Netzwerk Datenschutzexpertise GbR
Dr. Thilo Weichert
Waisenhofstr. 41
D-24103 Kiel
Tel.: +49 431 9719742
E-Mail: weichert@netzwerk-datenschutzexpertise.de

DR. THILO WEICHERT, WAISENHOFSTR. 41, 24103 KIEL

An die Fraktionen des Deutschen Bundestages

Kiel, den 22.03.2019

Stellungnahme des Netzwerks Datenschutzexpertise

zum Gesetzentwurf der Bundesregierung
Entwurf eines Zweiten Gesetzes zur Verbesserung der Registrierung und des Datenaustauschs zu aufenthalts- und asylrechtlichen Zwecken (Zweites Datenaustauschverbesserungesetz - 2. DAVG)
BR-Drs. 54/19 v. 01.02.2019

Sehr geehrte Damen und Herren,

mit dem Entwurf eines 2. DAVG soll die digitale Kommunikation über Asyl- und Schutzsuchende sowie Ausländer, die unerlaubt nach Deutschland einreisen oder sich unerlaubt aufhalten, verbessert werden. Dies insbesondere dadurch, dass das Ausländerzentralregister (AZR) weiter ausgebaut und die medienbruchfreie Datenbereitstellung durch das AZR ausgeweitet wird. Damit wird an das Datenaustauschverbesserungsgesetz vom 02.02.2016 (BGBl. I S. 130) angeknüpft, das die gleiche Intention verfolgt hat.

Als wesentliche neue Regelungsinhalte nennt der Entwurf folgende Aspekte:

- Authentisierung von Onlineabrufen vom AZR durch Organisationen statt Einzelpersonen,
- Verwendung der AZR-Nummer in der Kommunikation zwischen allen öffentlichen Stellen,
- erleichterte Weiterverarbeitung abgerufener AZR-Daten zu Grund-Personalien,
- Erweiterung des Umfangs der im AZR gespeicherten Grundpersonalien,
- verbindliche Festlegung einer technischen Kommunikationsschnittstelle mit dem AZR,
- Erweiterung der Zuständigkeit der Bundespolizei für erkennungsdienstliche (ED-) Behandlungen,
- Einbeziehung der Erkenntnisse der Bundespolizei bei der Visumserteilung,
- Ausweitung der Überprüfung von Drittstaatsangehörigen,
- flächendeckende Registrierung von unbegleiteten Minderjährigen mit zusätzlicher Erfassung von Fingerabdrücken, einschließlich der Verpflichtung der Jugendämter, hierauf hinzuwirken,
- Absenkung des Alters für die Identifizierung mit Fingerabdrücken von 14 auf 6 Jahre,
- Ausweitung der Speicherung von Identifizierungsdaten zur Durchführung von Abschiebungen,
- zentralisierte Speicherung von Daten zur Förderung der Ausreise im AZR.

In seinem Beschluss zum Gesetzentwurf vom 15.03.2019 hat der Bundesrat weitere Ausweitungen der Datenverarbeitung gefordert (BR-Drs. 54/19 – Beschluss). Nicht beschlossen wurde vom Bundesrat die Empfehlung des Ausschusses für Arbeit, Integration und Soziales (AIS), zu prüfen, inwieweit die Regelungen mit den in der Datenschutz-Grundverordnung (DSGVO) „vorgegebenen datenschutz-rechtlichen Grundsätzen der

Erforderlichkeit (Artikel 5 Absatz 1 Buchstabe a DSGVO) der Zweckbindung (Artikel 5 Absatz 1 Buchstabe b DSGVO) sowie der Datensparsamkeit (Artikel 5 Absatz 1 Buchstabe c DSGVO) vereinbar sind“ (BR-Drs. 54/1/19 v. 04.03.201, Nr. 6). Ebenso wurde empfohlen, die Vereinbarkeit der AZR-Nummer mit Art. 87 DSGVO (Nr. 7) sowie den Umfang der im AZR gespeicherten Stammdaten (Nr. 12) zu prüfen. Dem kam das Bundesratsplenum ebenso nicht nach.

