21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)167 F
vom 4. Mai 2026

Schriftliche Stellungnahme

von Prof. Dr. Sarah Rachut, Direktorin des Instituts für Rechtswissenschaften, Technische Universität Braunschweig vom 3. Mai 2026

Öffentliche Anhörung

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Weiterentwicklung der Digitalisierung in der Migrationsverwaltung

BT-Drucksache 21/4080

Technische Universität
Braunschweig
Institut für Rechtswissenschaften
Bienroder Weg 87
38106 Braunschweig

Prof. Dr. Sarah Rachut
Direktorin

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

Datum: 03. Mai 2026

Gutachterliche Stellungnahme

für den Innenausschuss
des Deutschen Bundestages

zum Entwurf eines Gesetzes zur Weiterentwicklung der Digitalisierung in der Migrationsverwaltung
(Migrationsverwaltungsdigitalisierungs-weiterentwicklungsgesetz – MDWG)

BT-Drucksache 21/4080

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

Inhalt

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

Vorbemerkung

Der Gesetzentwurf für ein Migrationsverwaltungsdigitalisierungsweiterentwicklungsgesetz (MDWG-E) tangiert eine Vielzahl von tatsächlichen und rechtlichen Fragestellungen. Ausgehend von der Expertise der Verfasserin und der Kurzfristigkeit der Anfrage konzentriert sich die gutachterliche Stellungnahme auf **ausgewählte datenrechtliche Aspekte des Gesetzentwurfs**.

Gegenstand der Stellungnahme sind (B.) die geplante Speicherung weiterer Daten (u.a. im Ausländerzentralregister) sowie (C.) die Zweckerweiterung ihrer Verarbeitung in Form einer Wiederverwendung iRv. elektronischen Aufenthaltstiteln. Darüber hinaus werden weitere Potentiale des Gesetzentwurfs mit Blick auf eine zunehmend digitale Verwaltung beleuchtet (D.) und schließlich ausgewählte Themenfelder in einem Ausblick (E.) erläutert. Bezüglich der rechtlichen Einordnung von Registerzusammenführung, automatischem Datenabruf und Datenaustausch verweise ich zudem auf die gutachterliche Stellungnahme von Prof. Dr. Dirk Heckmann.

Ausdrücklich **nicht betrachtet** wurden Fragen des Migrations- und Asylrechts. Eine verfassungsrechtliche Gesamtbewertung hinsichtlich des Zusammenwirkens der verschiedenen neuen Normen konnte im Rahmen dieser Stellungnahme ebenfalls nicht geleistet werden.

A. Einleitung

Der vorliegende Entwurf eines Gesetzes zur Weiterentwicklung der Digitalisierung in der Migrationsverwaltung (MDWG-E) **adressiert aktuelle administrative Herausforderungen** der Migrationsverwaltung. Kernaspekte der geplanten Neuregelung betreffen die bessere, einfachere und medienbruchfreie Kommunikation der beteiligten Behörden sowie Entlastungen der Bürgerinnen und Bürger bei der Antragstellung auf Verlängerung oder Änderung eines elektronischen Aufenthaltstitels. Dies soll primär durch die Speicherung zusätzlicher Informationen im Ausländerzentralregister (AZR), die Vereinheitlichung von Datenaustauschformaten und die rechtliche Ermächtigung zum Datenaustausch zwischen Behörden erfolgen.

Die **Intention** des MDWG-E, Entlastung innerhalb der Migrationsverwaltung sowie für die Betroffenen durch Bürokratieabbau (u.a. Prozessvereinfachung und Standards) zu schaffen, ist **zu begrüßen**. Weiter positiv hervorzuheben ist, dass im Rahmen der Entwurfserarbeitung ein **Digitalcheck**[1] durchgeführt wurde und somit die Digitaltauglichkeit, d.h. die Möglichkeiten zum digitalen Vollzug der Normen anhand eines erprobten Methodenkatalogs, berücksichtigt wurde.[2]

[1] https://digitalcheck.bund.de/.

[2] BT-Drs. 21/4080, Anlage 2.

