

Fachbeiträge

Das Gesetz zur Weiterentwicklung der Digitalisierung in der Migrationsverwaltung als Instrument der Verwaltungsmodernisierung im Ausländerrecht? – Eine Analyse

Stephanie Tonn*

Das Bundeskabinett hat am 18.12.2024 das »Gesetz zur Weiterentwicklung in der Digitalisierung der Migrationsverwaltung« (MDWG) als Formulierungshilfe für die Regierungskoalition beschlossen. Das Vorhaben hatte zum Ziel, Hindernisse zu überwinden, die der weiteren Digitalisierung von Arbeitsprozessen in der Migrationsverwaltung im Weg stehen. In einer entsprechenden Pressemitteilung des Bundesministeriums des Innern und für Heimat (BMI) hieß es dazu: »Wir haben heute einen weiteren Gesetzentwurf zur effektiven Steuerung und Ordnung der Migration auf den Weg gebracht. Dafür brauchen wir zügige und digitale Verfahren. Deshalb verbessern wir den Datenaustausch zwischen den Behörden, etwa bei der Identitätsfeststellung von Asylbewerberinnen und -bewerbern. Unser Gesetzentwurf dient nicht nur der Steigerung der Effektivität der Migrationsverwaltung, sondern verringert auch die Bürokratie.«¹

Das Gesetz wurde unter der SPD-geführten Koalition mit FDP und BÜNDNIS 90/DIE GRÜNEN jedoch nicht mehr vom Deutschen Bundestag beschlossen. Es ist allerdings davon auszugehen, dass die im MDWG vorgesehenen Regelungsvorhaben auch in der kommenden Legislaturperiode von der neuen Regierungskoalition mit großem Nachdruck verfolgt werden. So heißt es im am 09.04.2025 veröffentlichten Koalitionsvertrag zwischen CDU, CSU und SPD: »Ein Gesetz zur Weiterentwicklung der Digitalisierung in der Migrationsverwaltung werden wir zügig umsetzen.«²

Dies gibt Anlass, den Referentenentwurf zum MDWG³ erneut eingehend zu prüfen. Welche Änderungen waren geplant? Wo bestehen Schwächen? Wo sind Anpassungen erforderlich? Die folgende Abhandlung wird sich intensiv mit diesen Fragen auseinandersetzen und eine fundierte Analyse sowie konkrete Handlungsempfehlungen zur Weiterentwicklung des Gesetzes liefern, um die Digitalisierung in der Migrationsverwaltung sowohl effizient als auch nachhaltig voranzutreiben.

I. Ausgangslage

Die Arbeitsbelastung in den Ausländerbehörden, Auslandsvertretungen und im Bundesamt für Auswärtige Angelegenheiten ist in den letzten Jahren erheblich gestiegen. Dies resultiert aus dem Anstieg der Einwanderungszahlen, der zunehmenden Komplexität der verschiedenen rechtlichen und praktischen Aufgaben sowie dem Mangel an Personal. Trotz der erhöhten Arbeitsbelastung ist der Anstieg der Einwanderung v.a. zu Bildungs- und Erwerbszwecken aufgrund des

großen Bedarfs an Fach- und Arbeitskräften in Deutschland positiv zu bewerten. Den rechtlichen Rahmen, der die angestrebte Erhöhung der Zuwanderungszahlen unterstützen soll, hat der Gesetzgeber mit dem Gesetz und der Verordnung zur Weiterentwicklung der Fachkräfteeinwanderung⁴ geschaffen.

Um die Mitarbeiterinnen und Mitarbeiter der Migrationsverwaltung, insbesondere in den Ausländerbehörden, langfristig zu entlasten, arbeiten Fachleute aus Kommunen, Ländern und dem Bund an einem von der Ministerpräsidentenkonferenz mit Beschluss vom 15.06.2023⁵ beauftragten Digitalisierungsprogramm im Migrationsbereich. Dieses Programm wurde im Juni 2023 gestartet und wird mindestens bis Ende 2025 fortgeführt.

Das Ziel der gemeinsamen Anstrengungen ist die End-to-End-Digitalisierung der Verwaltungsverfahren, die Weiterentwicklung des Ausländerzentralregisters (AZR) zu einem zentralen Ausländer-Datensystem und der Abbau rechtlicher Hürden für die Digitalisierung. Langfristig soll dies zu einer Entlastung der Mitarbeitenden in den Behörden durch Standardisierung und Digitalisierung führen, wodurch auch die Prozesse für die Antragstellenden verbessert werden.

Für die Umsetzung des Programms wurde eine ressortübergreifende Arbeitsgruppe »Digitalisierung der Migrationsverwaltung« des Bundes und der Länder unter der Leitung des Bundesministeriums des Innern und für Heimat ins Leben gerufen. Diese umfasst u.a. Fachkräfte des Bundesamtes

* Die Verfasserin beschäftigt sich seit 2017 mit dem Ausländerrecht. Seit November 2021 ist sie für das Bundeskanzleramt als Referentin und dort im Arbeitsstab der Beauftragten der Bundesregierung für Migration, Flüchtlinge und Integration – zugleich Beauftragte der Bundesregierung für Antirassismus – tätig. Der Beitrag gibt ausschließlich ihre persönlichen Ansichten wieder.

1 Abrufbar unter: <https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/12/mdwg.html>.

2 »Verantwortung für Deutschland, Koalitionsvertrag zwischen CDU, CSU und SPD, 21. Legislaturperiode«, 96, Ziff. 3084 f., einsehbar u.a. unter <https://www.handelsblatt.com/politik/deutschland/koalitionsvertrag-was-union-und-spd-vereinbart-haben-im-wortlaut/100120345.html>.

3 Grundlage ist der Referentenentwurf (RefE) v. 28.10.2024, einsehbar unter <https://www.bay-landkreistag.de/zusatzliche-inhalte/newsletter/verwaltungsinfo/2024/10/vwi-30102024-gesetzes-weiterentwicklung-digitalisierung-in-der-migrationsverwaltung/>.