A. Allgemeine Bewertung des Gesetzesvorschlags

Der Gesetzentwurf zeichnet sich dadurch aus, dass hinsichtlich der technischen Überwachung von Flüchtlingen eine Ausweitung erfolgt, ohne dass auch nur eine einzige zusätzliche Vorkehrung getroffen wird, um deren Grundrechtsschutz, insbesondere den Datenschutz, also den Schutz des Rechts auf informationelle Selbstbestimmung, abzusichern. Die Betroffenen sind so einem zentralisierten bürokratischen Informationssystem mit zwangsweiser Erfassung und Kommunikation ausgesetzt, ohne hierbei einen wesentlichen eigenen bestimmenden Einfluss nehmen zu können. Trotz einer weiteren Erfassung von Daten, erweiterten Nutzungsmöglichkeiten und der damit verbundenen erhöhten Gefahr einer unzulässigen Zweckänderung der Daten und eines Datenmissbrauchs sieht der Entwurf keine Vorkehrungen zur Verhinderung solcher Aktivitäten und **keine zusätzlichen Garantien** für die Betroffenen vor.

Die Notwendigkeit zusätzlicher Sicherungen besteht auch angesichts des Umstands, dass das AZR als zentrale Datenspeicherungs- und Austauschplattform immer weiter ausgebaut wird und hierüber eine Totalkontrolle der Erfassten ermöglicht wird. Eine derartige zentrale Erfassung von Menschen ist in hohem Maße missbrauchsanfällig. Die Erfahrungen während des Nationalsozialismus mit der **zentralen Erfassung** von Menschen, die einer diskriminierungsgefährdeten Minderheit angehören, führte in der Bundesrepublik zu der Konsequenz, dass Geheimdienste und Polizei informationell voneinander getrennt und föderal strukturiert wurden (Polizeibrief der Alliierten zur Genehmigung des Grundgesetzes vom 14.04.1949) und dass in den 70er-Jahren die Planungen für ein zentralisiertes Meldewesen verworfen und anstelle dessen eine kommunale Meldeerfassung vorgenommen wurde. Von diesen Schlussfolgerungen unberührt blieb die zentralisierte Erfassung von Ausländerinnen und Ausländern in Deutschland (Weichert, AZRG, 1996, Einführung Rn. 2-5). Gemäß der Rechtsprechung bedarf es für zentrale Datenverarbeitungsstrukturen jeweils einer spezifischen Legitimation (EuGH 16.12.2008 – C 524/06 Rn. 66), die vom Entwurf nur ungenügend dargestellt wird. Angesichts zunehmender ausländerfeindlicher Tendenzen in Deutschland und dem Risiko, dass deren Vertreter auch administrativen Einfluss erhalten können, müssen Vorkehrungen für den Fall ergriffen werden, dass derartige Daten zur Diskriminierung und Verfolgung von Minderheiten genutzt werden. Dies wurde bisher und wird erneut im vorliegenden Entwurf versäumt.

Im vorliegenden Gesetzentwurf geht es insbesondere um die Verarbeitung von Daten zu Flüchtlingen, von denen viele wegen **politischer Verfolgung** Anträge auf Asyl und auf Anerkennung einer politischen Verfolgung stellen. Gemäß Art. 9 Abs. 1 der europäischen Datenschutz-Grundverordnung (DSGVO) ist die Verarbeitung besonderer Kategorien personenbezogener Daten grds. untersagt. Hierzu zählen u. a. Daten, aus denen politische Meinungen hervorgehen. Die Ansicht, politisch verfolgt zu sein und einen Anspruch auf Asyl nach Art. 16a GG zu haben, stellt selbst eine politische Meinung dar. Der Umstand, einen Asylantrag gestellt zu haben, kann die Grundlage für politische Verfolgung sein. Bei den Angaben des Flüchtlings zur Begründung seines Asylantrags sowie bei den Entscheidungen hierüber handelt es sich um Informationen über die politische Meinung des Betroffenen (Weichert in Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 9 Rn. 27; ders. in Huber, AufenthG, 1. Aufl. 2010, § 86 Rn. 45 f.; Wedde in Däubler u .a., EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Art. 9 Rn. 19). Gemäß Art. 9 Abs. 2 lit. g DSGVO ist die Verarbeitung von Angaben über die politische Meinung erlaubt, wenn dies auf der

Grundlage eines Gesetzes erfolgt, dies im erheblichen öffentlichen Interesse erforderlich ist und dabei der Wesensgehalt des Datenschutzgrundrechts sowie die Interessen der Betroffenen durch „angemessene und spezifische Maßnahmen“ gewahrt werden. Ein öffentliches Interesse an einer Verarbeitung nach dem AZRG, dem Asylgesetz (AsylG) oder nach anderen aufenthaltsrechtlichen Vorschriften kann grds. angenommen werden. Für die Zulässigkeit einer Verarbeitung bedarf der weiten in Art. 9 Abs. 2 lit. g DSGVO genannten Voraussetzungen (verstärkte Erforderlichkeitsprüfung sowie angemessene Schutzvorkehrungen). Der Entwurf ist an diesen Maßstäben zu messen.