Zugleich gilt es zu beachten, dass jede Verarbeitung von Daten und insbesondere die Zusammenführung besonders sensibler Daten (wie biometrische Lichtbilder oder Fingerabdrücke) in den Rechtskreis der Betroffenen hineinwirkt, (technische) Angriffspunkte erzeugt und Missbrauchspotentiale schafft. Diesen Risiken ist durch regulatorische Ausgestaltung, technische und organisatorische Maßnahmen sowie eine kontinuierliche Evaluation der neuen Prozesse zu begegnen.

Als Artikelgesetz sieht das MDWG-E in 14 Artikeln zahlreiche, v.a. punktuelle Änderungen verschiedener Gesetze und Verordnungen (inkl. ihrer Anlagen) vor, die in dieser Stellungnahme nicht vollständig thematisiert werden können. Entsprechend werden die hier betrachteten zentralen Regelungsvorhaben aus dem Ausländerzentralregistergesetz (AZRG), der dazugehörigen Durchführungsverordnung (AZRG-DV), dem Aufenthaltsgesetz (AufenthG) und der diesbezüglichen Verordnung (AufenthV) thematisch zusammengefasst betrachtet.

B. Verarbeitung biometrischer Daten (insb. Visadatei) & Identitätsklärung

Ein zentrales Anliegen des MDWG-E betrifft die Verarbeitung biometrischer Daten und eine damit verbundene Identitätsklärung. Dies adressieren insbesondere folgende Regelungen:

- § 3 Abs. 1 Nr. 4 AZRG-neu: Speicherung der „Angaben zur Identitätsklärung“ als Grundpersonalien
- § 3 Abs. 1 Nr. 11 AZRG-neu: Speicherung von Fingerabdrücken und Unterschrift
- § 6 Abs. 5 Nr. 7 AZRG-neu: Übermittlung von weiteren zur Identitätsabklärung geeigneten Dokumenten bei bestimmten Speichervorgängen
- § 29 Nr. 4 AZRG-neu: Speicherung der Fingerabdruckdaten in der Visadatei bei Erteilung eines Visums
- § 29 Nr. 4a AZRG-neu: Speicherung weiterer, die Erteilung eines nationalen Visums begründenden Unterlagen in der Visadatei
- § 19 AZRG-DV-neu: Löschung und Löschfristen für Daten der Visadatei

Das Ausländerzentralregister (AZR) ist ein vom Bundesamt für Migration und Flüchtlinge geführtes Register und besteht aus einem allgemeinen Datenbestand und einer gesondert geführten Visadatei, § 1 Abs. 1 AZRG. In der Visadatei werden Daten von ausländischen Personen gespeichert, die ein Visum bei einer deutschen Auslandsvertretung beantragen.

Durch die Speicherung biometrischer Daten in Form von Fingerabdruckdaten sowie Unterschriftsdaten und weiterer für die Identitätsabklärung geeigneter Daten im allgemeinen Datenbestand und in der Visadatei soll die Identitätsklärung für verschiedene Behörden erleichtert werden. Das Ziel, die Notwendigkeit des persönlichen Erscheinens bei der Antragstellung auf Verlängerung oder Änderung eines elektronischen Aufenthaltstitels entbehrlich zu machen, wird durch Änderungen des AufenthG verfolgt (s. C.).

I. Speicherung zusätzlicher (biometrischer) Daten

Die **Speicherung** von personenbezogenen Daten stellt selbst eine **datenschutzrechtlich relevante Verarbeitung** dar und bedarf daher einer entsprechenden Rechtfertigung nach Art. 6 DS-GVO. Werden besondere Kategorien personenbezogener Daten gespeichert, so sind die strengeren Vorgaben des Art. 9 DS-GVO zu berücksichtigen.

Als solche **besonders sensiblen personenbezogenen Daten** zählen gem. Art. 9 Abs. 1 DS-GVO Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. „Biometrischen Daten zur eindeutigen Identifizierung“ umfassen gem. Art. 4 Nr. 14 DS-GVO daktyloskopische Daten, sowie solche mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen.