4 Gesetz v. 16.08.2023 (BGBl. I Nr. 2017) und Verordnung v. 30.08.2023 (BGBl. I Nr. 233).

5 Abrufbar unter <https://www.niedersachsen.de/mpk/beschlusse-der-ministerpräsidentenkonferenz-215770.html>.

für Migration und Flüchtlinge, des Bundesministeriums für Arbeit und Soziales und des Bundesversicherungsamtes. Die Arbeitsgruppe hat sich zum Ziel gesetzt, die Datenübermittlung zwischen den Bundes-, Landes- und Kommunalbehörden, die mit der Verarbeitung von Ausländerdaten betraut sind, zu optimieren, insbesondere im Hinblick auf Automatisierung und medienbruchfreie Prozesse sowohl auf Behörden- als auch auf Länderebene. Hierzu wurden fünf Unterarbeitsgruppen (UAG) gebildet. Zusätzlich wurde eine sechste Unterarbeitsgruppe eingerichtet, um sich speziell dem Thema Erwerbsmigration zu widmen.

Die im Folgenden dargestellten, einst geplanten gesetzlichen Änderungen durch das MDWG sollten zum einen der rechtlichen Umsetzung des MPK-Beschlusses vom 15.06.2023 dienen. Zum anderen berücksichtigt der Referentenentwurf (RefE) die Empfehlungen der UAG Recht der Bund-Länder-Arbeitsgruppe »Digitalisierung der Migrationsverwaltung«. Diese hatte zur Frage von Hemmnissen der Digitalisierungsprozesse im Bereich der Migrationsverwaltung in einem mehrstufigen Verfahren unter Beteiligung von Ausländerbehörden eine Reihe von auflösbaren Defiziten identifiziert, die mit den im RefE vorgeschlagenen Neuregelungen behoben werden sollen.

II. Ziel und wesentlicher Inhalt des MDWG

Mit dem MDWG sollen bestehende Digitalisierungshemmnisse in der Migrationsverwaltung beseitigt werden. Dadurch soll die Verwaltung entlastet und die Verwaltungsverfahren für die betroffenen Personen beschleunigt werden. Der RefE enthält hierzu im Wesentlichen die nachfolgenden Änderungen im Ausländerzentralregister-Gesetz (AZRG), im Aufenthaltsgesetz (AufenthG) sowie in der Aufenthaltsverordnung (AufenthV).

1. Nachnutzung biometrischer Daten zur Entlastung der Ausländerbehörden

Zur Entlastung der Ausländerbehörden soll § 61a AufenthV (Art. 4 Nr. 2 RefE) neu gefasst werden, um sicherzustellen, dass biometrische Daten wie Lichtbild, Fingerabdrücke und Unterschrift für fünf Jahre (bei Kindern) bzw. zehn Jahre (bei Erwachsenen) gespeichert und im Rahmen der erneuten Beantragung eines elektronischen Aufenthaltstitels wiederverwendet werden können.

Die bisherige Regelung sieht vor, dass Fingerabdrücke bei der Ausstellung eines elektronischen Aufenthaltstitels nur bis zur Aushändigung des Dokuments gespeichert werden dürfen und danach gelöscht werden müssen. Einige Ausländerbehörden löschen die Daten aktuell sogar bereits bei Bestellung des elektronischen Aufenthaltstitels. Für die Verlängerung oder Änderung eines Aufenthaltstitels ist daher bisher die erneute Erfassung der Fingerabdrücke sowie eine persönliche Vorsprache erforderlich, was das Verfahren durchaus verzögern kann.

Mit der Neuregelung sollen für die Ausländerbehörden und die Antragstellenden die bislang erforderlichen zeitintensiven persönlichen Vorsprachen zur Neuerhebung der biometrischen Daten, insbesondere bei der Verlängerung von Aufenthaltstiteln, entfallen.⁶

2. Zentrale Ablage von Visumantragsdokumenten für vereinfachte Zugriffe

Die im RefE geplanten Änderungen in §§ 29 und 32 AZRG (Art. 1 Nr. 7 und 8 RefE) sollen allen im Visumverfahren beteiligten Behörden den direkten Zugriff auf die für Visumerteilungen nach § 6 Abs. 3 AufenthG erforderlichen antragsbegründenden Dokumente ermöglichen.

Bereits aktuell ist es gängige Praxis, dass die visumantragsbegründenden Unterlagen der zuständigen Ausländerbehörde über technische Schnittstellen zur Verfügung gestellt werden. Diese Unterlagen werden dann in das Fachverfahren übernommen, sodass im Verfahren zur Erteilung der Aufenthaltserlaubnis lediglich noch ergänzende Informationen von Antragstellenden eingeholt werden müssen.

Durch die im RefE vorgesehenen Änderungen der §§ 29 und 32 AZRG sollen Stellen, die bereits jetzt nach § 32 AZRG Zugang zu bestimmten Visadaten haben, künftig die Möglichkeit erhalten, auch unmittelbar auf die visumantragsbegründenden Unterlagen zuzugreifen. Dadurch soll die Notwendigkeit, diese Unterlagen separat beim Bundesverwaltungsamt oder der zuständigen Auslandsvertretung (oder beim Antragstellenden) anfordern zu müssen, entfallen. Dies soll zu einer spürbaren Entlastung des Bundesverwaltungsamts und der Auslandsvertretungen führen. In Fällen, in denen Antragstellende bspw. nicht in den Zuständigkeitsbereich der Ausländerbehörde ziehen, die im Visumverfahren beteiligt war oder als zuständige Behörde im Inland identifiziert wurde, soll durch die Änderung der Aufwand und die Notwendigkeit, zwischen den Ausländerbehörden zu kommunizieren, um die visumantragsbegründenden Unterlagen zu erhalten, entfallen. Mit den Änderungen soll explizit keine Erweiterung der Verarbeitungszwecke beabsichtigt sein, die über das bestehende Verwaltungshandeln hinausgeht.⁷

3. Informationskreislauf zwischen Behörden und AsylbLG-Trägern

Das Bundesamt für Migration und Flüchtlinge (BAMF) und die Ausländerbehörden sind verpflichtet, den zuständigen Leistungsbehörden alle relevanten Informationen gemäß dem Asylgesetz und dem Aufenthaltsgesetz mitzuteilen, die für die Gewährung von Leistungen nach dem Asylbewerberleistungsgesetz (AsylbLG) erforderlich sind (vgl. § 8 Abs. 2 Buchst. a) AsylG und § 90 Abs. 3 AufenthG). Hierzu gehören u.a. Umstände und Maßnahmen, die zu einer Einschränkung oder zum Ausschluss von Leistungen führen können, wie etwa Entscheidungen im laufenden Verfahren sowie Informationen über versäumte oder nachgeholte Mitwirkungshandlungen der Antragstellenden (vgl. § 1a Abs. 5 AsylbLG).