Eine aktuelle Gefährdung für betroffene Flüchtlinge besteht insbesondere darin, dass die Asylantrags- oder die AZR-Daten über das AZR oder über abfragende deutsche Stellen an Stellen und **Behörden der Heimatländer** gelangen, die diese für konkrete Repressionen oder Verfolgungsmaßnahmen nutzen können. Angesichts des gesteigerten Inhalts der AZR-Daten über viele höchstpersönliche Umstände insbesondere im Asylverfahren und die leichtere Zugänglichkeit dieser Daten besteht hierin eine besondere Gefahr für die Betroffenen (Weichert in Huber, AufenthG, 1. Aufl. 2010, § 86 Rn. 40). Der Entwurf sieht insofern keine adäquaten Schutzmechanismen vor. Ein solcher Mechanismus könnte darin bestehen, dass auf Antrag des Betroffenen Daten gezielt gesperrt, d. h. in der Verarbeitung beschränkt werden, wenn damit eine Gefahr von Verfolgung begründet werden kann. Eine solche Konkretisierung des in Art. 22 DSGVO vorgesehenen Widerspruchsrechts ist grundrechtlich geboten.

Gemäß Art. 87 DSGVO bedarf es bei der Normierung von nationalen Kennziffern oder anderer Kennzeichen von allgemeiner Bedeutung „geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person“. Bei der **AZR-Nummer** (§ 3 Nr. 2 AZRG) handelt es sich um eine solche Kennziffer, nachdem diese nicht nur für aufenthaltsrechtliche Zwecke, sondern generell für die Verwaltung von Ausländern bzw. deren Daten genutzt wird (kritisch dazu schon Weichert, AZRG, 1996, § 3 Rn. 6). Die Nutzung der AZR-Nummer wurde mit dem 1. DVAG auf die Versorgung und Unterstützung der Betroffenen und wird nun auf das gesamte Melderecht ausgeweitet (§ 18e Abs. 2 AZRG, § 3 Abs. 1 Nr. 17a BMG). Der Bundesratsbeschluss sieht gar eine Ausweitung der AZR-Nummer in Bereichen vor, wo eine eindeutige Zuordnung durch die Sozialversicherungsnummer oder in der Meldebehörde gewährleistet ist (BR-Drs. 54/19 – Beschluss, Nr. 2, 3, 4). Die europarechtlich geforderten Garantien sind aber nicht ersichtlich. Vielmehr beschränken sich die Betroffenenrechte und die technisch-organisatorischen und prozeduralen Vorkehrungen beim AZR auf einen Minimalstandard, ohne die besonderen Risiken dieser Datenbank zu berücksichtigen.

Ursprünglich handelte es sich bei dem AZR um eine Datenbank, die ausschließlich aufenthalts- und sicherheitsbehördliche Funktionen erfüllte. Schon mit dem 1. DAVG von 2016 wurde der Anwendungs- und Nutzungsbereich des AZR auf **Förderungs-, Hilfs- und soziale Maßnahmen** ausgeweitet (vgl. §§ 6 Abs. 1 Nr. 8, Abs. 2 Nr.6, 18a-18d AZRG). Eine informationelle Abschottung dieser neuen Nutzungen von den ursprünglichen Zwecken ist nicht vorgesehen. Dies führt dazu, dass die Vertraulichkeit, die für Hilfemaßnahmen oft erforderlich ist, und die z. B. über Berufsgeheimnisse oder das Sozialgeheimnis (§ 35 SGB I) normativ gewährleistet wird, für Ausländerinnen und Ausländer, insbesondere für die erfassten Flüchtlinge, teilweise nicht gilt (z. B. in Asylbewerberleistungsgesetz) bzw. über die Zwischenschaltung des AZR aufgehoben wird. Der Bundesrat will mit seinem Beschluss am 15.03.2019 noch weiter gehen, indem er fordert, das AZR noch stärker für Integrationsmaßnahmen zu nutzen (BR-Drs. 54/19 – Beschluss, Nr. 1).