Entsprechend sind die künftig in der Visadatei zu speichernden Fingerabdruckdaten als biometrische Daten zu klassifizieren. Gleiches kann für die Unterschriftsdaten gelten, wenn diese in der Praxis „mit speziellen technischen Verfahren“ gewonnen werden, um die eindeutige Identifizierung zu ermöglichen bzw. zu bestätigen. Die weiteren – durch den Gesetzentwurf – nicht näher spezifizierten Daten aus zur Identitätsabklärung geeigneten Dokumenten dürften im Regelfall nicht als biometrische Daten zu klassifizieren sein, da sie die von Art. 4 Nr. 14 DS-GVO aufgestellten drei Kriterien (Methode: spezielles technisches Verfahren, Zweck: eindeutiges Identifizieren und Art: physische, physiologische oder verhaltenstypische Merkmale)[3] nicht erfüllen.

Durch das **MDWG-E** sollen die gem. Art. 6 Abs. 1 lit. e, Abs. 3 DS-GVO bzw. Art. 9 Abs. 2 lit. g DS-GVO notwendigen **datenschutzrechtlichen Rechtsgrundlagen** für die Verarbeitung (Speicherung) geschaffen werden. Die – für die Fingerabdruckdaten maßgebliche – strengere Vorgabe des Art. 9 DS-GVO sieht vor, dass die rechtliche Vorgabe der Speicherung aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist und in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht.

[3] BeckOK DatenschutzR/Albers/Veit, 55. Ed. 1.2.2026, DS-GVO Art. 9 Rn. 44.

Die Speicherung von Fingerabdruckdaten aufgrund einer nationalen gesetzlichen Grundlage ist daher möglich. Auch besteht im vorliegenden Fall mit einer funktionierenden Identitätsfeststellung sowie der Aufrechterhaltung der Leistungsfähigkeit der Asylverwaltung ein **erhebliches öffentliches Interesse**, das diese Verarbeitung grundsätzlich rechtfertigen kann. Die hiermit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG) bzw. das Recht auf Schutz der personenbezogenen Daten (Art. 8 EU-GrCh) müssen jedoch einer **Verhältnismäßigkeitsprüfung** standhalten. Zu berücksichtigen sind hierbei insbesondere die Risiken, die sich aus der **zentralen Speicherung im AZR** (allgemeiner Datenbestand und Visadatei) ergeben und die Daten für einen großen Personenkreis über verschiedene Behörden zugänglich machen. Dadurch steigt nicht nur das (interne) Missbrauchspotential, sondern zugleich wird der Datenbestand in seiner Gesamtheit auch für mögliche externe Angreifer „attraktiver". Bereits aus **IT-sicherheitsrechtlicher Sicht** gelten daher für solche Datenbestände grundsätzlich **höhere Anforderungen**, da die Auswirkungen eines IT-Sicherheitsvorfalls ungleich höher wären. Weiter ist schon jetzt zu beachten, dass die Schaffung eines solchen zentralen Datenbestandes den Weg für eine künftig noch eingriffsintensivere Verarbeitung ebnet. Diese Entwicklungen laufen zudem dem **Grundsatz der Datenminimierung** (Art. 5 Abs. 1 lit. c DS-GVO) zuwider. Ausweislich der Entwurfsbegründung[4] sollen umfassende Protokollierungspflichten, Stichproben bei automatisierten Abrufen, das Datenschutzcockpit nach § 34 Abs. 6 S. 1 AZRG sowie die strafrechtliche Verfolgbarkeit von Datenmissbrauch als Schutzmaßnahmen dienen.

Dabei ist zu berücksichtigen, dass auch das Persönlichkeitsrecht nicht uneingeschränkt gilt, sich ein „Recht auf ein analoges Leben" in Form eines Abwehrrechts gegen jegliche Verarbeitung der eigenen personenbezogenen Daten gerade nicht aus den Grundrechten ableiten lässt.[5] Die Ausgestaltung anhand der oben genannten Grundsätze obliegt daher dem gesetzgeberischen Ermessensspielraum.