Mit dem Gesetz zur Anpassung von Datenübermittlungsvorschriften im Ausländer- und Sozialrecht (DÜV-AnpassG)⁸ wurde es zuletzt bereits ermöglicht, Angaben zu existenzsichernden Leistungen und zwar zu Beginn und Ende des (Ge-

6 Vgl. RefE, Begründung zu Art. 4 Nr. 2, 35 f.

7 Vgl. RefE, Begründung zu Art. 1 Nr. 7, 26.

8 Gesetz v. 08.05.2024 (BGBl. I Nr. 152).

samt-)Leistungszeitraums sowie zu der zuständigen Behörde in das AZR aufzunehmen. Seit dem 01.05.2025 erübrigen sich gem. § 3 Abs. 1 Nr. 6a AZRG entsprechende Anfragen bei der jeweils zuständigen Leistungsbehörde zum Ob und Zeitraum der Leistungsgewährung, da diese Angaben nunmehr automatisiert zur Verfügung stehen.

Im Sinne eines funktionierenden Informationskreislaufs zwischen BAMF und Ausländerbehörden auf der einen sowie Trägern für Leistungen nach dem AsylbLG auf der anderen Seite soll § 3 Abs. 1 Nr. 6a AZRG durch Art. 1 Nr. 2 Buchst. a) cc) RefE erneut geändert werden. Indem die Wörter »zu Beginn und Ende« durch die Wörter »zum Bezug« ersetzt werden, soll der Informationsaustausch zwischen Ausländer- und Leistungsbehörden um Informationen zu den Gründen und der Dauer von Leistungseinschränkungen bzw. -kürzungen ergänzt werden.⁹ Entsprechend ergeben sich Ergänzungen in der AZRG-Durchführungsverordnung; in der Anlage werden im Abschnitt I Allgemeiner Datenbestand in Spalte A nach Buchstabe c weitere Buchstaben d und e eingeführt.

Die Angaben der Leistungsbehörden zu Leistungskürzungen und Leistungsausschlüssen, die nur das Asylbewerberleistungsgesetz betreffen, sollen dem BAMF und den Ausländerbehörden ermöglichen, zu überprüfen, ob die von dort übermittelten Informationen tatsächlich zu einer Leistungseinschränkung oder einem -ausschluss geführt haben. Darüber hinaus sollen dadurch das BAMF und die Ausländerbehörden, wenn sie über eine Sanktion informiert sind, die Leistungsbehörde über nachgeholte Mitwirkungshandlungen der betroffenen Person benachrichtigen können, sodass die Kürzung gegebenenfalls wieder aufgehoben wird. Möglich werden soll dadurch zudem eine statistische Auswertung dieser Daten über das AZR.¹⁰

4. Erweiterung der elektronischen Abgabe der Verpflichtungserklärung

Bisher musste die aufenthaltsrechtliche Verpflichtungserklärung gem. § 68 AufenthG – basierend auf einer Entscheidung des Bundesverwaltungsgerichts aus dem Jahr 1998¹¹ – schriftlich abgegeben werden. Diese Verpflichtungserklärung entspricht einem zivilrechtlichen Schuldversprechen, das laut § 780 Satz 1 BGB nur in schriftlicher Form gültig ist. Der Ausschluss der elektronischen Abgabe einer solchen Erklärung diene vor allem dem – vermeintlich nur durch das Schriffterfordernis erzielbaren – Schutz vor übereilten Entscheidungen, da mit der Abgabe einer Verpflichtungserklärung ggf. umfangreiche finanzielle Folgen verbunden sein können.¹²

Aufgrund des zwischenzeitlich zunehmend elektronisch ausgerichteten Rechtsverkehrs überzeugt der Übereilungsschutz jedoch nicht mehr als tragfähiges Argument für das ausschließliche Schriftformerfordernis. Deswegen sieht § 68 Abs. 2 AufenthG-E (Art. 3 Nr. 2 a) und b) RefE) vor, dass Verpflichtungserklärungen künftig auch elektronisch abgegeben werden können. Um hierbei trotzdem weiterhin den Schutz vor übereilten Entscheidungen zu gewährleisten, soll die elektronische Abgabe künftig nur unter der Voraussetzung erlaubt sein, dass die Behörde geeignete Maßnahmen trifft, um die verpflichtungserklärende Person vor einer übereilten

Entscheidung zu warnen. Eine entsprechende Belehrung soll sowohl bei der schriftlichen als auch der elektronischen Abgabe der Verpflichtungserklärung erfolgen.¹³

5. Speicherung zusätzlicher Identifikationsdokumente

Die Änderung des § 3 Abs. 1 Nr. 4 AZRG (Art. 1 Nr. 2 Buchst. a) aa) RefE) soll es durch die Ergänzung »Angaben zur Identitätsklärung« ermöglichen, neben amtlichen Identifikationsdokumenten zukünftig auch nichtamtliche Dokumente und Volltextdokumente zu speichern, die für die rechtssichere Identifizierung eines/einer Drittstaatsangehörigen genutzt werden können. Begründet wird dies mit der Rechtsprechung des Bundesverwaltungsgerichts,¹⁴ wonach zur Identitätsklärung in Ermangelung amtlicher Ausweisdokumente nach einem mehrstufigen Prüfprogramm auch sonstige nach § 26 Abs. 1 Satz 1 und 2 VwVfG zugelassene Beweismittel zu berücksichtigen sind. Hierzu zählen insbesondere nichtamtliche Urkunden oder Dokumente, die geeignet sind, die Identität der betroffenen Person zu klären, erforderlichenfalls auch Zeugenaussagen.¹⁵

