschpflicht insbesondere für Daten, die nicht mehr für die Zweckerfüllung notwendig sind (Artikel 17 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679). 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 (Artikel 17 Absatz 3 der DSGVO). Dementsprechend sind entsprechende Löschfristen durch die entwickelnde Behörde festzulegen.

Zu Nummer 3 (§§ 7a, 7b)

Zu § 7a

§ 7a schafft eine ausdrückliche Rechtsgrundlage für den Einsatz automatisierter Anwendungen zur Datenverarbeitung zum Zwecke der Analyse, um ein Verfahrensmonitoring in asylrechtlichen Verfahren durch die zuständigen Behörden zu ermöglichen. Die Vorschrift trägt dem gestiegenen Bedarf an effizienter Auswertung umfangreicher Datenbestände Rechnung und ermöglicht eine technisch zeitgemäße Aufgabenerfüllung. Zugleich werden die verfassungsrechtlich gebotenen Grenzen staatlicher Datenverarbeitung gewahrt.

Die Norm legt den zulässigen Umfang der automatisierten Weiterverarbeitung fest (Absatz 1), definiert klare Zweckbindungen (Absatz 2) und enthält umfassende Schutzmechanismen, insbesondere zum Schutz des Kernbereichs privater Lebensgestaltung, zur Vermeidung diskriminierender algorithmischer Verfahren sowie zur Sicherstellung menschlicher Entscheidungsverantwortung (Absatz 3 und 4). Darüber hinaus regelt § 7a organisatorische und technische Anforderungen sowie die Einbindung externer Dienstleister, um ein hohes Datenschutzniveau und die Integrität der Datenverarbeitung zu gewährleisten (Absatz 5 und 6).

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 (vgl. Artikel 6 Absatz 3 der Verordnung (EU) 2024/1689 – Verordnung über künstliche Intelligenz).

Zu Absatz 1

Absatz 1 schafft eine ausdrückliche gesetzliche Ermächtigungsgrundlage für die mit der Ausführung dieses Gesetzes betrauten Behörden zur Durchführung eines automatisierten Verfahrensmonitoring zur Analyse des Ablaufs abgeschlossener Verfahren und der bisherigen Praxis der Entscheidungen über Asylanträge unter Nutzung personenbezogener Daten. Satz 2 stellt klar, dass die Verarbeitung personenbezogener Daten nur zulässig ist, soweit diese für den Zweck des Verfahrensmonitorings erforderlich sind. Zugleich normiert Satz 2 die Voraussetzungen, unter denen eine Verarbeitung personenbezogener Echtdaten zu diesem Zweck erfolgen darf (hierzu wird auf die Begründung zu Artikel 1 Nummer 2 Buchstabe c (§ 7 Absatz 2a AsylG) verwiesen). Satz 3 beinhaltet die Bereichsausnahme für biometrische Daten. Diese dürfen grundsätzlich nicht im Rahmen des Verfahrensmonitoring verarbeitet werden. Eine Verarbeitung ist nur ausnahmsweise zulässig. Dies kann beispielsweise bei eingescannten Passdokumenten der Fall sein, wenn eine vorherige Aussonderung des Passfotos vor der Verarbeitung technisch nicht möglich ist oder einen unverhältnismäßig hohen technischen Aufwand erfordert.

Die Regelung gilt nicht für Sozialdaten, die den genannten Behörden nach § 71 Absatz 2 Satz 1 Nummer 6 SGB X in Verbindung mit den § 8 Absatz 1c AsylG übermittelt wurden. Gemäß § 78 Absatz 1 Satz 1 und 3 SGB X ist die Zweckänderung bezüglich dieser übermittelten Daten unzulässig.

Zu Absatz 2

Der Einsatz des Verfahrensmonitorings ist strikt zweckgebunden. Eine darüberhinausgehende Nutzung oder eine Erweiterung des ursprünglichen Erhebungszwecks ist ausgeschlossen. Die Norm erlaubt ausschließlich die Verarbeitung bereits rechtmäßig erhobener Daten; eine neue Datenerhebung wird nicht eröffnet.

Der Einsatz der automatisierten Anwendung zur Datenverarbeitung verfolgt den Zweck, die Bearbeitung von asylrechtlichen Anträgen systematisch zu untersuchen. Bei der systematischen Untersuchung wertet die automatisierte Anwendung die Verfahren und die Praxis der Schutzzuerkennung bzw. Ablehnung des Asylantrags statistisch aus. Diese statistische Auswertung umfasst nicht nur das Auftreten einzelner Daten, sondern auch die Kombination verschiedener Daten sowie eine Analyse und eine Bewertung dieser Auswertung. Dadurch können die Daten verschiedener Antragsteller auf Beziehungen untereinander, zu Personengruppierungen wie beispielsweise den Familien der Antragsteller, zu Herkunfts- und Durchreiseländern sowie zu relevanten Schutzkategorien – Flüchtlingsschutz oder subsidiärer Schutz – hin untersucht werden. Im Detail etwa die Beziehungen von Faktoren wie Herkunftsland, dem Vorhandensein familiärer Bindungen in Deutschland, positiven Schutzentscheidungen, zeitlichen Trends wie zum Beispiel Anstiege von Anträgen aus bestimmten Regionen nach politischen Ereignissen, sowie die Bewertung von Entscheidungsvariablen, die besonders stark das Ergebnis und etwa die Glaubhaftigkeit von Fluchtgründen beeinflussen. Diese statistischen Ergebnisse dienen der Gewinnung verallgemeinerungsfähiger Erkenntnisse über den Ablauf des Verfahrens und die Praxis der Schutzzuerkennung beziehungsweise Ablehnung des Asylantrages. Dazu können beispielsweise Erkenntnisse zählen über vergleichbare Eigenschaften von Antragstellern aus verschiedenen Herkunftsländern und mögliche Korrelationen im Vergleich zur Erteilungspraxis (z. B. kommen aus einem bestimmten Herkunftsland mehrheitlich Personen eines bestimmten Geschlechts, werden Anträge von Personen mit bestimmten Eigenschaften besonders häufig abgelehnt oder positiv beschieden, wirken sich bestimmte Eigenschaften besonders stark oder besonders wenig aus), die Plausibilität ihrer Angaben (z. B. kommen Menschen mit bestimmten Namen typischerweise aus einer bestimmten Region). Es ist dabei nicht möglich, den Datenkranz/Gegenstand der Analyse auf bestimmte Daten zu beschränken, da die Behörden eine umfassende Prüfung durchführen und insbesondere unbekannte Strukturen im Verfahren und in der Praxis der Schutzzuerkennung bzw. Ablehnung des Asylantrages aufdecken möchten. In vielen ausländischen Staaten enthalten dabei gerade die Namen der Antragsteller aufgrund der aus ihnen erkennbaren Informationen über den soziokulturellen Kontext wesentliche Informationen, die für die genannten Untersuchungsaspekte relevant sind.

Mit Hilfe dieser Erkenntnisse sollen zum einen durch das Ableiten von Indikatoren und Parametern das jeweils asylrechtliche Verfahren weiterentwickelt, die Verfahren beschleunigt und die Entscheidungsqualität erhöht werden. Die Erkenntnisse sollen zum zweiten in die zukünftige Prüfungsintensität der Einzelfallentscheidungen über einen Asylantrag einfließen.

Die dadurch verbesserte Ressourcennutzung dient auch der Schaffung von Kapazitäten zur Beschleunigung der Verfahren in komplexeren Fällen. Eine sich dadurch verbesserte Entscheidungsqualität kann sich in einer einheitlicheren Rechtsanwendung niederschlagen, wenn die Entscheidungspraxen verschiedener Entscheider angeglichen werden können.

Absatz 2 Satz 2 Nummer 1 bis 4 enthält eine abschließende Aufzählung der möglichen Formen der Weiterverarbeitung im Rahmen einer automatisierten Anwendung zur Datenverarbeitung.

Absatz 2 Satz 3 dient der Klarstellung, dass das Verfahrensmonitoring nicht unmittelbar der Einzelfallentscheidung dient und eine Profilbildung im Sinne des Artikels 4 Nummer 4 der Datenschutz-Grundverordnung unzulässig ist.

Zu Absatz 3

Absatz 3 enthält grundrechtsschützende Schranken.

Die Behörden haben sicherzustellen, dass diskriminierende Algorithmen weder entwickelt noch eingesetzt werden. Damit wird dem Risiko algorithmischer Verzerrungen und unzulässiger Ungleichbehandlungen Rechnung getragen.

Zu Absatz 4

Absatz 4 enthält weitere grundrechtsschützende Schranken.

Der Schutz des Kernbereichs privater Lebensgestaltung folgt den verfassungsrechtlichen Vorgaben. Erkenntnisse, die ausschließlich diesen höchstpersönlichen Bereich betreffen, dürfen nicht gewonnen werden. Werden solche Erkenntnisse dennoch erlangt, sind sie unverzüglich zu löschen; die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Eine Verwertung ist ausgeschlossen.

Zu Absatz 5

Soweit beim Einsatz der automatisierten Anwendung zur Datenverarbeitung die Anwendungsbereiche der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) sowie der Verordnung über künstliche Intelligenz eröffnet sind, gelten die entsprechenden Vorgaben unmittelbar und sind bereits beim Design, Training und Einsatz zu berücksichtigen. Insbesondere haben die Behörden zum Schutz der Interessen der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen.