Insgesamt erscheint es, ob der deutlich gestiegenen Risiken, die mit der invasiven Verarbeitung biometrischer Daten in einem zentralen Register einhergehen, **fraglich, ob** diese durch den bisherigen Gesetzentwurf **verhältnismäßige Ausgleichsmechanismen** erfahren.

Unklar bleibt zudem, auf welche Daten sich die Ermächtigung zur Speicherung von weiteren zur Identitätsabklärung geeigneten Dokumenten erstreckt.

II. Löschung der (biometrischen) Daten

Zentral für die Verhältnismäßigkeit der Rechtsgrundlage zur Speicherung biometrischer Daten sind die vorgesehenen Löschfristen. Diese tragen weiter den Grundsätzen der Datenminimierung und Speicherbegrenzung (Art. 5 Abs. 1 lit. c, e DS-GVO) Rechnung. Insoweit ist es kritisch zu sehen, dass die zentralen Regelungen zur Löschung mit § 19 AZRG-DV-neu auf die untergesetzliche Ebene einer

[4] BT-Drs. 21/4080, S. 65.

[5] *Heckmann*, Grundrecht auf IT-Abwehr?, MMR 2006, S. 3, 6; *Botta*, „Digital First" und „Digital Only" in der öffentlichen Verwaltung, NVwZ 2022, S. 1247, 1250 ff.; *Rachut*, Grundrechtsverwirklichung in digitalen Kontexten, 2025, S. 248 ff.

Durchführungsverordnung verschoben werden. Hier wäre angesichts der Verarbeitung besonders sensibler personenbezogener Daten und der mit dieser zentralen Speicherung im AZR einhergehenden Risiken eine **gesetzliche Vorgabe vorzuziehen**. Gem. § 19 Abs. 1 S. 1 AZRG-DV-neu sind Datensätze in der Visadatei spätestens nach fünf Jahren zu löschen. Ausnahmen gelten gem. § 19 Abs. 1 S. 2 AZRG-DV-neu für Angehörige bestimmter Staaten (diese werden vom Bundesministerium des Innern im Einvernehmen mit dem Auswärtigen Amt festgelegt). Diese Datensätze sind erst nach zehn Jahren zu löschen. Eine kürzere Löschfrist von drei Jahren ist für gem. § 29 Nr. 4a AZRG-neu in der Visadatei gespeicherte weitere, die Erteilung eines nationalen Visums begründende Unterlagen vorgesehen. Aus Gründen des im Datenschutzrecht geltenden **Zweckbindungsgrundsatzes** sollte zudem normativ klargestellt werden, dass eine Löschung bereits vor Ablauf dieses Zeitraums zu erfolgen hat, wenn der Zweck der Speicherung nicht mehr besteht. Dies wird bisher nur mittelbar durch „spätestens […] zu löschen“ ausgedrückt.

C. Wiederverwendung iRv elektronischen Aufenthaltstiteln

Ein weiteres Anliegen des MDWG-E ist die Möglichkeit, Lichtbild, Fingerabdrücke und Unterschrift bei einer erneuten Antragstellung nach dem AufenthG wiederverwenden zu können und so eine wiederholte persönliche Vorstellung der Antragstellenden entbehrlich zu machen.

Dies adressieren insbesondere folgende Regelungen:

- § 49 Abs. 6a AufenthG-neu: Möglichkeit der Identitätsfeststellung bei der Beantragung eines nationalen Visums aufgrund bereits von einer deutschen Auslandsvertretung abgenommener Lichtbilder und Fingerabdrücke
- § 82 Abs. 5 S. 2 AufenthG-neu: Datenverarbeitungsermächtigung für die erneute Ausstellung der Dokumente
- § 99 Nr. 13 AufenthG-neu: Erweiterung der Verordnungsermächtigung auf Vorgaben bzgl. verwendender Vordrucke hinsichtlich „Unterschriften“
- § 61a AufenthV-neu: Löschfristen für bei der Ausländerbehörde gespeicherte Fingerabdrücke, Lichtbild und Unterschrift