Diese vertikal ausgerichtete Stufenprüfung – die insbesondere von Einbürgerungsbehörden für das Einbürgerungsverfahren zu berücksichtigen ist – ist jedoch bisher nicht im Speicherprogramm des AZR abgebildet, sodass Dokumente und Beweismittel gem. § 26 Abs. 1 und 2 VwVfG derzeit noch bilateral zwischen den Behörden auf Grundlage der jeweiligen Verfahrensakten ausgetauscht werden müssen. Zur Beschleunigung der Verwaltungsverfahren sollen deswegen die Informationen zur Identitätsklärung in Zukunft zentral im AZR und dort vertikal entsprechend der Stufentheorie erfasst und den zuständigen Behörden digital bereitgestellt werden. Eine zentrale Ablage und Dokumentation der Validität ermögliche es den Behörden, bei denen ausländische Personen vorsprechen, vorgelegte Dokumente mit den gespeicherten Informationen abzugleichen. Für die betroffenen Personen sei die digitale Speicherung von Dokumenten ebenfalls vorteilhaft, weil sie ihre Dokumente nur einmal einreichen müssten, was den Bearbeitungsprozess deutlich effizienter und schneller machen würde. Wenn ein Dokument nach der Erfassung verloren geht, bliebe es durch die Speicherung im AZR weiterhin im System verfügbar. Dies würde – so die Begründung im RefE – auch für Personen gelten, die bei polizeilichen Kontrollen keine Dokumente bei sich haben.¹⁶

Durch die vorgesehene Änderung des § 6 Abs. 5 Nr. 7 AZRG (Art. 1 Nr. 3 Buchst. b) bb) RefE) soll gewährleistet werden, dass alle in § 6 Abs. 1 AZRG genannten Stellen (u.a. Ausländerbehörden, Aufnahmeeinrichtungen, BAMF, Bundeskriminalamt, Bundespolizeibehörden) auf diese Dokumente zugreifen können.

⁹ Vgl. RefE, Begründung zu Art. 1 Nr. 2 Buchst. a) cc), 22.

¹⁰ Vgl. RefE, Begründung zu Art. 1 Nr. 2 Buchst. a) cc), 22.

¹¹ BVerwG, Urt. v. 05.11.1998 – 1 C 24.97 –, BVerwGE 108, 333.

¹² Vgl. RefE, Begründung zu Art. 3 Nr. 2, 30 f.

¹³ Vgl. RefE, Begründung zu Art. 3 Nr. 2, 31.

¹⁴ Zuletzt BVerwG, Urt. v. 23.09.2020 – 1 C 36.19.

¹⁵ Vgl. RefE, Begründung zu Art. 1 Nr. 2 Buchst. a) aa), 21.

¹⁶ Vgl. RefE, Begründung zu Art. 1 Nr. 2 Buchst. a) aa), 22.

6. Verwaltungserleichterungen durch weitere Änderungen

Schließlich enthält der RefE einige weitere Änderungen, die der Verwaltungserleichterung dienen bzw. Wünsche aus der Praxis umsetzen sollen:

- In Vorgriff auf das Gesetz zur besseren Verhinderung missbräuchlicher Anerkennungen der Vaterschaft wird in § 3 Abs. 1 Nr. 11 AZRG-E (Art. 1 Nr. 2 Buchst. a) ee) RefE) der Speichersachverhalt »Zustimmung zur Anerkennung der Vaterschaft« im AZR vorgesehen.
- § 3 Abs. 4 AZRG-E (Art. 1 Nr. 2 Buchst. b) RefE) soll die vorstehenden Änderungen auf Unionsbürger übertragen.
- Die Einfügung des § 6 Abs. 5 Nr. 2a AZRG-E (Art. 1 Nr. 3 Buchst. b) aa) RefE) ermöglicht es Ausländerbehörden, im AZR von ihnen ausgestellte Grenzübertrittsbescheinigungen abzurufen, die von freiwillig Ausreisenden an die Grenzbehörden übergeben wurden. Ausländerbehörden erhalten derzeit bereits Pushnachrichten über den Fortzug eines Ausländers (vgl. § 15a Abs. 1 AZRG).
- Mit der Änderung in § 22 Abs. 1 AZRG (Art. 1 Nr. 6 RefE) werden auch Stellen, die bereits zum automatisierten Verfahren zugelassen sind, verpflichtet, Einzelabrufe behördenintern zu protokollieren.

Im AufenthG sind zudem folgende weitere Änderungen vorgesehen:

- Die Regelung in § 72 Abs. 3 Buchst. a) AufenthG (Art. 3 Nr. 3 RefE) wird dahingehend geändert, dass statt eines Zustimmungserfordernisses ein Beteiligungserfordernis zur Aufhebung einer Wohnsitzverpflichtung nach § 12a Abs. 5 Satz 1 AufenthG eingeführt wird.
- § 81a Abs. 2 Nr. 2 AufenthG (Art. 3 Nr. 4 RefE) soll neu gefasst werden, so dass die Versicherung des Arbeitgebers, dass er durch den Ausländer bevollmächtigt und gegebenenfalls auch berechtigt ist, Untervollmacht zu erteilen, ausreichen soll.
- Mit der Änderung des § 87 Abs. 2 Satz 1 Nr. 2a AufenthG (Art. 3 Nr. 6 a) RefE) wird der Datenaustausch verbessert.
- § 87 Abs. 4 Satz 1 AufenthG (Art. 3 Nr. 6 b) RefE) wird geändert, um den Datenaustausch zwischen Ausländerbehörden und Strafverfolgungsbehörden künftig elektronisch zu ermöglichen.

Schließlich sieht der RefE eine Änderung des § 1a Abs. 3 AsylbLG (Art. 8 RefE) vor. Hiermit soll klargestellt werden, dass bei einer Duldung für Personen mit ungeklärter Identität der Tatbestand der Leistungseinschränkung erfüllt ist, um den Prüfaufwand der Leistungsbehörden zu reduzieren.