Eine zentrale Vorgabe aus der Verordnung über künstliche Intelligenz ist das Risikomanagementsystem nach Artikel 9 der Verordnung über künstliche Intelligenz, das vor 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. Artikel 9 Absatz 2 Buchstabe c der Verordnung über künstliche Intelligenz verpflichtet insbesondere zur fortlaufenden Überwachung der KI-Leistung und zum Umgang mit Abweichungen und Fehlverhalten. Darüber hinaus schreibt Artikel 10 Absatz 2 Buchstabe f der Verordnung über künstliche Intelligenz 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. Nach Artikel 10 Absatz 3 Satz 1 der Verordnung über künstliche Intelligenz müssen die Datensätze ferner „relevant, hinreichend repräsentativ, fehlerfrei und vollständig“ sein – dies ist besonders wichtig zur Vermeidung strukturell benachteiligender Trainingsgrundlagen. Ergänzend verlangt Artikel 13 der Verordnung über künstliche Intelligenz 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. Auch dies dient mittelbar der Kontrolle und Korrektur diskriminierender Tendenzen. Nach Artikel 14 der Verordnung über künstliche Intelligenz muss zudem eine menschliche Aufsicht gewährleistet werden, um beispielsweise potenziell diskriminierende Entscheidungen erkennen und korrigieren zu können. Die Aufsichtspersonen müssen angemessen geschult und befugt sein (Artikel 14 Absatz 4).

Diesen Vorgaben dienen die Absätze 3 bis 5 und verpflichten die Behörden, organisatorische und technische Maßnahmen zu treffen, um den Schutz der Daten sicherzustellen. Das eingesetzte Personal ist besonders zu schulen, um die Funktionsweise der automatisierten Anwendungen, deren Grenzen sowie die datenschutzrechtlichen Anforderungen zu verstehen. Angemessene technische und organisatorische Maßnahmen müssen auch ergriffen werden, um die Daten vor unbefugter Kenntnisnahme zu schützen. Hierzu zählen insbesondere Zugriffsregelungen, Protokollierungen und IT-Sicherheitsmaßnahmen.

Zu Absatz 6

Die Entwicklung und der Betrieb von automatisierten Anwendungen zur Datenverarbeitung, wie KI-Systemen, erfordert den Einsatz hochspezialisierter Expertise, weshalb die Hinzuziehung externer, technisch besonders qualifizierter Unternehmen im Wege der Auftragsverarbeitung notwendig sein kann. Um sicherzustellen, dass die hierbei verarbeiteten personenbezogenen Daten weiterhin dem hohen Schutzniveau der der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) unterliegen, begrenzt Absatz 6 die Einbindung solcher Dritten auf Auftragsverarbeiter mit Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat. Die Dritten dürfen die Daten nicht für eigene Zwecke weiterverarbeiten. Insbesondere dürfen Dritte die personenbezogenen Daten nicht an den Herkunftsstaat der betroffenen Person oder an Stellen, die dem Herkunftsstaat zuzurechnen sind, übermitteln.

Die Übermittlung personenbezogener Daten ist ausschließlich an Amtsträger sowie für den öffentlichen Dienst besonders oder zur Geheimhaltung verpflichtete Personen zulässig. Damit stellt Absatz 6 sicher, dass unbefugte Stellen keinen Zugang zu den sensiblen Daten erhalten und dass der datenschutzrechtliche Schutz über sämtliche Phasen der Entwicklung und des Betriebs der automatisierten Anwendung gewährleistet bleibt, auch wenn hierfür externe Dienstleister eingesetzt werden müssen.

Zu § 7b

§ 7b schafft eine begrenzte Befugnis des Bundesamtes öffentlich zugängliche personenbezogene Daten aus dem Internet allein mit den entscheidungserheblichen Angaben, hinsichtlich derer begründete Zweifel an ihrer Richtigkeit bestehen, automatisiert abzugleichen. Die Vorschrift trägt dem Bedürfnis des Bundesamtes Rechnung, bei begründeten Zweifeln an der Richtigkeit von Angaben im Einzelfall effizient und verlässlich zu prüfen, ob öf-

fentlich zugängliche Informationen bestätigende oder widersprüchliche Hinweise enthalten. Anders als § 15b AsylG, welcher der Identifizierung der betroffenen Person dient, bezweckt diese Vorschrift, Angaben und insbesondere eingereichte Unterlagen bei begründeten Zweifeln durch einen automatisierten Internetabgleich zu verifizieren.

Zu Absatz 1

Absatz 1 schafft die Rechtsgrundlage für einen automatisierten Abgleich öffentlich zugänglicher personenbezogener Daten aus dem Internet mit entscheidungserheblichen Angaben hinsichtlich derer begründete Zweifel an ihrer Richtigkeit bestehen, wenn dies im Einzelfall zur Überprüfung der Richtigkeit der Angaben erforderlich ist. Der Abgleich dient allein dazu, die Richtigkeit von bestimmten, im Einzelfall angezweifelten, entscheidungserheblichen Angaben im Antragsverfahren zu überprüfen und enthält keine Vorfestlegung in Bezug auf das Ergebnis der Antragsprüfung.

Dem Bundesamt stehen zum Zeitpunkt der Antragstellung in vielen Fällen keine Daten zu den Antragstellenden zur Verfügung, sofern nicht noch Daten aus früheren Asylverfahren in den Datenbeständen vorhanden sind. Es fehlt damit die Möglichkeit, die Angaben der Antragstellenden zu verifizieren, sofern im Rahmen der Antragsbearbeitung Auffälligkeiten erkannt werden, die Zweifel an der Richtigkeit der Angaben begründen.

Solche begründeten Zweifel liegen vor, wenn tatsächliche Anhaltspunkte die Richtigkeit der Angaben plausibel infrage stellen. Sie können sich insbesondere im Rahmen der Aufbereitung der Antragsunterlagen oder der Einzelfallbearbeitung ergeben. Ein begründeter Zweifel kann bestehen, wenn die Angaben in sich widersprüchlich sind oder sonst unplausibel sind, etwa wenn die gesprochene Sprache oder der Dialekt nicht zur behaupteten Herkunftsregion passt, der geschilderte Reiseweg im Widerspruch zu den Ein- und Ausreisestempeln oder sonstigen Erkenntnissen steht oder sich die Angaben zu Aufenthaltsorten, familiären Verhältnissen oder der Flucht- und Verfolgungsgeschichte im Verlauf des Verfahrens wesentlich ändern. Gleiches gilt, wenn eingereichte Dokumente, etwa behördliche Bescheinigungen, Urkunden oder Zeugnisse, von vergleichbaren Unterlagen anderer Antragstellender abweichen oder in dieser Form bislang unbekannt sind. Dies kann beispielsweise der Fall sein, wenn Format, Gestaltung oder Sicherheitsmerkmale von bekannten Mustern abweichen, Dokumente ungewöhnliche Schreibweisen oder untypische Stempel aufweisen oder sich Anhaltspunkte dafür ergeben, dass sie nachträglich verändert oder nicht von der angegebenen ausstellenden Stelle herrühren. Ebenso können konkrete Erkenntnisse aus der Beobachtung vergangener Verfahren vorliegen, dass bestimmte Dokumente oder Angaben von bestimmten Orten oder Regionen besonders häufig als falsch aufgefallen sind und daher besonders kritischer Überprüfung bedürfen.

Für den Abgleich können nur die entscheidungserheblichen Angaben herangezogen werden, bei denen begründete Zweifel an der Richtigkeit bestehen. Dies können auch personenbezogene Daten der Antragstellenden sein, die das Bundesamt zur Erfüllung seiner Aufgaben rechtmäßig erhoben hat und bei denen begründete Zweifel an ihrer Richtigkeit bestehen. Hierunter können ebenso besondere Kategorien personenbezogener Daten nach Artikel 9 der Datenschutz-Grundverordnung fallen, sofern der Abgleich in Bezug auf diese Daten zur Aufklärung der Zweifel erforderlich ist. Hiervon ausgenommen sind biometrische Daten (§ 7b Absatz 1 Satz 2 AsylG). Diese dürfen im Rahmen des automatisierten Internetabgleichs nicht verarbeitet werden. Sofern besondere Kategorien personenbezogener Daten verarbeitet werden, gelten die in § 7a Absatz 5 AsylG normierten Schutzmaßnahmen gleichermaßen (§ 7b Absatz 5 AsylG).

Der Abgleich setzt notwendigerweise die Erhebung öffentlich zugänglicher personenbezogener Daten voraus. Unter öffentlich zugänglichen Daten fallen solche Daten, die von jedermann eingesehen werden können, beispielsweise aus sozialen Medien, soweit sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten. Konkretisierend fallen darunter Daten, die jede Person ohne oder nach vorheriger Registrierung, Genehmigung oder Entgeltzahlung nutzen kann. Nicht umfasst sind Daten, die einer spezifischen Schwelle unterzogen sind, beispielsweise der Einstellung von Daten in sozialen Medien für einen begrenzten Kreis, dessen Zugang einer Kontrolle unterzogen wird. Privatkommunikation über Messenger-Dienste von sozialen Medien kann nicht von der Maßnahme erfasst werden.

Der Abgleich kann mittels einer automatisierten Anwendung zur Datenverarbeitung durchgeführt werden. Für den Begriff der „automatisierten Anwendung“ wird auf Artikel 1 Nummer 2 Buchstabe c verwiesen. Im Vergleich zu einer ausschließlich manuellen Recherche ermöglicht der automatisierte Abgleich eine deutlich effizientere, schnellere und einheitliche Auswertung öffentlich zugänglicher Informationen. Es handelt sich dabei um

einen methodisch einfachen Datenabgleich. Ausgeschlossen sind komplexe Anwendungen, die nicht auf einem auf den bislang erkennbaren Sachverhalt bezogenen Suchbegriff gründen, sondern darauf zielen, allein statistische Auffälligkeiten in den Datenmengen zu entdecken, die darüber hinaus (automatisiert) in weiteren Abgleichschritten mit bestimmten Datenbeständen verknüpft werden und so zu weiteren Informationen führen können.