Die zuständigen Ausländerbehörden sind für den Vollzug des AufenthG ebenfalls auf eine Identitätsfeststellung angewiesen. **§ 49 Abs. 1 AufenthG stellt die zentrale Rechtsgrundlage für die Datenverarbeitung** der zuständigen Behörden beim Vollzug dieses Gesetzes dar. Um dem vorbenannten Regelungsziel gerecht zu werden, ist der Verarbeitungszweck der erhobenen Daten auf die spätere Verarbeitung im Rahmen einer (erneuten) Antragstellung und einer erneuten Ausstellung von Dokumenten (z.B. bei Verlängerung oder Änderung eines elektronischen Aufenthaltstitels) auszuweiten. Personenbezogene Daten dürfen grundsätzlich nur für festgelegte, eindeutige und legitime Zwecke, Art. 5 Abs. 1 lit. b DS-GVO (**Zweckbindungsgrundsatz**), verarbeitet werden. Die hierfür notwendigen gesetzlichen Grundlagen – die eine Verarbeitung auf die benannten Zwecke ausweiten – werden durch § 49 Abs. 6a AufenthG-neu und § 82 Abs. 5 S. 2 AufenthG-neu geschaffen.

Die in § 61a AufenthV-neu aufgestellten **Vorgaben für die Speicherung und Löschung** für bei der Ausländerbehörde gespeicherte Fingerabdrücke, das Lichtbild und die Unterschrift sind für die Umsetzung von § 82 Abs. 5 S. 2 AufenthG-neu erforderlich. Hinsichtlich der datenschutzrechtlichen Maßstäbe sowie den Einwand gegen eine Normierung auf Verordnungsebene s.o. (B.). Die vorgesehene Speicherdauer von fünf (Minderjährige) bzw. sieben Jahren (Erwachsene) soll die erneute Erhebung von Fingerabdrücken, Lichtbild und Unterschrift in einer Vielzahl von Fällen entbehrlich machen und so zur Entlastung beitragen. Diese Annahme fußt auf einer Prognose und ist grundsätzlich von der Einschätzungsprärogative des Gesetzgebers gedeckt. Indes sollte diese künftig überprüft werden, um die Geeignetheit einer kürzeren Speicherdauer bewerten zu können.

D. Digitale Verfahren

Dass im Rahmen der Entwurfserstellung bereits die **Digitaltauglichkeit** der Regelungen angedacht wurde, ist sehr zu begrüßen.

In weiteren Normen, wie z.B. **§ 68 Abs. 2 AufenthG-neu**, zeigt sich, dass digitale Verfahren auch weiteren Beteiligten zugutekommen können und Potentiale digitaler Verfahren in diesem Kontext weitergedacht wurden. Die Norm schafft die Möglichkeit, die Verpflichtungserklärung zur Haftungsübernahme für den Lebensunterhalt eines anderen künftig auch elektronisch abgeben zu können. § 68 Abs. 2 AufenthG sah bisher ausschließlich „Schriftform“ vor. Durch die ausdrückliche Zulässigkeit der elektronischen Form als Alternative werden **Rechtsunsicherheiten bzgl. eines Schriftformersatzes** nach § 126a BGB (mM § 3a Abs. 2, 3 VwVfG) **beseitigt**. Die Abgabe der aufenthaltsrechtlichen Verpflichtungserklärung stellt nach hM eine einseitige empfangsbedürftige Willenserklärung dar, die (im Wesentlichen) einem zivilrechtlichen Schuldversprechen im Sinne des § 780 BGB entspricht.[6] Eine Erklärung nach § 780 BGB hat in Form der „schriftlich[en] Erteilung des Versprechens“ zu erfolgen, wobei gem. § 780 S. 2 BGB die elektronische Form ausgeschlossen ist. Hinsichtlich der Verpflichtungserklärung aus § 68 AufenthG war somit fraglich, inwieweit die Einschränkung des § 780 S. 2 BGB (der Sache nach oder im Ergebnis) zu übernehmen war.[7]