III. Vorteile vs. Schwachstellen der geplanten Neuregelungen

1. Nachnutzung biometrischer Daten zur Entlastung der Ausländerbehörden

Durch die Möglichkeit, bereits erhobene biometrische Daten für spätere Anträge oder Verlängerungen zu nutzen, werden die Ausländerbehörden von wiederholten, zeitintensiven Erfassungen entlastet. Dies spart Personalressourcen und Zeit. Antragstellende müssen nicht mehr für jede Verlängerung

oder Änderung des Aufenthaltstitels persönlich erscheinen, um erneut biometrische Daten zu hinterlegen. Dies reduziert den Aufwand und mögliche Wartezeiten für die Antragstellenden. Die Wiederverwendung der biometrischen Daten führt zu einer beschleunigten Bearbeitung von Anträgen, da der Verwaltungsaufwand verringert wird. Durch den Wegfall der wiederholten Erhebung biometrischer Daten entstehen geringere Kosten für die Verwaltung und die Antragstellenden.

Dem RefE zum MDWG lässt sich aber zur Begründung der dort festgelegten Länge der Speicherfrist nichts entnehmen. Die geplante Speicherfrist von 10 Jahren ist nicht nachvollziehbar, legt man zu Grunde, dass nach dem Aufenthaltsrecht bzw. dem Staatsangehörigkeitsrecht bereits nach drei oder fünf Jahren eine Niederlassungserlaubnis bzw. ein deutscher Pass erteilt werden kann. Insoweit darf auch die Datenschutzgrundverordnung (DSGVO)¹⁷ nicht unberücksichtigt bleiben. Gem. Art. 5 Abs. 1 Buchst. e) DSGVO dürfen personenbezogene Daten, einschließlich biometrischer Daten, nur so lange gespeichert werden, wie sie für den spezifischen Zweck erforderlich sind. Die Speicherung biometrischer Daten im Reisepass erfolgt bspw. unter Berücksichtigung dieser Vorgaben, und die Daten werden nicht über die Gültigkeitsdauer des Passes hinaus gespeichert. Nach Ablauf des Passes werden die biometrischen Daten gelöscht oder, wie bei der Schengen-Datenbank, nicht mehr verwendet.¹⁸

Die längere Speicherung biometrischer Daten wirft schließlich auch Bedenken hinsichtlich der Datensicherheit und des Schutzes der Privatsphäre auf. Je länger die Daten aufbewahrt werden, desto höher ist das Risiko eines Missbrauchs oder eines Datenlecks. Falls die biometrischen Daten aufgrund von Veränderungen der physischen Merkmale (z.B. durch Alterung oder Unfälle) ungenau sind, könnte dies zu Problemen bei der Identifikation führen. Dies könnte sowohl die Ausländerbehörden als auch die Antragstellenden betreffen. Manche Antragstellenden könnten sich durch die längerfristige Speicherung ihrer biometrischen Daten unsicher oder überwacht fühlen, was das Vertrauen in die Verwaltung beeinträchtigen könnte.

2. Zentrale Ablage von Visumantragsdokumenten für vereinfachte Zugriffe

Durch die zentrale Ablage der antragsbegründenden Dokumente in der Visadatei wird der Zugriff für alle im Visumverfahren beteiligten Behörden erleichtert. Dies dürfte zu einer schnelleren Bearbeitung von Visumanträgen führen. Da die Unterlagen nicht erneut angefordert werden müssen, sondern direkt von den zuständigen Stellen abgerufen werden können, entfällt unnötige Bürokratie und Ressourcenverschwendung. Insbesondere den Ausländerbehörden soll dadurch die Vorbereitung des Antragsverfahrens »auf Erteilung einer

¹⁷ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119 v. 04.05.2016, 1.

¹⁸ Siehe hierzu ergänzende Überlegungen unter IV.

Aufenthaltsurlaubnis« erleichtert werden.¹⁹ Die Abrufbarkeit der Rechtsgrundlage und der Nebenbestimmungen für die Visumerteilung sorgt für mehr Klarheit und Transparenz im Prozess. Dies hilft den Behörden, fundierte und nachvollziehbare Entscheidungen zu treffen und reduziert mögliche Missverständnisse oder Fehler. Durch die zentrale Speicherung können Behörden effizient miteinander kommunizieren und Informationen austauschen, was die Zusammenarbeit im Visumverfahren verbessert und zu einer besseren Koordination führt.

Eine zentrale Datenquelle reduziert die Wahrscheinlichkeit von Fehlern, die auftreten könnten, wenn Dokumente manuell oder per Mail übermittelt oder zwischen verschiedenen Behörden geteilt werden. Dies sorgt für mehr Genauigkeit bei der Bearbeitung von Anträgen.

Die zentrale Speicherung von sensiblen persönlichen Daten birgt jedoch auch hier Risiken im Hinblick auf die Datensicherheit. Ein Datenleck oder Missbrauch könnte schwerwiegende Folgen haben, insbesondere, wenn nicht ausreichend Schutzmaßnahmen getroffen werden.

Bei technischen Problemen oder Systemausfällen könnte der Zugriff auf wichtige Daten verzögert werden, was den gesamten Visumprozess beeinträchtigen könnte.

Eine zentrale Datenspeicherung macht das System anfälliger für Cyberangriffe. Sollte ein Angreifer Zugang zu dieser zentralen Visadatei erhalten, könnten alle gespeicherten Daten gefährdet sein. Zu erinnern sei an den Cyberangriff in Dänemark. Im Oktober 2023 wurde Dänemark Ziel eines umfangreichen Hackerangriffs, bei dem Ransomware eingesetzt wurde, um die Computerinfrastruktur mehrerer öffentlicher Behörden und Einrichtungen zu infiltrieren. Die Angreifer verschlüsselten wichtige Daten und forderten ein Lösegeld, was zu erheblichen Störungen im öffentlichen Dienst führte, einschließlich Verzögerungen bei der Bearbeitung von Anträgen und der Bereitstellung von Dienstleistungen für die Bürger.²⁰

3. Informationskreislauf zwischen Behörden und AsylbLG-Trägern

Der Informationskreislauf zwischen dem BAMF, den Ausländerbehörden und den Trägern der Asylbewerberleistungen wird durch die angedachten Regelungen grundsätzlich gestärkt.