Art. 6 Abs. 4 DSGVO verbietet bei der personenbezogenen Datenverarbeitung das Verfolgen von **Zwecken, die miteinander nicht vereinbar sind**. Bei tendenziell unvereinbaren Zwecken müssen negative „Folgen der beabsichtigten Weiterverarbeitung“ regulativ ausgeschlossen werden (lit. d) oder „geeignete Garantien“ vorhanden sein (lit. e). Der sowohl europarechtlich bei der Verarbeitung von sensitiven Daten (Art. 9 DSGVO) wie auch verfassungsrechtlich

geforderte gesteigerte Schutz (Weichert DuD 2017, 539) wird bei Flüchtlingen weder im AZRG noch in den sonstigen Gesetzen gewährleistet.

Nicht weiter ausgeführt werden können und sollen hier weitergehende **verfassungsrechtliche Bedenken**, die schon langfristig hinsichtlich der Regelungen des AZRG bestehen und welche die Bestimmtheit von Regelungen, die Erforderlichkeit von zugelassenen Verarbeitungen, die Verhältnismäßigkeit im engeren Sinne sowie den Gleichheitsgrundsatz betreffen (dazu schon Weichert, AZRG, 1996, Einführung Rn. 13-46).

Die oben aufgeführten allgemeinen Kritikpunkte wurden schon im Rahmen der **Verbändeanhörung** zum Referentenentwurf des Bundesinnenministeriums von verschiedenen Stellen vorgetragen. Leider hat sich diese Kritik in keiner Weise im nun vorgelegten Regierungsentwurf oder in der Stellungnahme des Bundesrates niedergeschlagen.

B. Kompensatorische Maßnahmen zur Sicherung des Grundrechts für Datenschutz für Nichtdeutsche

Die obigen Ausführungen weisen darauf hin, dass mit dem Gesetzesvorschlag weitere massive Eingriffe in das Grundrecht auf Datenschutz der Betroffenen vorgesehen sind. Mit ihnen werden die schon bestehenden **Erfassungs- und Überwachungsmaßnahmen gegenüber Nichtdeutschen** und insbesondere gegenüber Flüchtlingen weiter verstärkt. Derartige Eingriffe sind nur verfassungsgemäß, wenn diese verhältnismäßig sind, d. h. wenn sie geeignet, erforderlich und angemessen sind. Sind neue gesetzliche Maßnahmen geeignet und für legitime Zwecke erforderlich, so bedarf es zur Sicherung des Datenschutzes und der Angemessenheit der informationellen Eingriffe geeigneter Garantien und Schutzmaßnahmen.

Für derartige Schutzmaßnahmen sind folgende Aspekte von besonderer Relevanz:

- Nichtdeutsche, insbesondere Flüchtlinge aus Ländern außerhalb der EU, haben in gleichem Maße wie Bürgerinnen und Bürger der Bundesrepublik Deutschland bzw. von EU-Mitgliedstaaten einen **Schutzanspruch hinsichtlich ihres Grundrechtes auf Datenschutz**.

- Viele dieser Menschen sind nicht bzw. nur in einem geringen Maße der deutschen Sprache mächtig und sind mit den gesetzlichen, organisatorischen und technischen Rahmenbedingungen informationeller Eingriffe nicht vertraut. Sie kennen oft weder die teilweise hochkomplexen Regelungen noch die faktischen Gegebenheiten und Hintergründe ihrer informationellen Erfassung und Kontrolle. Sie haben, strukturell und kulturell bedingt, faktisch nur sehr begrenzte oder keine Möglichkeiten, ihre informationellen Grundrechte individuell durchzusetzen. Sie sind bisher auch nicht so organisiert und mit Rechten ausgestattet, dass sie ihre gemeinsamen Interessen kollektiv vertreten können. Sie sind deshalb ihrer informationellen Erfassung und Überwachung oft **schutzlos ausgeliefert**.