Der angefügte § 68 Abs. 2 S. AufenthG-neu „Wird die Erklärung elektronisch abgegeben, ist die die Erklärung abgebende Person durch geeignete Maßnahmen vor einer übereilten Abgabe der Erklärung zu warnen.“ verdeutlicht, dass man sich mit den verschiedenen Funktionen eines (bisherigen) Formerfordernisses[8] auseinandergesetzt hat.[9] Aufgrund der mit der Verpflichtungserklärung nach § 68 AufenthG einhergehenden weitreichenden Haftungsverpflichtung und des dazugehörigen Risikos erscheint ein Formerfordernis mit einer **Warnfunktion** generell erforderlich.

---

[6] Vgl. BVerwG, Urt. v. 24.11.1998 – 1 C 33.97; BeckOK AuslR/Kluth, 47. Ed. 1.1.2026, AufenthG § 68 Rn. 7 mwN.

[7] Vgl. z.B. VGH Mannheim, Urt. v. 07.12.2022 – 11 S 148/22.

[8] S. allgemein zur Bedeutung von Formvorschriften im Rechtsverkehr BeckOK BGB/Wendtland BGB § 125 Rn. 1 mwN.

[9] BT-Drs. 21/4080, S. 74.

Durch § 68 Abs. 2 S. AufenthG-neu wird sichergestellt, dass auch bei einer von überall und zu jeder Zeit möglichen elektronischen Erklärung dem Erklärenden die Bedeutung seiner Entscheidung bewusst gemacht wird. Darüber hinaus trägt die ausdrückliche Zulassung der elektronischen Form dem **gewandelten Kommunikationsverständnis** Rechnung. War es früher unüblich Rechtsgeschäfte, insbesondere solche mit großer Tragweite elektronisch vorzunehmen, hat sich dies inzwischen gewandelt und die schriftliche und elektronische Form sind in vielen Bereichen des Alltags- und Geschäftslebens gleichberechtigt.[10] Dies zeigt sich nicht zuletzt in den Neuregelungen des Onlinezugangsgesetzes (OZG), die auf eine zunehmend elektronische Abwicklung von Verwaltungsleistungen abzielen, wobei sich mit § 9a OZG zentrale Vorgaben für die elektronische Abwicklung über Verwaltungsportale und Schriftformersatz finden.[11]

In seiner Stellungnahme vom 30.01.2026[12] hat der Bundesrat zudem angeregt, die Antragstellung nach § 81 AufenthG (Beantragung des Aufenthaltstitels) und antrags- oder sonstige Verfahrenshandlungen nach dem StAG künftig **im Regelfall** als **digitale Antragstellung** vorzusehen („soll die Vornahme dieser Verfahrenshandlungen über diesen digitalen Verwaltungsdienst erfolgen"). Durch die Soll-Vorschrift wird ausgedrückt, dass die Antragstellung „soweit […] ein digitaler Verwaltungsdienst nach dem Onlinezugangsgesetz oder ein sonstiger von einer zuständigen Behörde bereitgestellter digitaler Verwaltungsdienst zur Verfügung steht" digital zu erfolgen hat, es sei denn, der Einzelfall gebietet aufgrund bestimmter Umstände eine Abweichung. Im Kontext des seit mehreren Jahrzehnten verfolgten Ansatzes des E-Governments und den in den letzten Jahren verstärkten Bemühungen, Verwaltungsleistungen elektronisch bzw. digital anzubieten, erscheint der Vorstoß des Bundesrates konsequent. Hierbei muss berücksichtigt werden, dass eine digitale Verwaltung nicht nur wünschenswert, sondern zunehmend notwendig ist, um den veränderten Realbedingungen (regulatorische und tatsächliche Komplexität, Herausforderungen für den Rechtsstaat, demographischer Wandel, Veränderungen in Selbstverständnis und Erwartungshaltung usw.) Rechnung zu tragen und die Funktionsfähigkeit von Staat und Verwaltung langfristig aufrechterhalten zu können.[13] Insoweit Bürgerinnen und Bürgern ein bestimmtes Verfahren (hier das digitale bzw. elektronische[14]) vorgeschrieben werden soll, ist aus Gründen des Rechtsstaatsprinzips und des allgemeinen Gleichheitsgrundsatzes, Art. 3 Abs. 1 GG, darauf zu achten, dass dies nicht unverhältnismäßig den Zugang zum Staat bzw. staatlichen Leistungen und auch nicht für bestimmte Personengruppen einschränkt. Die Frage, ob „digital-only" bzw. „digital-first"[15] rechtlich möglich ist, ist daher nach den tatsächlichen Begebenheiten zu beurteilen. Ein Recht auf analoge Verfahren oder