Sozialdaten sind jedoch in besonderem Maße durch das Sozialgeheimnis (§ 35 SGB I) geschützt. Zweck des Sozialgeheimnisses ist es, zu verhindern, dass durch Kenntniserlangung der Hilfsbedürftigkeit den Betroffenen ungerechtfertigte Nachteile entstehen. Um dies zu erreichen, bedarf es einer verstärkten Zweckbindung dieser Daten. Hierzu sind bisher keine Ausführungen im RefE enthalten. Schließlich sollte klar sein: werden Informationen im AZR fehlerhaft eingetragen, kann dies zu ungerechtfertigten Leistungseinschränkungen oder -ausschlüssen führen. Ein Fehler in der zentralen Datenbank könnte eine Kettenreaktion von falschen Entscheidungen und Problemen bei der Bereitstellung von Leistungen auslösen. Es könnte problematisch sein, dass Daten im AZR auch für statistische Auswertungen verwendet werden, ohne dass die betroffenen Personen ausreichend

informiert werden oder die Zweckbindung hinreichend klar ist.

4. Erweiterung der elektronischen Abgabe der Verpflichtungserklärung

Die elektronische Abgabe der Verpflichtungserklärung erleichtert den Antragstellenden den Prozess, da sie nicht mehr auf den Postweg oder persönliche Vorsprachen angewiesen sind. Das spart Zeit und Mühe, sowohl für die Antragstellenden als auch für die Behörden. Die Digitalisierung dieses Schrittes trägt zur Reduzierung von Papierdokumenten bei, was umweltfreundlich ist und die Ressourcennutzung optimiert. Durch die elektronische Abgabe können die Behörden schneller auf die eingereichten Dokumente zugreifen, was die Bearbeitungszeiten verkürzt und die Effizienz steigert.

Die Erweiterung auf die elektronische Abgabemöglichkeit entspricht dem Trend hin zu digitalen Verwaltungsprozessen, der insgesamt eine Modernisierung und Vereinfachung der Behördenabläufe fördert.

Personen, die weniger technikaffin sind, könnten aber Schwierigkeiten haben, das elektronische System zu nutzen. Dies könnte den Prozess erschweren und zu Verzögerungen führen. Bei der elektronischen Abgabe entfallen zudem mögliche persönliche Beratungen oder Erklärungen, die in manchen Fällen für Antragstellende hilfreich, wenn nicht gar notwendig sein dürften. Immerhin sieht der RefE vor, die die Erklärung abgebende Person durch »geeignete Maßnahmen« vor einer übereilten Abgabe der Erklärung zu warnen.

5. Speicherung zusätzlicher Identifikationsdokumente

Durch die Möglichkeit, auch nichtamtliche Dokumente zu speichern, können Behörden eine genauere und umfassendere Identifikation der Person vornehmen, was besonders bei komplexen Fällen oder Unsicherheiten hilfreich ist. Die Speicherung zusätzlicher Dokumente ermöglicht es, eine vollständige Historie der Identifikation einer Person zu führen, was die Transparenz und Nachvollziehbarkeit von behördlichen Entscheidungen und Prozessen verbessert. Wenn mehr Dokumente gespeichert sind, können Antragsprozesse effizienter gestaltet werden, da alle relevanten Informationen an einem zentralen Ort verfügbar sind und schnell abgerufen werden können, ohne dass zusätzliche Dokumente angefordert werden müssen.

Nichtamtliche Dokumente könnten zudem zusätzliche wertvolle Informationen liefern, die nicht in amtlichen Papieren enthalten sind, wie etwa Nachweise zu früheren Aufenthalten, Bildungs- oder Berufshistorien.

Die Speicherung zusätzlicher nichtamtlicher (Volltext-)Dokumente wirft dennoch datenschutzrechtliche Bedenken auf, da solche Dokumente oft sehr persönliche Informationen

¹⁹ Vgl. RefE, Begründung zu Art. 1 Nr. 7 Buchst. b), 26, wobei es richtigerweise eines »im Inland erteilten Aufenthaltstitels« heißen müsste, da nach der Einreise mit einem nationalen Visum auch die Erteilung einer Blauen Karte EU (vgl. § 18g AufenthG), einer ICT-Karte (vgl. § 19 AufenthG), einer Mobiler-ICT-Karte (vgl. § 19b AufenthG) oder einer Niederlassungserlaubnis (vgl. §§ 18c Abs. 3, 23 Abs. 2 AufenthG) möglich ist.

²⁰ <https://taz.de/Datenleck-in-Daenemark/16064263/>.

enthalten. Es muss sichergestellt werden, dass die Daten sicher gespeichert und nur unter strengen Auflagen zugänglich sind. Es besteht die Gefahr, dass nichtamtliche Dokumente fehlerhaft gespeichert oder einer falschen Person zugeordnet werden. Das Sammeln und Speichern zusätzlicher Dokumente könnte den Verwaltungsaufwand erhöhen. Bei der Speicherung von nichtamtlichen Dokumenten könnten bestimmte Informationen missbraucht werden, bspw. bei unbefugtem Zugriff oder bei der Nutzung von Dokumenten, die nicht die notwendige Authentizität oder Gültigkeit aufweisen.

Nicht zuletzt ist kritisch zu betrachten, dass durch die jetzige Fassung des RefE und der geplanten vertikalen Speicherung der Dokumente i.R.d. Stufentheorie der Anschein erweckt wird, als würden die im AZR gespeicherten Dokumente materiell-rechtliche Wirkung zur Frage der Identitätsklärung entfalten. Die materiell-rechtliche Prüfung zur Klärung der Identität muss indes weiterhin den Behörden obliegen.

IV. Fazit

Die Digitalisierung der Migrationsverwaltung durch das MDWG stellt einen bedeutenden Schritt in Richtung effizienter und zukunftsfähiger Verwaltungsprozesse dar. Sie bietet das Potenzial, die Arbeitsbelastung der Ausländerbehörden zu verringern, bürokratische Hürden zu überwinden und den Service für die Antragstellenden zu verbessern. Besonders die Nachnutzung biometrischer Daten, die zentrale Ablage von Visumantragsdokumenten sowie die Erweiterung der elektronischen Abgabe von Verpflichtungserklärungen können zu spürbaren Effizienzgewinnen und einer beschleunigten Bearbeitung führen. Auch die stärkere Vernetzung der verschiedenen Behörden im Rahmen eines funktionierenden Informationskreislaufs ist ein zukunftsreicher Ansatz, der das Zusammenwirken von Behörden optimiert und eine präzisere Datenverarbeitung ermöglicht.