Satz 3 stellt klar, dass der automatisierte Abgleich im Einzelfall lediglich ein technisches Unterstützungsinstrument darstellt und keine eigenständige Entscheidungsbefugnis begründet. Die abschließende Bewertung der durch den automatisierten Abgleich generierten Ergebnisse bleibt dem Bundesamt nach Überprüfung und Verifizierung durch eine natürliche Person vorbehalten. Damit wird sichergestellt, dass die Entscheidung über die Richtigkeit oder Relevanz der gewonnenen Hinweise stets einer menschlichen Kontrolle unterliegt. Dies ist insbesondere vor dem Hintergrund möglicher Fehlzuordnungen, algorithmischer Verzerrungen oder unvollständiger Datengrundlagen erforderlich. Die Verpflichtung zur manuellen Einordnung und gegebenenfalls notwendigen Verifizierung gewährleistet, dass die Ergebnisse des Abgleichs in den behördlichen Entscheidungsprozess nur nach einer qualifizierten fachlichen Prüfung einfließen dürfen.

Zu Absatz 2

Das Bundesamt hat organisatorisch und technisch sicherzustellen, dass durch den automatisierten Abgleich diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Dem Erfordernis tragen ebenso § 7b Absatz 1 Satz 3 und Absatz 5 AsylG Rechnung.

Zu Absatz 3

Erkenntnisse aus dem Kernbereich privater Lebensgestaltung dürfen weder erhoben noch verwertet werden; werden sie dennoch erlangt, sind sie unverzüglich zu löschen und die Löschung ist zu dokumentieren. Soweit technisch möglich, ist bereits im Vorfeld sicherzustellen, dass kernbereichsrelevante Daten nicht erhoben werden.

Zu Absatz 4

Die im Rahmen des Abgleichs erhobenen Daten dürfen ausschließlich für den Abgleich verwendet werden und sind nach dessen Durchführung unverzüglich zu löschen, sobald sie nicht mehr erforderlich sind. Die durch den Abgleich im Einzelfall gewonnenen Erkenntnisse dürfen nicht zu anderen Zwecken weiterverarbeitet werden. Der Abgleich dient ausschließlich der Überprüfung von Daten im Rahmen der Unterstützung bei der Prüfung eines Antrags auf Schutzzuerkennung (Einzelfallprüfung). Der Abgleich, sein Ergebnis sowie die Löschung der Daten sind vollständig zu dokumentieren, um Transparenz und Nachvollziehbarkeit zu gewährleisten.

Zu Absatz 5

Absatz 5 stellt klar, dass die Vorgaben des § 7a Absatz 5 und 6 AsylG entsprechend gelten. Damit werden sowohl die Anforderungen an die besondere Schulung des eingesetzten Personals als auch die technischen und organisatorischen Maßnahmen zum Schutz der Daten auf den automatisierten Abgleich einschließlich der besonderen Schutzmaßnahmen für Daten nach Artikel 9 der Datenschutz-Grundverordnung übertragen. Zudem gelten die Beschränkungen für den Einsatz externer Auftragsverarbeiter entsprechend.

Zu Artikel 2 (Änderung des Aufenthaltsgesetzes)

Zu Nummer 1

Zu Buchstabe a

Es handelt sich um eine notwendige Folgeänderung zu Artikel 2 Nummer 3. Im Weiteren wird auf die Begründung zu Artikel 2 Nummer 3 verwiesen.

Zu Buchstabe b

Es handelt sich um eine notwendige Folgeänderung zu Artikel 2 Nummer 5.

Zu Nummer 2

Zu Buchstabe a

Es handelt sich um eine notwendige Folgeänderung zu Artikel 2 Nummer 5. Mit der Regelung wird klargestellt, dass das Bundesamt für Auswärtige Angelegenheiten im Rahmen seiner Zuständigkeit ebenfalls befugt ist, eine Datenverarbeitung im Sinne der §§ 90d und 90e AufenthG vorzunehmen.

Zu Buchstabe b

Es handelt sich um eine redaktionelle Änderung. Durch Organisationserlasse des Bundeskanzlers vom 8. Dezember 2021 (BGBl. 2021 I Nr. 83, S. 5176) und vom 6. Mai 2025 (BGBl. 2025 I Nr. 131) gemäß § 9 der Geschäftsordnung der Bundesregierung trägt das vormals bezeichnete Bundesministerium des Innern, für Bau und Heimat nunmehr die Bezeichnung Bundesministerium des Innern.

Zu Nummer 3

§ 86 wird neu gefasst. Durch die Neufassung der Überschrift wird verdeutlicht, dass der bisherige Begriff „Erhebung“ als Oberbegriff für den Umgang mit personenbezogenen Daten im Aufenthaltsrecht durch den Begriff „Verarbeitung“ als unionsrechtlich harmonisierten Begriff ersetzt wird. Im Weiteren wird auf die Begründung zu Absatz 1 verwiesen.

Mit der Regelung in § 86 Absatz 2 werden die datenschutzrechtlichen Befugnisse der Behörden erweitert und klar ausgestaltet. Die Regelung trägt den technischen Entwicklungen Rechnung und sorgt für Rechtssicherheit im Umgang mit innovativen automatisierten Anwendungen.

Der Begriff „mit der Ausführung dieses Gesetzes betraute Behörden“ umfasst dabei alle Behörden, denen das Aufenthaltsgesetz ausdrücklich oder der Sache nach Aufgaben zuweist. Maßgeblich ist nicht die Bezeichnung der Behörde, sondern die funktionale Zuständigkeit, die sich aus den spezialgesetzlichen Regelungen des Aufenthaltsgesetzes ergibt. Zu diesem Behördenkreis gehören 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. Das Bundesverwaltungsamt zählt ebenfalls zu den „mit der Ausführung dieses Gesetzes betrauten Behörden“, soweit ihm das Aufenthaltsgesetz spezifische Aufgaben zuweist. Durch diese gesetzlich zugewiesenen Funktionen ist das Bundesverwaltungsamt unmittelbar in die Durchführung des Aufenthaltsrechts außerhalb der Entscheidung im Einzelfall eingebunden. Es erfüllt zentrale Verwaltungs-, Register- und Unterstützungsaufgaben, die für die Anwendung des Aufenthaltsgesetzes erforderlich sind. Ebenfalls umfasst sind die Bundespolizei und die Polizeibehörden der Länder, soweit ihnen das Aufenthaltsgesetz eigene Aufgaben zuweist (§ 71 Absatz 3 des Aufenthaltsgesetzes). Dies betrifft zum Beispiel die Erteilung eines Visums.

Zu Absatz 1

Die bisherige Fassung des § 86 wird in veränderter Form als Absatz 1 der Norm übernommen. Mit der Änderung wird der Wortlaut der Regelung an die Begrifflichkeiten der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) angepasst, indem das Wort „erheben“ durch das Wort „verarbeiten“ ersetzt wird. Die bisherige Fassung verwendet den Begriff „Erhebung“ als Oberbegriff für den Umgang mit personenbezogenen Daten im Aufenthaltsrecht. Nach der Definition in Artikel 4 Nummer 2 der DSGVO umfasst der Begriff „Verarbeitung“ sämtliche Vorgänge im Zusammenhang mit personenbezogenen Daten, einschließlich der Erhebung, Speicherung, Organisation, Anpassung, Übermittlung, Löschung und Vernichtung solcher Daten. Die Änderung hat ausschließlich klarstellenden Charakter. Eine materielle Änderung der bestehenden Befugnisse oder Verpflichtungen der betroffenen Behörden ist mit der Anpassung nicht verbunden. Durch die Aufnahme des unionsrechtlich harmonisierten Begriffs „verarbeiten“ wird sichergestellt, dass die nationale Regelung mit der Systematik des europäischen Datenschutzrechts konsistent bleibt und stellt somit eine terminologische Präzisierung im Einklang mit der DSGVO dar.

Zum Schutz der besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 der DSGVO wurde im Vergleich zur bisherigen Version des § 86 klarstellend auf die Schutzvorschriften des § 22 Absatz 2 des Bundesdatenschutzgesetzes Bezug genommen. Durch die unmittelbare Verweisung auf § 22 Absatz 2 des Bundesdatenschutzgesetzes wird sichergestellt, dass ein hohes Datenschutzniveau gewahrt bleibt. Die Regelung schafft einen Ausgleich zwischen den praktischen Erfordernissen der Verwaltung und dem Schutz besonders sensibler Daten.

Zu Absatz 2

Satz 1 schafft für die genannten Stellen im Rahmen ihrer Aufgabenerfüllung eine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten zum Zwecke der Entwicklung von KI-Systemen oder anderen automatisierten Anwendungen zur Datenverarbeitung.

Der Begriff des „KI-Systems“ richtet sich nach der Begriffsbestimmung des Artikels 3 Nummer 1 der Verordnung (EU) 2024/1689 (Verordnung über künstliche Intelligenz).

Der Begriff der „automatisierten Anwendung zur Datenverarbeitung“ ist demgegenüber technik- und produktneutral ausgestaltet. Er erfasst nicht nur KI-Technologie, sondern auch herkömmliche datenanalytische Anwendungen, die regelbasiert oder statistisch arbeiten und im Rahmen der behördlichen Aufgaben entsprechend zu entwickeln sind. Damit wird sichergestellt, dass die Norm auch gegenüber zukünftigen technologischen Entwicklungen offen bleibt.

Die Verwendung beider Begriffe stellt sicher, dass die Vorschrift sowohl KI-Systeme im unionsrechtlichen Sinne als auch andere bestehende und künftige Formen automatisierter Datenverarbeitung erfasst und damit gegenüber technologischen Entwicklungen offen ausgestaltet ist.