- Angesichts dieses faktischen Ausgeliefertseins muss eine Instanz befugt werden, die Interessen sowie die Freiheits- und Grundrechte von Nichtdeutschen auch rechtlich wahrzunehmen. Hierfür ist im Aufenthaltsgesetz generell die Etablierung der oder des **Integrationsbeauftragten** vorgesehen (§§ 92-94 AufenthG). Dieser hat aber nur geringe finanzielle und personelle Ressourcen und ist wegen seiner Benennung und seiner hierarchischen Einbindung nicht unabhängig. Seine rechtlichen Möglichkeiten beschränken sich auf informelle Aktivitäten. Es bedarf daher zusätzlicher, geeigneterer Maßnahmen, um das Grundrecht auf Datenschutz von Nichtdeutschen zu gewährleisten.

- Für die Datenschutzkontrolle – auch soweit sie Nichtdeutsche betrifft – sind die unabhängigen **Datenschutzaufsichtsbehörden** des Bundes und der Länder zuständig. Ausweislich der Tätigkeitsberichte dieser Behörden spielt der Datenschutz für ausländische Staatsangehörige trotz der gerade gegenüber diesen Menschen erfolgenden speziellen Erfassungs- und Kontrollmaßnahmen hier eine untergeordnete Rolle. Dies ist zum einen dem Umstand zuzuschreiben, dass von Nichtdeutschen dort wenig Eingaben und Beschwerden eingehen, was insbesondere auf deren kulturelle Distanz zum Thema Datenschutz zurückzuführen ist. Dies macht umso mehr anlasslose Kontrollen nötig, wofür vor allem bei den zuständigen Aufsichtsbehörden der Länder die erforderlichen Ressourcen fehlen.

  Dringend nötig ist daher die Bereitstellung der nötigen **personellen und finanziellen Ressourcen für Aufsichtsbehörden**, damit diese in dem sensiblen Bereich der Ausländerüberwachung die erforderlichen Informations- und Kontrollmaßnahmen durchführen können.

Art. 80 DSGVO sieht vor, dass der nationale Gesetzgeber befugt ist, speziellen Einrichtungen die Befugnis zu übertragen, die Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten rechtlich – auch gerichtlich – wahrzunehmen. Eine derartige gesetzliche Beauftragung erfolgte gegenüber zertifizierten Verbraucherschutzorganisationen zur Wahrung des Datenschutzes für Verbraucherinnen und Verbraucher (§ 2 Abs. 1 Nr. 11 UKlaG). Nichtdeutsche sind hinsichtlich ihrer informationellen Erfassung und Kontrolle in einer ähnlichen individuellen Situation des Ausgeliefertseins wie Verbraucherinnen und Verbraucher gegenüber ökonomisch mächtigen Datenverarbeitern. Es sollte daher vorgesehen werden, entsprechende **gesetzliche kollektive Rechtsschutzmöglichkeiten** zu etablieren. Dies kann in der Form erfolgen, dass privatrechtlich organisierte Institutionen (z. B. Pro Asyl, Flüchtlingsräte, Beratungsstellen der Wohlfahrtsverbände) nach einer entsprechenden Zertifizierung (vgl. § 4 UKlaG) gesetzlich befugt werden, kollektiv das Recht auf Datenschutz für ausländische Staatsangehörige in der Verwaltung und vor Gerichten wahrzunehmen. Eine derartige gesetzliche Garantie ist europarechtlich und verfassungsrechtlich geboten. Eine entsprechende Zulassung der kollektiven Rechtswahrnehmung i. S. v. Art. 80 DSGVO ist deshalb zusätzlich im 2. DAVG vorzusehen.

C. Stellungnahme zu einzelnen Regelungen

Zu folgenden Einzelvorschlägen erfolgt eine spezifische Stellungnahme:

Zu § 3 Abs. 3a AZRG-E
Bei vollziehbar ausreisepflichtigen Ausländern sollen künftig zusätzlich u. a. **biometrische Daten** (Fingerabdrücke, Größe, Augenfarbe) gespeichert werden. Eine generelle Erforderlichkeit hierfür ist nicht zu erkennen. Dies gilt insbesondere, wenn bei den Betroffenen eine Ausreisebereitschaft besteht. Der angegebene Zweck einer besseren Identifizierbarkeit im Sicherheitsverfahren (S. 51) wird nicht näher erläutert.