---

[10] Vgl. BT-Drs. 21/4080, S. 74.

[11] Ausweislich der Gesetzesbegründung orientiert sich § 68 S. 2 AufenthG-neu an den Vorgaben des § 9a OZG, BT-Drs. 21/4080, S. 74.

[12] BT-Drs. 21/4080, Anlage 3.

[13] Grundsätzlich hierzu *Rachut/Heckmann*, Verwaltungsdigitalisierung de lege lata und de lege ferenda – Auf dem Weg zu einem impulsgesteuerten Verwaltungsverfahren, VerwArch 2025, S. 133 ff.

[14] Zur Synonymität der Begriffe im deutschen Verwaltungsrecht s. *Rachut*, Grundrechtsverwirklichung in digitalen Kontexten, 2025, S. 184 ff.

[15] Zu diesen Begriffen s. *Botta*, „Digital First" und „Digital Only" in der öffentlichen Verwaltung, NVwZ 2022, S. 1247 ff.

ein Abwehrrecht gegen jede elektronische Verarbeitung personenbezogener Daten lässt sich aus den Grundrechten nicht ableiten.[16] Die durch den Bundesrat vorgebrachten Anregungen enthalten die Einschränkung der technischen Verfügbarkeit und durch die Ausgestaltung als Sollvorschrift einen **aus Verhältnismäßigkeitsgesichtspunkten notwendigen Ermessensspielraum** für Härtefälle. Darüber hinaus müsste sichergestellt werden, dass die Antragstellenden die tatsächlichen Gegebenheiten vorfinden, um Anträge digital zu stellen. Dies umfasst die dafür notwendige Infrastruktur sowie eine entsprechende digitale Kompetenz. Weiter wäre zu beurteilen, ob die Antragstellenden insgesamt oder Teile hiervon durch einen Wechsel auf die digitale Form benachteiligt und etwa unverhältnismäßig hohe Verfahrenshürden aufgestellt würden. Ebenso ist es denkbar, dass digitale Antragsverfahren den Zugang zum Recht für bestimmte Personengruppen vereinfachen können.[17] Erfreulicherweise hat die Bundesregierung in ihrer Stellungnahme[18] bereits angegeben, diesen Regelungsvorschlag prüfen zu wollen.

E. Ausblick

Insoweit der Gesetzentwurf auf das laufende **Gesetzgebungsverfahren zur besseren Verhinderung missbräuchlicher Anerkennungen der Vaterschaft (BT-Drs. 21/4081)** Bezug nimmt und diesbezügliche Regelungen trifft, verweise ich an dieser Stelle auf die grundlegende verfassungsrechtliche Kritik der Sachverständigen in der Anhörung vom 23.03.2026.[19]

Bei der Umsetzung können die vom Normenkontrollrat gemachten Anregungen zum **Föderalen Informationsmanagement** (FIM) wertvoll sein. Deren Umsetzung wurde ausweislich der Stellungnahme des Normenkontrollrats bereits angestoßen.[20]

Mit dem MDWG-E werden vielfältige Herausforderungen in der Praxis (z.B. bei der Identitätsfeststellung, bei der Informationsübermittlung) adressiert und neue Rechtsgrundlagen für Datenverarbeitung (Speicherung, Übermittlung, Verarbeitung zu erweiterten Zwecken) geschaffen. Die mit der weitreichenderen Datenverarbeitung einhergehenden Einwirkungen auf die Persönlichkeitsrechte der Betroffenen unterliegen indes Rechtfertigungsanforderungen. Folglich sollten die mit dem MDWG-E verfolgten Ziele nach einer angemessenen Zeit evaluiert und bewertet werden (**Wirksamkeitsbetrachtung**), ob die Zielerreichung die vorgesehenen Datenverarbeitungen tatsächlich rechtfertigt.