Der Begriff „Entwicklung“ umfasst insbesondere das Trainieren, Validieren und Testen. Die Begriffe gewährleisten ein weites Verständnis hinsichtlich der Entwicklung von KI-Systemen insbesondere aufgrund divergierender Begrifflichkeiten in der Verordnung über künstliche Intelligenz. Unter Training wird die Anwendung von Verfahren beziehungsweise Methoden des maschinellen Lernens oder vergleichbarer Techniken auf einen Datensatz verstanden. Bei dem Validieren und Testen wird unter anderem die Leistungsfähigkeit, Robustheit und Generalisierungsfähigkeit geprüft. Zudem sollten potenzielle Verzerrungen geprüft werden. Der Begriff der Entwicklung schließt auch die wesentliche Veränderung eines bereits bestehenden KI-Systems oder KI-Modells ein, das von einem externen Anbieter zur Verfügung gestellt und durch die Veränderung der Parameter im Zuge eines weiteren Trainings mit den gespeicherten Daten weiterentwickelt wurde. Bei der Entwicklung soll dem KI-System u. a. beigebracht werden, 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 Schaffung einer ausdrücklichen gesetzlichen Grundlage ist erforderlich, da die Verarbeitung personenbezogener Daten zu Entwicklungszwecken regelmäßig eine Zweckänderung darstellt. Die Daten wurden ursprünglich im Rahmen aufenthaltsrechtlicher Verwaltungsverfahren zur Einzelfallbearbeitung erhoben und verarbeitet. Die Nutzung dieser Daten für die Entwicklung von automatisierten Anwendungen zur Datenverarbeitung ist von diesem Zweck nicht umfasst und stellt daher eine rechtfertigungsbedürftige Verarbeitung für einen anderen Zweck im Sinne des Artikels 5 Absatz 1 Buchstabe b der DSGVO dar.

Soweit jedoch – wie hier – eine Zweckänderung im öffentlichen Bereich erfolgt, kann der Gesetzgeber gemäß Artikel 6 Absatz 3 Satz 1 DSGVO eine Rechtsgrundlage schaffen, die eine notwendige und verhältnismäßige Maßnahme zum Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses des Mitgliedstaates darstellt. Mit der Vorschrift in Absatz 2 Satz 1 wird von dieser Öffnungsklausel Gebrauch gemacht und eine Ermächtigung zur zweckändernden Verarbeitung normativ abgesichert.

Die Regelung gilt nicht für Sozialdaten, die den genannten Behörden nach § 71 Absatz 2 Satz 1 Nummer 1 bis 3 und Satz 2 Nummer 2 des SGB X in Verbindung mit den jeweiligen Vorschriften des AufenthG übermittelt wurden. Gemäß § 78 Absatz 1 Satz 1 und Satz 3 SGB X ist die Zweckänderung bezüglich dieser Daten unzulässig.

Satz 2 begrenzt die Zulässigkeit dieser Verarbeitung auf automatisierte Anwendungen, die der Aufgabenerfüllung der zuständigen Stelle dienen. Dies setzt einen hinreichenden funktionalen Zusammenhang zwischen der Entwicklung der automatisierten Anwendung und den gesetzlichen Aufgaben der zuständigen Stellen voraus und stellt sicher, dass eine Nutzung zu sachfremden Zwecken ausgeschlossen ist.

Die Nutzung personenbezogener Daten für die Entwicklung, insbesondere dem Trainieren, Validieren und Testen einer automatisierten Anwendung zur Datenverarbeitung wird gestattet, wenn dies der Erfüllung einer gesetzlichen Aufgabe dient, etwa wenn die Entwicklung der Beschleunigung und der Erhöhung der Entscheidungsqualität in aufenthaltsrechtlichen Verfahren dient und damit zur Effizienzsteigerung und Qualitätssicherung beiträgt.

Darüber hinaus stellt Satz 2 klar, dass die Verarbeitung personenbezogener Daten nur zulässig ist, soweit sie zur Entwicklung, insbesondere dem Trainieren, Validieren und Testen einer automatisierten Anwendung zur Datenverarbeitung erforderlich ist. Die Erforderlichkeit der Verarbeitung personenbezogener Daten ist unter Beachtung

des Grundsatzes der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c in Verbindung mit Artikel 25 der Datenschutz-Grundverordnung zu beurteilen. Hierbei ist zu prüfen, ob die Verarbeitung in Bezug auf den jeweiligen Entwicklungszweck angemessen, erheblich und auf das notwendige Maß beschränkt ist. Die Rechtsgrundlage benennt hierbei bewusst keine konkreten technischen oder organisatorischen Maßnahmen in diesem Sinne.

Nach der DSGVO kommen als technische oder organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik neben der Anonymisierung oder Pseudonymisierung eine Vielzahl anderer Maßnahmen in Betracht. Eine Anonymisierung oder Pseudonymisierung der Daten ist nicht erforderlich, wenn eine solche Verarbeitung nicht technisch möglich ist oder nur mit unverhältnismäßigem Aufwand erreicht werden kann oder hierdurch die Qualität oder Aussagekraft der Entwicklungsergebnisse wesentlich beeinträchtigt würde. Bei der Auswahl der geeigneten Trainingsdaten ist nach der Verordnung über künstliche Intelligenz dabei unter anderem zu berücksichtigen, ob und inwieweit die Trainings-, Validierungs- und Testdaten im Hinblick auf die Zweckbestimmung relevant, hinreichend repräsentativ, fehlerfrei und vollständig sind, die Verarbeitung für die Erkennung und Korrektur von Verzerrungen (Bias) erforderlich ist. Hieraus kann sich beispielsweise auch eine Verpflichtung zur Nutzung von Echtdaten ergeben.

Für die Entwicklung automatisierter Anwendungen zur Unterstützung aufenthaltsrechtlicher Verfahren kann es notwendig 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 gerichtet sind. In solchen Konstellationen kann eine Anonymisierung oder Pseudonymisierung dazu führen, dass zentrale inhaltliche Zusammenhänge nicht mehr erkannt oder zutreffend bewertet werden können.

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 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.

Des Weiteren werden mit den Sätzen 3 und 4 Schutzmaßnahmen angeordnet. Bei der Entwicklung der Anwendung zur automatisierten Datenverarbeitung hat die zu entwickelnde Stelle die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen, um Missbrauch zu verhindern und die Daten vor unbefugter Kenntnisnahme zu schützen. Zu beachten sind die unmittelbar anwendbaren Regelungen sowohl für die Verarbeitung personenbezogener Daten nach der DSGVO als auch für die Gewährung ausreichenden Schutzes nach der Verordnung über künstliche Intelligenz. Insbesondere ergreift die entwickelnde Behörde die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Interessen der betroffenen Personen. Durch die technische Ausgestaltung und ein Kontrollsystem ist sicherzustellen, dass eine Diskriminierung der Antragstellenden durch das KI-System ausgeschlossen ist. Artikel 10 Absatz 2 Buchstabe f der Verordnung über künstliche Intelligenz schreibt insoweit 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. Nach Artikel 10 Absatz 3 Satz 1 der Verordnung über künstliche Intelligenz müssen die Datensätze ferner „relevant, hinreichend repräsentativ, fehlerfrei und vollständig“ sein – dies ist besonders wichtig zur Vermeidung strukturell benachteiligender Trainingsgrundlagen. Als geeignete Vorkehrungen kommen des Weiteren in Betracht: die technische Zugriffsbeschränkung auf eine begrenzte Anzahl von Mitarbeitenden und die besondere Qualifizierung dieser, die technische Trennung von Datenbestän-

den nach ihren unterschiedlichen Verarbeitungszwecken sowie die Verschleierung von sensiblen Inhalten. Der Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte ist durch geeignete technische und organisatorische Maßnahmen entgegenzuwirken.

Die besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 der DSGVO sind besonders schutzwürdig. Über die entsprechende Anwendung des § 22 Absatz 2 des Bundesdatenschutzgesetzes sind diese Daten auch bei der Verarbeitung zu anderen Zwecken durch geeignete Maßnahmen besonders zu schützen. Im Einklang mit Artikel 5 Absatz 1 Buchstabe f der DSGVO ist die Integrität und Vertraulichkeit der Verarbeitung der personenbezogenen Daten sicherzustellen, indem sie nur an bestimmte Personen übermittelt werden dürfen. Die Entwicklung der Anwendungen zur automatisierten Datenverarbeitung bzw. des KI-Systems erfordert den Einsatz hochspezialisierter Experten, der die Hinzuziehung von spezialisierten Unternehmen bei der Umsetzung notwendig macht. Sofern Dritte im Wege der Auftragsverarbeitung tätig werden, ist sicherzustellen, dass dies nur unter Einhaltung der engen Voraussetzungen der DSGVO erfolgt. Es ist sicherzustellen, dass Unbefugte die Daten nicht verarbeiten und das hohe Schutzniveau der DSGVO über alle Schritte der Entwicklung und des Trainings auch dann sichergestellt ist, wenn hierzu auf Dritte zurückgegriffen werden muss. Aus Artikel 5 und Artikel 17 der DSGVO ergibt sich ergänzend die allgemeine Löschpflicht insbesondere für Daten, die nicht mehr für die Zweckerfüllung notwendig sind (Artikel 17 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679). 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 (Artikel 17 Absatz 3 der DSGVO). Dementsprechend sind entsprechende Löschfristen durch die entwickelnde Behörde festzulegen.

Zu Nummer 4

Es handelt sich um eine notwendige Folgeänderung zu Artikel 2 Nummer 3 .