Jedoch zeigt sich bei näherer Betrachtung, dass das MDWG nicht ohne Schwachstellen ist. So wirft etwa die geplante Speicherung biometrischer Daten über längere Zeiträume hinweg datenschutzrechtliche Bedenken auf. Insbesondere der Schutz der Privatsphäre und die mögliche Gefahr von Datenmissbrauch oder -lecks müssen zwingend berücksichtigt werden. Es muss sichergestellt werden, dass die Speicherung nicht nur technisch, sondern auch rechtlich und ethisch vertretbar ist. Die für die elektronische Abgabe von Verpflichtungserklärungen vorgesehene Warnfunktion gegen übereilte Entscheidungen ist grundsätzlich zu begrüßen, doch bleibt die Frage offen, wie effektiv diese Maßnahme tatsächlich ist, wenn Antragstellende nicht ausreichend über die Tragweite ihrer Entscheidung aufgeklärt werden. Zudem gibt es Unsicherheiten hinsichtlich der Umsetzung und Handhabung von nichtamtlichen Dokumenten, die künftig ebenfalls gespeichert werden sollen, da dies datenschutzrechtliche Risiken birgt.

Um die Digitalisierung der Migrationsverwaltung auf eine noch stabilere und nachhaltig wirksame Grundlage zu stellen, wäre bei einem Neuanlauf des Regelungsvorhabens u.a. eine Reduzierung der Speicherfristen auf einen kürzeren Zeitraum, der im Einklang mit den Aufenthaltsrechten steht, anzuregen. Im Schengen-Recht bspw. ist die zulässige

Speicherdauer für biometrische Daten, wie sie im Rahmen des Visa-Informationssystems (VIS) verwendet werden, auf 59 Monate begrenzt. Diese Frist entspricht in etwa der maximalen Gültigkeitsdauer eines Schengen-Visums, das für maximal fünf Jahre ausgestellt werden kann. Die Speicherdauer von 59 Monaten ist darauf ausgerichtet, die Daten nur so lange aufzubewahren, wie sie für den spezifischen Aufenthalt und die Überprüfung von Visa-Anträgen oder Einreiseentscheidungen erforderlich sind. Nach Ablauf der Frist werden die Daten gelöscht, da sie dann für die Verwaltung von Visa und Grenzkontrollen nicht mehr erforderlich sind.

Überträgt man diese Logik auf das nationale Aufenthaltsrecht, sollten die biometrischen Daten grundsätzlich gelöscht werden, sobald sie seitens der Ausländerbehörde nicht mehr gebraucht werden, bspw. bei Erteilung der Niederlassungserlaubnis oder bei positiver Entscheidung über einen Einbürgerungsantrag. Eine grundlose weitere Speicherung biometrischer Daten von bis zu 10 Jahren ist weder nachvollziehbar noch angemessen. Eine Verlängerung der Speicherung sollte vielmehr nur in Ausnahmefällen zugelassen werden, z.B. bei laufenden Ermittlungen oder rechtlichen Verfahren. Wichtig dabei ist, dass jede Verlängerung gut begründet wird und die betroffenen Personen über die Speicherung ihrer Daten sowie die Gründe dafür informiert werden. Nur so würde im Ergebnis auch Art. 5 Abs. 1 Buchst. e) DSGVO entsprochen, wonach personenbezogene Daten nur so lange gespeichert werden dürfen, wie sie für den jeweiligen Zweck benötigt werden.

Die zentrale Ablage von Visumantragsdokumenten und die Nachnutzung bereits gespeicherter Daten haben das Potenzial, doppelte Erfassungen zu verhindern und unnötige Bürokratie abzubauen. Gleichzeitig muss jedoch sichergestellt werden, dass die Prozesse tatsächlich transparent und fehlerfrei durchgeführt werden, um Missverständnisse und zusätzliche Arbeit zu vermeiden. Auch hier ist eine kontinuierliche Überprüfung der Effizienz der digitalen Abläufe und der Vermeidung von Medienbrüchen erforderlich.

Im Einklang mit dem Grundrecht auf informationelle Selbstbestimmung sollte jede betroffene Person grundsätzlich die Kontrolle darüber haben, wie ihre personenbezogenen Daten verarbeitet werden. Die Europäische Datenschutz-Grundverordnung, das Bundesdatenschutzgesetz sowie die jeweiligen Datenschutzgesetze der Bundesländer stellen in diesem Zusammenhang klare Vorgaben für die Datenverarbeitung auf. Diese beinhalten insbesondere Regelungen zu den rechtlichen Grundlagen der Datenverarbeitung, Anforderungen an die Informationsweitergabe und Auskunftserteilung sowie Vorschriften zu den technischen und organisatorischen Maßnahmen, die den Schutz personenbezogener Daten gewährleisten sollen. Angesichts der Vielzahl sensibler Daten, die künftig zentral gespeichert und abgerufen werden sollen, ist der Ausbau von Datensicherheitsmaßnahmen daher unerlässlich. Hierzu gehört die Implementierung robuster Verschlüsselungstechnologien, regelmäßiger Sicherheitsüberprüfungen und ein umfassendes Zugriffsmanagement, das nur autorisierten Personen Zugang zu den Daten gewährt. Auch die Transparenz gegenüber den Antragstellenden muss erhöht werden, um ein höheres Vertrauen in die digitale Verwal-

tung zu schaffen. Weiterhin sollte eine stärkere Aufklärung über den Umgang mit sensiblen Daten erfolgen, um das Bewusstsein für Datenschutz zu schärfen. Idealerweise könnte parallel zu den erweiterten Möglichkeiten zur Speicherung und zum Abrufen von Daten ein digitales »Datenscockpit« entwickelt werden, das speziell auf die Bedürfnisse der Bürger zugeschnitten ist. Mit einem solchen System würde den Bürgern ein klarer Überblick über ihre persönlichen Daten ermöglicht, die von verschiedenen Behörden gespeichert, verarbeitet und genutzt werden. Dies würde Transparenz in Bezug auf die Datenspeicherung und -verwendung schaffen und das Vertrauen in die Verwaltung stärken. Bürger könnten auf diese Weise einsehen, welche Daten wo gespeichert sind und möglicherweise auch festlegen, wer Zugang zu diesen Daten hat und zu welchem Zweck sie verwendet werden. Im Rahmen der geplanten Reformen des Registermodernisierungsgesetzes wird allgemein angestrebt, mehr Transparenz und Kontrolle über personenbezogene Daten in öffentlichen Datenbanken herzustellen, bspw. durch die Einführung eines Datenschutzcockpits.²¹ Wenn Zugewanderte über ein solches Cockpit Zugriff auf ihre gespeicherten Datensätze haben, könnten sie diese beispielsweise eigenständig mit der Integrationsberatung teilen.²²