---

[16] *Heckmann*, Grundrecht auf IT-Abwehr?, MMR 2006, S. 3, 6; *Botta*, „Digital First“ und „Digital Only“ in der öffentlichen Verwaltung, NVwZ 2022, S. 1247, 1250 ff.; *Rachut*, Grundrechtsverwirklichung in digitalen Kontexten, 2025, S. 248 ff.

[17] *Heckmann*, Grundrecht auf IT-Abwehr?, MMR 2006, S. 3, 6.

[18] BT-Drs. 21/4080, Anlage 4.

[19] Insbesondere *von Scheliha* und *Chebout.*

[20] BT-Drs. 21/4080, Anlage 2.

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

F. Fazit und Empfehlungen

1. Die **Zielsetzung** des MDWG-E, die Migrationsverwaltung durch bessere, einfachere und medienbruchfreie Kommunikation effizienter zu gestalten sowie Bürgerinnen und Bürger bei der Antragstellung auf Verlängerung oder Änderung eines elektronischen Aufenthaltstitels zu entlasten, ist **begrüßenswert**.

2. Die hierfür **geplanten rechtlichen Regelungen**, die die Speicherung zusätzlicher Informationen im Ausländerzentralregister (AZR), die Vereinheitlichung von Datenaustauschformaten und die Ermächtigung zum Datenaustausch zwischen Behörden ermöglichen, erscheinen für diese Zwecke grundsätzlich **sinnvoll und geeignet.**

3. Hinsichtlich der im AZRG-neu und AufenthG-neu zu schaffenden Rechtsgrundlagen für die weitere Verarbeitung personenbezogener Daten ist zu beachten, dass diese einen verhältnismäßigen Ausgleich zwischen der oben benannten Zweckverfolgung und dem Schutz der Persönlichkeitsrechte der Betroffenen schaffen. Für die Verarbeitung von besonders sensiblen Daten wie Fingerabdruckdaten (und weiterer biometrischer Daten) gelten hierbei die höheren Anforderungen des Art. 9 Abs. 2 DS-GVO. Es ist fraglich, ob die mit der zentralen Speicherung weiterer – auch besonders sensibler – Daten im Ausländerzentralregister einhergehenden Risiken durch den vorliegenden Gesetzentwurf bereits ausreichend adressiert werden. **Vorzugswürdig** wäre insbesondere, dass die **Löschfristen auf gesetzlicher** (und nicht wie vorgesehen auf untergesetzlicher) **Ebene** normiert würden.

4. Um die Potentiale der mit dem MDWG-E gelegten Grundlagen in Form digitaler Verfahren weiter nutzen zu können, sollten die Anregungen des Normenkontrollrats zum Föderalen Informationsmanagement (FIM) weiterverfolgt und der **Vorschlag des Bundesrates zur digitalen Antragstellung** aufgegriffen werden.

5. Punktuell enthält der Gesetzentwurf noch **redaktionelle Fehler**, die es auszubessern gilt. Außerdem sollten **Begriffe** (etwa „Fingerabdruckdaten“ und „Fingerabdrücke“) **vereinheitlicht** werden.

6. Angesichts der geplanten Ausweitung der Datenverarbeitung sollte eine zeitnahe **Evaluation** der mit dem MDWG-E verfolgten Maßnahmen erfolgen, um bewerten zu können, ob die gewünschten Effizienzgewinne erzielt werden konnten und ob und welche weniger eingriffsinvasiven Verarbeitungsprozesse (z.B. kürzere Speicherdauern) gleichfalls geeignet wären.