Zu Nummer 5 (§§ 90d, 90e)

Zu § 90d

§ 90d schafft eine ausdrückliche Rechtsgrundlage für den Einsatz automatisierter Anwendungen zur Datenverarbeitung zum Zwecke der Analyse, um ein Verfahrensmonitoring in aufenthaltsrechtlichen Verfahren durch die zuständigen Behörden zu ermöglichen. Die Vorschrift trägt dem gestiegenen Bedarf an effizienter Auswertung umfangreicher Datenbestände Rechnung und ermöglicht eine technisch zeitgemäße Aufgabenerfüllung. Zugleich werden die verfassungsrechtlich gebotenen Grenzen staatlicher Datenverarbeitung gewahrt.

Die Norm legt den zulässigen Umfang der automatisierten Weiterverarbeitung fest (Absatz 1), definiert klare Zweckbindungen (Absatz 2) und enthält umfassende Schutzmechanismen, insbesondere zum Schutz des Kernbereichs privater Lebensgestaltung, zur Vermeidung diskriminierender algorithmischer Verfahren sowie zur Sicherstellung menschlicher Entscheidungsverantwortung (Absatz 3 und 4). Darüber hinaus regelt § 90d organisatorische und technische Anforderungen sowie die Einbindung externer Dienstleister, um ein hohes Datenschutzniveau und die Integrität der Datenverarbeitung zu gewährleisten (Absatz 5 und 6).

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 (vgl. Artikel 6 Absatz 3 der Verordnung (EU) 2024/1689 – Verordnung über künstliche Intelligenz).

Zu Absatz 1

Absatz 1 schafft eine ausdrückliche gesetzliche Ermächtigungsgrundlage für die mit der Ausführung dieses Gesetzes betrauten Behörden (hierzu wird auf die Begründung zu Artikel 2 Nummer 3 verwiesen) zur Durchführung eines automatisierten Verfahrensmonitoring zur Analyse des Ablaufs abgeschlossener Verfahren und der bisherigen Praxis der Erteilung von Aufenthaltstiteln unter Nutzung personenbezogener Daten. Satz 2 stellt klar, dass die Verarbeitung personenbezogener Daten nur zulässig ist, soweit diese für den Zweck des Verfahrensmonitorings erforderlich sind. Zugleich normiert Satz 2 die Voraussetzungen, unter denen eine Verarbeitung personenbezogener Echtdaten zu diesem Zweck erfolgen darf (hierzu wird auf die Begründung zu Artikel 2 Nummer 3 (§ 86 Absatz 2 AufenthG) verwiesen). Satz 3 beinhaltet die Bereichsausnahme für biometrische Daten. Diese dürfen grundsätzlich nicht im Rahmen des Verfahrensmonitoring verarbeitet werden. Eine Verarbeitung ist nur ausnahmsweise zulässig. Dies kann beispielsweise bei eingescannten Passdokumenten der Fall sein, wenn eine vor-

herige Aussonderung des Passfotos vor der Verarbeitung technisch nicht möglich ist oder einen unverhältnismäßig hohen technischen Aufwand erfordert.

Die Regelung gilt nicht für Sozialdaten, die den genannten Behörden nach § 71 Absatz 2 Satz 1 Nummer 1 bis 3 und Satz 2 Nummer 2 SGB X in Verbindung mit den jeweiligen Vorschriften des AufenthG übermittelt wurden. Gemäß § 78 Absatz 1 Satz 1 und 3 SGB X ist die Zweckänderung bezüglich dieser Daten unzulässig.

Zu Absatz 2

Der Einsatz des Verfahrensmonitorings ist strikt zweckgebunden. Eine darüberhinausgehende Nutzung oder eine Erweiterung des ursprünglichen Erhebungszwecks ist ausgeschlossen. Die Norm erlaubt ausschließlich die Verarbeitung bereits rechtmäßig erhobener Daten; eine neue Datenerhebung wird nicht eröffnet.

Der Einsatz der automatisierten Anwendung zur Datenverarbeitung verfolgt den Zweck, die Bearbeitung von aufenthaltsrechtlichen Anträgen systematisch zu untersuchen. Bei der systematischen Untersuchung wertet die automatisierte Anwendung die Verfahren und die Praxis der Titelerteilung statistisch aus. Diese statistische Auswertung umfasst nicht nur das Auftreten einzelner Daten, sondern auch die Kombination verschiedener Daten sowie eine Analyse und eine Bewertung dieser Auswertung. Dadurch können die 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, untersucht werden. Diese statistischen Ergebnisse dienen der Gewinnung verallgemeinerungsfähiger Erkenntnisse über den Ablauf des Verfahrens und die Praxis der Titelerteilung. Dazu können beispielsweise Erkenntnisse zählen über vergleichbare Eigenschaften von Antragstellern aus verschiedenen Ländern und mögliche Korrelationen im Vergleich zur Erteilungspraxis (z. B. kommen aus einem bestimmten Land mehrheitlich Personen eines bestimmten Geschlechts, werden Anträge von Personen mit bestimmten Eigenschaften besonders häufig abgelehnt oder positiv beschieden, wirken sich bestimmte Eigenschaften besonders stark oder besonders wenig aus), die Plausibilität ihrer Angaben (z. B. kommen Menschen mit bestimmten Namen typischerweise aus einer bestimmten Region und besuchen dort bestimmte Schulen, sind bestimmte Beschäftigungsverhältnisse besonders häufig oder besonders ungewöhnlich) oder Missbrauchsmuster (z. B. beantragen Antragsteller mit dem vorgetäuschten Abschluss einer bestimmten Universität an einem bestimmten Ort besonders häufig den gleichen Aufenthaltstitel, weichen bei bestimmten ausländischen Staatsangehörigen bestimmte Beschäftigungsangebote auffällig voneinander ab, die von anderen Staatsangehörigen zur Erlangung von Titeln vorgelegt wurden). Es ist dabei nicht möglich, den Datenkranz/Gegenstand der Analyse auf bestimmte Daten zu beschränken, da die Behörden eine umfassende Prüfung durchführen und insbesondere unbekannte Strukturen im Verfahren und in der Praxis der Titelerteilung aufdecken möchten. In vielen ausländischen Staaten enthalten dabei gerade die Namen der Antragsteller aufgrund der aus ihnen erkennbaren Informationen über den soziokulturellen Kontext wesentliche Informationen, die für die genannten Untersuchungsaspekte relevant sind.

Mit Hilfe dieser Erkenntnisse sollen zum einen durch das Ableiten von Indikatoren und Parametern das jeweils aufenthaltsrechtliche Verfahren weiterentwickelt, die Verfahren beschleunigt und die Entscheidungsqualität erhöht werden. Die Erkenntnisse sollen zum zweiten in die zukünftige Prüfungsintensität der Einzelfallentscheidungen über einen Antrag auf Erteilung eines Aufenthaltstitels einfließen.

Die dadurch verbesserte Ressourcennutzung dient auch der Schaffung von Kapazitäten zur Beschleunigung der Verfahren in komplexeren Fällen. Eine sich dadurch verbesserte Entscheidungsqualität kann sich in einer einheitlicheren Rechtsanwendung niederschlagen, wenn die Entscheidungspraxen verschiedener Entscheider angeglichen werden können.

Absatz 2 Satz 2 Nummer 1 bis 4 enthält eine abschließende Aufzählung der möglichen Formen der Weiterverarbeitung im Rahmen einer automatisierten Anwendung zur Datenverarbeitung.

Absatz 2 Satz 3 dient der Klarstellung, dass das Verfahrensmonitoring nicht unmittelbar der Einzelfallentscheidung dient und eine Profilbildung im Sinne des Artikels 4 Nummer 4 der Datenschutz-Grundverordnung unzulässig ist.

Zu Absatz 3

Absatz 3 enthält grundrechtsschützende Schranken.

Die Behörden haben sicherzustellen, dass diskriminierende Algorithmen weder entwickelt noch eingesetzt werden. Damit wird dem Risiko algorithmischer Verzerrungen und unzulässiger Ungleichbehandlungen Rechnung getragen.

Zu Absatz 4

Absatz 4 enthält weitere grundrechtsschützende Schranken.

Der Schutz des Kernbereichs privater Lebensgestaltung folgt den verfassungsrechtlichen Vorgaben. Erkenntnisse, die ausschließlich diesen höchstpersönlichen Bereich betreffen, dürfen nicht gewonnen werden. Werden solche Erkenntnisse dennoch erlangt, sind sie unverzüglich zu löschen; die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Eine Verwertung ist ausgeschlossen.

Zu Absatz 5

Soweit beim Einsatz der automatisierten Anwendung zur Datenverarbeitung die Anwendungsbereiche der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) sowie der Verordnung über künstliche Intelligenz eröffnet sind, gelten die entsprechenden Vorgaben unmittelbar und sind bereits beim Design, Training und beim Einsatz zu berücksichtigen. Insbesondere haben die Behörden zum Schutz der Interessen der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen.

Eine zentrale Vorgabe aus der Verordnung über künstliche Intelligenz ist das Risikomanagementsystem nach Artikel 9 der Verordnung über künstliche Intelligenz, das vor 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. Artikel 9 Absatz 2 Buchstabe c der Verordnung über künstliche Intelligenz verpflichtet insbesondere zur fortlaufenden Überwachung der KI-Leistung und zum Umgang mit Abweichungen und Fehlverhalten. Darüber hinaus schreibt Artikel 10 Absatz 2 Buchstabe f der Verordnung über künstliche Intelligenz 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. Nach Artikel 10 Absatz 3 Satz 1 der Verordnung über künstliche Intelligenz müssen die Datensätze ferner „relevant, hinreichend repräsentativ, fehlerfrei und vollständig“ sein – dies ist besonders wichtig zur Vermeidung strukturell benachteiligender Trainingsgrundlagen. Ergänzend verlangt Artikel 13 der Verordnung über künstliche Intelligenz 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. Auch dies dient mittelbar der Kontrolle und Korrektur diskriminierender Tendenzen. Nach Artikel 14 der Verordnung über künstliche Intelligenz muss zudem eine menschliche Aufsicht gewährleistet werden, um beispielsweise potenziell diskriminierende Entscheidungen erkennen und korrigieren zu können. Die Aufsichtspersonen müssen angemessen geschult und befugt sein (Artikel 14 Absatz 4).