In diesem Zusammenhang ist auch zu erwähnen, dass innerhalb des Förderprogramms »Sichere Digitale Identitäten« des Bundesministeriums für Wirtschaft und Klimaschutz²³ die beiden Schaufensterprojekte ID-Ideal und ONCE gemeinsam die »kommunale Datenkarte« erprobt haben – eine digitale Identitätslösung, die es Bürgern ermöglicht, digitale Nachweise zu erstellen und eigenständig über die Weitergabe ihrer Daten und Nachweise zu entscheiden. Mit der Nutzung von Self-sovereign Identity Technologie haben Bürger die Möglichkeit, ihre Daten sicher in einer digitalen Wallet auf ihrem Smartphone zu verwalten und sie bei Bedarf vorzulegen – dabei geben sie nur die notwendigsten Informationen preis. Dieser Ansatz stellt einen bedeutenden Fortschritt hin zu einer modernen, serviceorientierten und datenschutzkonformen Verwaltung dar. Solche Reformvorhaben bieten vielversprechende Potenziale, zukünftig den Aufwand für die Datenhaltung zu minimieren, die Qualität von Daten zu verbessern und Daten interessengerechter verarbeiten zu können.²⁴

Entscheidend wird jedoch sein, dass die Belange der Migrations- und Integrationsverwaltung frühzeitig berücksichtigt werden – und idealerweise nicht erst am Ende des vermutlich langwierigen und schrittweisen Reformprozesses. Angesichts der Sensibilität der Daten, der hohen Fehleranfälligkeit und des Ausbaus der zentralen Datenspeicherung im AZR ist es in jedem Fall notwendig, ein höheres Maß an Transparenz und effektiven Kontrollmöglichkeiten für Zugewanderte zu gewährleisten.²⁵

Der Informationsaustausch zwischen Behörden muss klarer und transparenter geregelt werden. Es muss sichergestellt werden, dass personenbezogene Daten nicht für Zwecke verwendet werden, die über die ursprünglich festgelegten Ziele hinausgehen. Insbesondere im Hinblick auf Sozialdaten und

Leistungseinschränkungen im AsylbLG sollten klare Regeln und Transparenz hinsichtlich der Nutzung dieser Daten eingeführt werden. Eine klare Zweckbindung der Daten und die Information der betroffenen Personen über die Verwendung ihrer Daten ist essentiell, um rechtlichen und ethischen Problemen vorzubeugen. Allgemein empfiehlt sich, dass zu den vorgesehenen Änderungen datenschutzrechtliche Fragen bestenfalls von Bundesebene verbindlich geklärt werden, um Kommunen zu entlasten und ihnen Handlungssicherheit zu geben.

Abschließend lässt sich sagen, dass das MDWG einen grundlegenden Schritt in der Modernisierung der Migrationsverwaltung darstellt. Dennoch muss die Umsetzung sorgfältig überwacht werden, um sicherzustellen, dass das Gesetz nicht nur in technischer Hinsicht Fortschritte erzielt, sondern auch die Rechte der betroffenen Personen gewahrt bleiben. Die Handlungsempfehlungen zielen darauf ab, die potenziellen Schwächen zu adressieren und eine noch nachhaltigere, datenschutz- und benutzerfreundlichere digitale Verwaltung zu schaffen, die langfristig sowohl den Behörden als auch den Antragstellenden zugutekommt. Zugewanderte haben insbesondere aufgrund fehlender Transparenz bei der Nutzung ihrer Daten häufig Unsicherheiten. Ein Datenschutzcockpit könnte hier Chancen bieten, wenn es relevante Register wie das AZR einbezieht und sprachlich auf die Bedürfnisse einer Migrationsgesellschaft abgestimmt ist. Dabei ist es entscheidend, den Integrationsbereich sowie die Anforderungen einer vielfältigen Gesellschaft bereits frühzeitig in den Prozess der Verwaltungsmodernisierung und -digitalisierung einzubeziehen und in den entsprechenden Reformen zu berücksichtigen. Die nachfolgende Legislaturperiode bietet die Möglichkeit, die ausstehenden Fragen und Bedarfe zu klären und das MDWG weiter zu optimieren. Schlussendlich ist aber auch eines klar: Digitalisierung allein nützt wenig, wenn nicht gleichzeitig die rechtlichen Rahmenbedingungen vereinfacht werden. Insbesondere müssen die komplexen Regelungen des Aufenthaltsgesetzes entschlackt werden, um die Anwendung des Gesetzes für alle Beteiligten zu erleichtern. In diesem Zusammenhang ist es ausdrücklich zu begrüßen, dass der Koalitionsvertrag auch eine redaktionelle Überarbeitung und Entbürokratisierung des Aufenthaltsgesetzes vorsieht, um eine effizientere Migrationsverwaltung zu gewährleisten.

21 <https://www.digitale-verwaltung.de/Webs/DV/DE/registermodernisierung/elemente/datenschutzcockpit/datenschutzcockpit-node.html>.

22 Kühn/Gluns, Studie »Vernetzte Daten, vernetzte Behörden? Datenmanagement, Datenschutz und Kooperation in der lokalen Integration«, 39.

23 https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html.

24 Zu den Potenzialen ausführlich Hempell/Anke, »Privacy Management mit Self-Sovereign Identity: Potenziale zur Erhöhung der informationellen Selbstbestimmung«, abrufbar unter <https://fs.bib.htw-dresden.de/esploro/outputs/bookChapter/Privacy-Management-mit-Self-Sovereign-Identity-Potenziale/99557318802581>.

25 So auch Kühn/Gluns, Studie »Vernetzte Daten, vernetzte Behörden? Datenmanagement, Datenschutz und Kooperation in der lokalen Integration«, 35.