Diesen Vorgaben dienen Absatz 3, Absatz 4 und Absatz 5 und verpflichten die Behörden, organisatorische und technische Maßnahmen zu treffen, um den Schutz der Daten sicherzustellen. Das eingesetzte Personal ist besonders zu schulen, um die Funktionsweise der automatisierten Anwendungen, deren Grenzen sowie die datenschutzrechtlichen Anforderungen zu verstehen. Angemessene technische und organisatorische Maßnahmen müssen auch ergriffen werden, um die Daten vor unbefugter Kenntnisnahme zu schützen. Hierzu zählen insbesondere Zugriffsregelungen, Protokollierungen und IT-Sicherheitsmaßnahmen.

Zu Absatz 6

Die Entwicklung und der Betrieb von automatisierten Anwendungen zur Datenverarbeitung, wie KI-Systemen, erfordert den Einsatz hochspezialisierter Expertise, weshalb die Hinzuziehung externer, technisch besonders qualifizierter Unternehmen im Wege der Auftragsverarbeitung notwendig sein kann. Um sicherzustellen, dass die hierbei verarbeiteten personenbezogenen Daten weiterhin dem hohen Schutzniveau der der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) unterliegen, begrenzt Absatz 6 die Einbindung solcher Dritten auf Auftragsverarbeiter mit Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat. Die Dritten dürfen die Daten nicht für eigene Zwecke weiterverarbeiten. Insbesondere dürfen Dritte die personenbezogenen Daten nicht an den Herkunftsstaat der betroffenen Person oder an Stellen, die dem Herkunftsstaat zuzurechnen sind, übermitteln.

Die Übermittlung personenbezogener Daten ist ausschließlich an Amtsträger sowie für den öffentlichen Dienst besonders oder zur Geheimhaltung verpflichtete Personen zulässig. Damit stellt Absatz 6 sicher, dass unbefugte Stellen keinen Zugang zu den sensiblen Daten erhalten und dass der datenschutzrechtliche Schutz über sämtliche Phasen der Entwicklung und des Betriebs der automatisierten Anwendung gewährleistet bleibt, auch wenn hierfür externe Dienstleister eingesetzt werden müssen.

Zu § 90e

§ 90e schafft eine begrenzte Befugnis öffentlich zugängliche personenbezogene Daten aus dem Internet allein mit den Angaben, hinsichtlich derer begründete Zweifel an ihrer Richtigkeit bestehen, automatisiert abzugleichen. Die Vorschrift trägt dem Bedürfnis der zuständigen Behörden Rechnung, bei begründeten Zweifeln an der Richtigkeit von Angaben im Einzelfall effizient und verlässlich zu prüfen, ob öffentlich zugängliche Informationen bestätigende oder widersprüchliche Hinweise enthalten**.**

Zu Absatz 1

Absatz 1 schafft die Rechtsgrundlage für einen automatisierten Abgleich öffentlich zugänglicher personenbezogener Daten aus dem Internet mit den entscheidungserheblichen Angaben hinsichtlich derer begründete Zweifel an ihrer Richtigkeit bestehen, wenn dies im Einzelfall zur Überprüfung der Richtigkeit der Angaben erforderlich ist. Der Abgleich dient allein dazu, die Richtigkeit von bestimmten, im Einzelfall angezweifelten, entscheidungserheblichen Angaben im Antragsverfahren zu überprüfen und enthält keine Vorfestlegung in Bezug auf das Ergebnis der Antragsprüfung.

Den mit der Ausführung des Aufenthaltsgesetzes betrauten Behörden (hierzu wird auf die Begründung zu Artikel 2 Nummer 3 verwiesen) stehen zum Zeitpunkt der Antragstellung in vielen Fällen keine Daten zu den Antragstellenden zur Verfügung, sofern nicht noch Daten aus früheren aufenthaltsrechtlichen Verfahren in den Datenbeständen vorhanden sind. Es fehlt damit die Möglichkeit, die Angaben der Antragstellenden zu verifizieren, sofern im Rahmen der Antragsbearbeitung Auffälligkeiten erkannt werden, die Zweifel an der Richtigkeit der Angaben begründen.

Solche begründeten Zweifel liegen vor, wenn tatsächliche Anhaltspunkte die Richtigkeit der Angaben plausibel infrage stellen. Sie können sich insbesondere im Rahmen der Aufbereitung der Antragsunterlagen oder der Einzelfallbearbeitung ergeben. Ein begründeter Zweifel kann bestehen, wenn die Angaben in sich widersprüchlich sind oder sonst unplausibel sind, etwa wenn die gesprochene Sprache oder der Dialekt nicht zur behaupteten Herkunftsregion passt, der geschilderte Reiseweg im Widerspruch zu den Ein- und Ausreisestempeln oder sonstigen Erkenntnissen steht oder sich die Angaben zu Aufenthaltsorten, familiären Verhältnissen oder der Schul- und Berufslaufbahn im Verlauf des Verfahrens wesentlich ändern. Gleiches gilt, wenn eingereichte Dokumente, etwa behördliche Bescheinigungen, Personenstandsurkunden oder Zeugnisse von Universitäten oder Studiengängen, von vergleichbaren Unterlagen anderer Antragstellender abweichen oder in dieser Form bislang unbekannt sind. Dies kann beispielsweise der Fall sein, wenn Format, Gestaltung oder Sicherheitsmerkmale von bekannten Mustern abweichen, Dokumente ungewöhnliche Schreibweisen oder untypische Stempel aufweisen oder sich Anhaltspunkte dafür ergeben, dass sie nachträglich verändert oder nicht von der angegebenen ausstellenden Stelle herrühren. Ebenso können konkrete Erkenntnisse aus der Beobachtung vergangener Verfahren vorliegen, dass bestimmte Dokumente oder Angaben von bestimmten Orten oder Regionen besonders häufig als falsch aufgefallen sind und daher besonders kritischer Überprüfung bedürfen.

Für den Abgleich können nur die entscheidungserheblichen Angaben herangezogen werden, bei denen begründete Zweifel an der Richtigkeit bestehen. Dies können auch personenbezogene Daten der Antragstellenden sein, die die zuständigen Behörden zur Erfüllung ihrer Aufgaben rechtmäßig erhoben haben und hinsichtlich derer begründete Zweifel an ihrer Richtigkeit bestehen. Hierunter können ebenso besondere Kategorien personenbezogener Daten nach Artikel 9 der Datenschutz-Grundverordnung fallen, sofern der Abgleich dieser Daten zur Aufklärung der Zweifel erforderlich ist. Hiervon ausgenommen sind biometrische Daten (§ 90d Absatz 1 Satz 2 AufenthG). Diese dürfen im Rahmen des automatisierten Internetabgleichs nicht verarbeitet werden. Sofern besondere Kategorien personenbezogener Daten verarbeitet werden, gelten die in § 90d Absatz 5 normierten Schutzmaßnahmen gleichermaßen.

Der Abgleich setzt notwendigerweise die Erhebung öffentlich zugänglicher personenbezogener Daten voraus. Unter öffentlich zugänglichen Daten fallen solche Daten, die von jedermann eingesehen werden können, bei-

spielsweise aus sozialen Medien, soweit sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten. Konkretisierend fallen darunter Daten, die jede Person ohne oder nach vorheriger Registrierung, Genehmigung oder Entgeltzahlung nutzen kann. Nicht umfasst sind Daten, die einer spezifischen Schwelle unterzogen sind, beispielsweise der Einstellung von Daten in sozialen Medien für einen begrenzten Kreis, dessen Zugang einer Kontrolle unterzogen wird. Privatkommunikation über Messenger-Dienste von sozialen Medien kann nicht von der Maßnahme erfasst werden.

Der Abgleich kann mittels einer automatisierten Anwendung zur Datenverarbeitung durchgeführt werden. Für den Begriff der „automatisierten Anwendung“ wird auf Artikel 2 Nummer 3 verwiesen. Im Vergleich zu einer ausschließlich manuellen Recherche ermöglicht der automatisierte Abgleich eine deutlich effizientere, schnellere und einheitliche Auswertung öffentlich zugänglicher Informationen. Es handelt sich dabei um einen methodisch einfachen Datenabgleich. Ausgeschlossen sind komplexe Anwendungen, die nicht auf einem auf den bislang erkennbaren Sachverhalt bezogenen Suchbegriff gründen, sondern darauf zielen, allein statistische Auffälligkeiten in den Datenmengen zu entdecken, die darüber hinaus (automatisiert) in weiteren Abgleichschritten mit bestimmten Datenbeständen verknüpft werden und so zu weiteren Informationen führen können.

Satz 3 stellt klar, dass der automatisierte Abgleich im Einzelfall lediglich ein technisches Unterstützungsinstrument darstellt und keine eigenständige Entscheidungsbefugnis begründet. Die abschließende Bewertung der durch den automatisierten Abgleich generierten Ergebnisse bleibt der zuständigen Stelle nach Überprüfung und Verifizierung durch eine natürliche Person vorbehalten. Damit wird sichergestellt, dass die Entscheidung über die Richtigkeit oder Relevanz der gewonnenen Hinweise stets einer menschlichen Kontrolle unterliegt. Dies ist insbesondere vor dem Hintergrund möglicher Fehlzuordnungen, algorithmischer Verzerrungen oder unvollständiger Datengrundlagen erforderlich. Die Verpflichtung zur manuellen Einordnung und gegebenenfalls notwendigen Verifizierung gewährleistet, dass die Ergebnisse des Abgleichs in den behördlichen Entscheidungsprozess nur nach einer qualifizierten fachlichen Prüfung einfließen dürfen.

Zu Absatz 2

Die Behörden haben organisatorisch und technisch sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Dem Erfordernis tragen ebenso § 90d Absatz 1 Satz 3 und Absatz 5 AufenthG Rechnung.

Zu Absatz 3

Erkenntnisse aus dem Kernbereich privater Lebensgestaltung dürfen weder erhoben noch verwertet werden; werden sie dennoch erlangt, sind sie unverzüglich zu löschen und die Löschung ist zu dokumentieren. Soweit technisch möglich, ist bereits im Vorfeld sicherzustellen, dass kernbereichsrelevante Daten nicht erhoben werden.

Zu Absatz 4

Die im Rahmen des Abgleichs erhobenen Daten dürfen ausschließlich für den Abgleich verwendet werden und sind nach dessen Durchführung unverzüglich zu löschen, sobald sie nicht mehr erforderlich sind. Die durch den Abgleich im Einzelfall gewonnenen Erkenntnisse dürfen nicht zu anderen Zwecken weiterverarbeitet werden. Der Abgleich dient ausschließlich der Überprüfung von Daten im Rahmen der Unterstützung bei der Prüfung eines Antrags auf Erteilung eines Aufenthaltstitels (Einzelfallprüfung). Der Abgleich, sein Ergebnis sowie die Löschung der Daten sind vollständig zu dokumentieren, um Transparenz und Nachvollziehbarkeit zu gewährleisten.

Zu Absatz 5

Absatz 5 stellt klar, dass die Vorgaben des § 90d Absatz 5 und 6 entsprechend gelten. Damit werden sowohl die Anforderungen an die besondere Schulung des eingesetzten Personals als auch die technischen und organisatorischen Maßnahmen zum Schutz der Daten auf den automatisierten Abgleich einschließlich der besonderen Schutzmaßnahmen für Daten nach Artikel 9 der Datenschutz-Grundverordnung übertragen. Zudem gelten die Beschränkungen für den Einsatz externer Auftragsverarbeiter entsprechend.

Zu Artikel 3 (Inkrafttreten)

Artikel 3 bestimmt den Tag des Inkrafttretens.

Anlage 2

Stellungnahme des Bundesrates

Der Bundesrat hat in seiner 1068. Sitzung am 25. September 2026 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. Zu Artikel 1 Nummer 3 (§ 7a Absatz 7 – neu – AsylG), Artikel 2 Nummer 3 (§ 86 Absatz 3 – neu – AufenthG), Nummer 5 (§ 90d Absatz 7 – neu – AufenthG)

   a) Nach Artikel 1 Nummer 3 § 7a Absatz 6 ist der folgende Absatz 7 einzufügen:

   „(7) Verarbeitungstätigkeiten öffentlicher Stellen der Länder, die bereits nach dem jeweiligen Landesrecht zulässig sind, bleiben unberührt."

   b) Artikel 2 ist wie folgt zu ändern:

   aa) Nach Nummer 3 § 86 Absatz 2 ist der folgende Absatz 3 einzufügen:

   „(3) Verarbeitungstätigkeiten öffentlicher Stellen der Länder, die bereits nach dem jeweiligen Landesrecht zulässig sind, bleiben unberührt."

   bb) Nach Nummer 5 § 90d Absatz 6 ist der folgende Absatz 7 einzufügen:

   „(7) Verarbeitungstätigkeiten öffentlicher Stellen der Länder, die bereits nach dem jeweiligen Landesrecht zulässig sind, bleiben unberührt."

   Begründung:

   Landesbehörden, wie die Ausländerbehörden, verarbeiten personenbezogene Daten nach dem jeweiligen Datenschutzgesetz des Landes.

   Soweit durch § 7a AsylG-E, § 86 AufenthG-E und § 90d AufenthG-E Ermächtigungsgrundlagen für die mit der Ausführung des jeweiligen Gesetzes betrauten Behörden zu besonderen Formen der Datenverarbeitung – wie beispielsweise im automatisierten Verfahrensmonitoring – geschaffen werden, entsteht ein Konkurrenzverhältnis zu den Rechtsgrundlagen der Datenverarbeitungen in den Landesgesetzen, soweit diese Rechtsregeln (gleichzeitig) auf denselben Sachverhalt passen.

   So ermöglicht beispielsweise § 11a des Landesdatenschutzgesetzes Baden-Württemberg die Verarbeitung personenbezogener Daten für die Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von KI-Systemen bereits unter den dort bestehenden, weniger eng gefassten Voraussetzungen für die Datenverarbeitung.

   Als fachgesetzliche Regelungen und im Übrigen für spezielle Formen der Datenverarbeitung, wie beispielsweise im Verfahrensmonitoring zum Zweck der Analyse von Verwaltungsverfahren, dürften die Rechtsgrundlagen des Regierungsentwurfs dann Anwendungsvorrang vor den (allgemeinen) datenschutzrechtlichen Regelungen in Landesgesetzen haben (lex specialis derogat legi generali).

   Eine Verdrängung der bestehenden landesrechtlichen Ermächtigungen ist auszuschließen, um die Innovationsfähigkeit der Ausländerverwaltungen der Länder nicht zu beschränken, speziell die Ausländerverwaltung gegenüber anderen Verwaltungszweigen im jeweiligen Land nicht zu benachteiligen und um den föderalen Wettbewerb um die beste Anwendung aufrechtzuerhalten.

   Daher sollte jeweils eingefügt werden, dass Verarbeitungstätigkeiten öffentlicher Stellen der Länder, die bereits nach dem jeweiligen Landesrecht zulässig sind, unberührt bleiben.

2. Zu Artikel 2 Nummer 5 (§ 90e Absatz 1a – neu – AufenthG)

Nach Artikel 2 Nummer 5 § 90e Absatz 1 ist der folgende Absatz 1a einzufügen:

„(1a) Die Maßnahme nach Absatz 1 ist auch zulässig, wenn sie der Gewinnung von Erkenntnissen dient, die für die Feststellung der Identität und Staatsangehörigkeit oder für die Feststellung und Geltendmachung einer Rückführungsmöglichkeit in einen anderen Staat von Bedeutung sein könnten."

Begründung:

Die Ergänzung erweitert die Möglichkeit des automatisierten Abgleichs mit öffentlich zugänglichen Daten aus dem Internet auf Fälle, in denen die hierdurch gewonnenen Erkenntnisse für die Feststellung der Identität und Staatsangehörigkeit des Ausländers oder für die Feststellung und Geltendmachung einer Rückführungsmöglichkeit in einen anderen Staat von Bedeutung sein können.

Die Klärung der Identität und Staatsangehörigkeit sowie die Beschaffung der für eine Rückführung erforderlichen Reisedokumente sind wesentliche Voraussetzungen für die tatsächliche Durchsetzung der Ausreisepflicht. Aufenthaltsbeendende Maßnahmen scheitern in der Praxis häufig oder verzögern sich erheblich, da die Identität oder Staatsangehörigkeit des Ausländers ungeklärt ist oder die für die Rückführung erforderlichen Reisedokumente fehlen. Dies gilt insbesondere, wenn keine oder keine hinreichend aussagekräftigen Identitätsdokumente vorliegen, Angaben zur Person oder Staatsangehörigkeit widersprüchlich sind oder die betroffene Person bei der Identitätsklärung und Passbeschaffung nicht oder nur unzureichend mitwirkt.

Öffentlich zugängliche Informationen im Internet können in solchen Fällen zusätzliche Erkenntnisse liefern, die zur Bestätigung oder Widerlegung vorhandener Angaben oder zur Feststellung weiterer Anknüpfungspunkte für die Identitäts- und Staatsangehörigkeitsklärung beitragen können. Dies können etwa Informationen zu persönlichen, familiären, beruflichen oder sonstigen Bezügen zu einem bestimmten Staat sein. Der Einsatz automatisierter Anwendungen ermöglicht es, die hierfür in Betracht kommenden öffentlich zugänglichen Informationen effizienter auszuwerten. Die auf diesem Weg von den Behörden gewonnenen Erkenntnisse können als wichtiger Sachnachweis dienen, um das für die Rückführung erforderliche Passersatzdokument bei der Vertretung des Herkunftslandes zu beschaffen und in der Folge die Rückführung zu ermöglichen.

Es besteht kein sachlicher Grund, die im Gesetzentwurf vorgesehene Möglichkeit eines solchen automatisierten Abgleichs auf die Überprüfung von Angaben im Zusammenhang mit der Erteilung eines Aufenthaltstitels zu beschränken. Ein vergleichbares, in der Praxis teilweise noch gesteigertes Bedürfnis nach einer effektiven Sachverhaltsaufklärung besteht bei der Vorbereitung und Durchführung aufenthaltsbeendender Maßnahmen. Gerade dort kann die fehlende Klärung von Identität oder Staatsangehörigkeit beziehungsweise das Fehlen erforderlicher Reisedokumente die Aufenthaltsbeendigung erheblich erschweren oder sogar dauerhaft verhindern.

Die Regelung orientiert sich hinsichtlich ihres Zwecks an den bereits im Aufenthaltsgesetz vorgesehenen Maßnahmen zur Feststellung der Identität und Staatsangehörigkeit sowie zur Feststellung und Geltendmachung einer Rückführungsmöglichkeit in einen anderen Staat. Sie ergänzt das bestehende Instrumentarium um die Möglichkeit, hierfür auch öffentlich zugängliche Informationen im Internet unter Einsatz automatisierter Anwendungen auszuwerten.

Die durch die automatisierte Anwendung gewonnenen Erkenntnisse ersetzen nicht die eigenständige Bewertung durch die zuständige Behörde. Sie dienen vielmehr als zusätzliches Hilfsmittel der Sachverhaltsaufklärung und sind von der Behörde einzuordnen und erforderlichenfalls durch weitere Ermittlungen oder Nachweise zu verifizieren. Die für die Maßnahme nach Absatz 1 geltenden Voraussetzungen und Schutzmechanismen bleiben unberührt.

3. Zu Artikel 2 Nummer 5 (§ 90e AufenthG)

Der Bundesrat begrüßt die Schaffung des datenschutzrechtlichen Erlaubnistatbestandes zum Abgleich der personenbezogenen Daten.

Durch § 90e AufenthG-E soll geregelt werden, dass im Einzelfall öffentlich zugängliche personenbezogene Daten aus dem Internet mit entscheidungserheblichen Daten aus dem Antrag auf Erteilung eines Aufenthaltstitels unter den festgelegten Voraussetzungen abgeglichen werden dürfen. In § 90e Absatz 4 AufenthG-E soll dann festgelegt werden, dass die Weiterverarbeitung der beim Abgleich erhobenen Daten zu anderen Zwecken unzulässig ist.

Der Bundesrat bittet um Prüfung, inwieweit eine Zweckänderung bei der Weiterverarbeitung der Daten möglich ist, und bejahendenfalls eine Weiterverarbeitung der Daten zum Zwecke der Strafverfolgung, Gefahrenabwehr sowie für aufenthaltsrechtliche Maßnahmen gesetzgeberisch umzusetzen.

Begründung:

Durch Artikel 6 Absatz 4 Halbsatz 1 DSGVO wird festgelegt, dass eine Rechtssetzung zur zweckverändernden Datenverarbeitung möglich ist (vgl. auch ErwGr 50 Satz 3, 5). Hierzu muss die Rechtsvorschrift eines Mitgliedstaates die in Artikel 23 Absatz 1 DSGVO festgelegten Ziele schützen und eine notwendige und verhältnismäßige Maßnahme sein.

Sicherstellung der festgelegten Ziele

Durch Buchstabe d ermöglicht Artikel 23 Absatz 1 DSGVO eine Beschränkung zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten. Daher ist die Weiterverwendung von personenbezogenen Daten zur Strafverfolgung ein legitimes Ziel.

Die Gefahrenabwehr stellt ein wichtiges Ziel des allgemeinen öffentlichen Interesses der Union und der Bundesrepublik Deutschland dar (Artikel 23 Absatz 1 Buchstabe e DSGVO).

Die Weiterverwendung von personenbezogenen Daten zu ausländerrechtlichen Zwecken lässt sich auf Artikel 23 Absatz 1 Buchstabe c und e DSGVO stützen.

Artikel 23 Absatz 1 Buchstabe c DSGVO erlaubt die Beschränkung zur Sicherstellung der öffentlichen Sicherheit. Die öffentliche Sicherheit ist der Schutz der Integrität von Rechtsgütern und Rechtsnormen. Durch eine unzureichende Datenlage ist die Steuerung und Begrenzung des Zuzugs von Ausländern in die Bundesrepublik Deutschland (§ 1 Absatz 1 Satz 1 AufenthG) gefährdet. Eine Grundvoraussetzung für die durch § 1 Absatz 1 Satz 1 AufenthG festgelegten Ziele ist die Gewinnung von Nachweisen, die für die Feststellung der Identität und Staatsangehörigkeit oder für die Feststellung und Geltendmachung einer Rückführungsmöglichkeit in einen anderen Staat von Bedeutung sein können. Daher stellt die Weiterverarbeitung der personenbezogenen Daten zu diesem Zweck ein legitimes Ziel dar.

Artikel 23 Absatz 1 Buchstabe d DSGVO sieht die Sicherstellung sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaates vor. Durch Artikel 79 Absatz 1 AEUV wird eine Einwanderungspolitik vereinbart, die in allen Phasen eine wirksame Steuerung der Migrationsströme und eine Verhütung sowie verstärkte Bekämpfung von illegaler Einwanderung gewährleistet. Auch die in § 1 Absatz 1 Satz 1 AufenthG festgelegten Ziele zählen zu den allgemeinen öffentlichen Interessen. Der Kompromisstext zur EU-Rückkehrverordnung sieht vor, dass eine wirksame Rückkehrpolitik zentrales Element für ein glaubwürdiges Migrationsmanagement-System ist (ErwGr 1). Der Europäische Rat hat stets betont, wie wichtig entschlossenes Handeln auf allen Ebenen ist, um die Rückkehr aus der Europäischen Union zu erleichtern, zu verstärken und zu beschleunigen (ErwGr 4). Illegale Einwanderung in die Union soll bewältigt und unerlaubte Migrationsbewegungen illegal aufhältiger Drittstaatsangehöriger zwischen Mitgliedstaaten sollen unter Wahrung der Grundrechte verhindert werden (ErwGr 6). Daher sind ausländerrechtliche Maßnahmen ein öffentliches Interesse der Europäischen Union und der Bundesrepublik Deutschland und mithin ein legitimes Ziel.

Der Nachweis der Staatsbürgerschaft bzw. die Identitätsklärung stellt die zuständigen Behörden vor erhebliche Herausforderungen. Dem könnte durch die Weiterverarbeitung der Daten abgeholfen werden.

Notwendigkeit und Verhältnismäßigkeit

Die Schaffung einer entsprechenden Norm zur Weiterverarbeitung der Daten ist zur Erreichung der oben beschriebenen Ziele notwendig. Die ursprüngliche Datenerhebung ist nicht eingriffsintensiv, da es sich um die Erhebung von öffentlichen Daten aus dem Internet handelt. Der Betroffene hat seine Datensouveränität

dahingehend genutzt, die Daten freiwillig in diesem Umfang zur Verarbeitung durch jedermann ins Internet zu stellen. Dies schlägt auf eine Weiterverarbeitung durch. Berechtigte Erwartungen des Betroffenen bei einer öffentlichen Bekanntgabe stehen nicht entgegen. Die gewichtigen öffentlichen Interessen, die in den oben dargelegten Zielen offenbar werden, überwiegen ein eventuell entgegenstehendes Interesse. Dies ist im Bereich der Strafverfolgung und Gefahrenabwehr, insbesondere zum Schutz der Rechtsgüter Leib, Leben und Freiheit, selbstredend („Datenschutz ist nicht Tatenschutz“). Auch im Bereich des Ausländerrechts überwiegt das besonders ausgeprägte öffentliche Interesse an der Umsetzung gesetzmäßiger Zustände. Es besteht kein schutzwürdiges Interesse daran, öffentlich zugänglich gemachte Daten nicht zu verwenden, um bspw. die Umsetzung einer Ausreisepflicht zu realisieren.

Das Datenschutzniveau ändert sich zwischen Verarbeitung und Weiterverarbeitung nicht, da diese durch dieselbe öffentliche Stelle vorgenommen werden.

Die Norm selbst lässt sich so ausgestalten, dass Einzelfallgerechtigkeit und Verhältnismäßigkeit gewahrt sind.

Anlage 3

Gegenäußerung der Bundesregierung

Die Bundesregierung äußert sich zur Stellungnahme des Bundesrates vom 25. September 2026 wie folgt:

Zu Nummer 1 (Zu Artikel 1 Nummer 3 (§ 7a Absatz 7 – neu – AsylG), Artikel 2 Nummer 3 (§ 86 Absatz 3 – neu – AufenthG), Nummer 5 (§ 90d Absatz 7 – neu – AufenthG)):

Die Bundesregierung begrüßt grundsätzlich das Anliegen, innovative Lösungen zu ermöglichen, ohne dabei die Effizienz und Modernisierungsfähigkeit der Ausländerbehörden zu beeinträchtigen. Sie teilt grundsätzlich das Anliegen, dass diese Behörden im Vergleich zu anderen Verwaltungsbereichen innerhalb desselben Landes keine strukturellen Nachteile erfahren sollen.

Die Bundesregierung wird den Vorschlag prüfen.

Zu Nummer 2 (Zu Artikel 2 Nummer 5 (§ 90e Absatz 1a – neu – AufenthG)):

Die Feststellung der Identität und Staatsangehörigkeit sowie die Ermittlung von Rückführungsmöglichkeiten sind für einen wirksamen Vollzug des Aufenthaltsrechts von erheblicher Bedeutung. Das Bundesministerium des Innern prüft daher bereits, inwieweit hierfür künftig Möglichkeiten eines automatisierten Internetdatenabgleichs zur Feststellung der Identität und Staatsangehörigkeit im Aufenthaltsgesetz geschaffen werden können.

Zu Nummer 3 (Zu Artikel 2 Nummer 5 (§ 90e AufenthG)):

Der Bundesrat bittet um Prüfung, inwieweit eine Zweckänderung bei der Weiterverarbeitung der nach § 90e Absatz 1 AufenthG-E erhobenen Daten möglich ist. Die Weiterverarbeitung neu gewonnener Daten für weitere aufenthaltsrechtliche Maßnahmen sowie andere Zwecke ist im Gesetzentwurf unter Berücksichtigung grundrechtlicher und datenschutzrechtlicher Erwägungen nicht vorgesehen. Die Bundesregierung wird den Vorschlag prüfen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333