Zu § 10 Abs. 4 AZRG-E
Durch die zusätzlichen **Nutzungsmöglichkeiten der AZR-Nummer**, insbesondere für Datenübermittlungen zu Flüchtlingen von öffentlichen Stellen untereinander (Nr. 3) überschreitet diese ihre Funktion als zweckbezogene Ordnungsnummer (Weichert in Däubler u .a., EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Art. 87 Rn. 19) und wird zur nationalen Kennziffer, ohne dass die nach Art. 87 DSGVO vorgesehenen Garantien gegeben werden (s. o. A und B)

Zu § 11 Abs. 2 AZRG-E

Die Regelung enthält eine generelle **Befugnis zur Weiterübermittlung** von erlangten AZR-Daten, wenn die Daten „unmittelbar hätten übermittelt werden dürfen“. Damit wird die Funktion des AZR als Datendrehscheibe weiter ausgebaut, ohne dass die Zweckbindung noch wirksam überprüft werden kann. Eine auf S. 3 vorgesehene Verpflichtung zur Überprüfung der Richtigkeit und Aktualität der Daten erfolgt, wie in der Begründung behauptet (S. 54), nicht obligatorisch durch eine erneute AZR-Abfrage. So besteht die Gefahr, dass übermittelte, für den Betroffenen negative Informationen ein Eigenleben entwickeln, ohne dass diese hiergegen eine wirksame Handhabe hätten. Gerade bei AZR-Daten kommt es wegen deren existenzieller Relevanz sowie den möglichen kurzen Änderungsperioden darauf an, dass die Daten von der (verifizierten) Datenquelle stammen. Mit der Regelung wird damit dem Grundsatz der Datenrichtigkeit nach Art. 5 Abs. 1 lit. d DSGVO nicht hinreichend genügt.

Zu § 13 Abs. 3 AZRG-E
Die neue Regelung sieht vor, dass bei **AZR-Abrufen durch deutsche Nachrichtendienste** (BfV, LfV, MAD, BND) eine Protokollierung ausschließlich dort und nicht mehr beim AZR erfolgt. Dies hat zur Folge, dass das weiterhin für die Übermittlung mit verantwortliche AZR keine Überprüfung durchführen kann und dass generell die Prüfung der Zulässigkeit der Abrufe massiv erschwert wird. Hackern würde es ermöglicht, mit den Zugangsmöglichkeiten der Nachrichtendienste unerkannt Daten aus dem AZR abzurufen. Die Begründung für die Regelung, nämlich die „Vermeidung von Doppelaufwänden“ (S. 54), ist vorgeschoben, da Protokollierungen automatisiert erfolgen und die damit verbundene Speicherung keinen wesentlichen zusätzlichen Aufwand darstellt. Die Begründung ignoriert zudem mit ihrem Hinweis auf die Geheimhaltungsbedürftigkeit dieser Protokolldaten den Umstand, dass Protokolldaten durch eine enge Zweckbindung ohnehin einer spezifischen Geheimhaltung unterliegen (vgl. § 37 Abs. 1 S. 1 Nr. 2 AZRG). Von „massiven Kostenfolgen“, selbst bei einer gesonderten abgeschotteten Protokollierung, kann keine Rede sein.

Zu § 18g AZRG-E
Die zusätzlich vorgesehene Datenübermittlung an die **Träger der Deutschen Rentenversicherung** folgt dem Ansatz, das AZR zu einer umfassenden Informationsdrehscheibe für sämtliche Verwaltungsaufgaben zu Nicht-Deutschen auszubauen. Zwar wird für die Übermittlung die Einwilligung der Betroffenen vorausgesetzt. Diese reduziert sich aber wegen der sozialrechtlichen Kooperationspflicht auf eine wenig freiwillige Obliegenheit (§ 60 SGB I).

Zu § 22 Abs. 1, 2 AZRG-E
Die Voraussetzungen für die Einrichtung von **automatisierten Abrufmöglichkeiten** sollen abgesenkt und auf eine Vielzahl weiterer Stellen ausgeweitet werden. Es genügt die Häufigkeit der Übermittlungsersuchen oder deren Eilbedürftigkeit. Dadurch wird das Risiko einer unzulässigen Zweckänderung oder eines Missbrauchs von AZR-Daten massiv erhöht, ohne dass hinreichende zusätzliche Sicherungsvorkehrungen vorgesehen sind.

Zu § 22 Abs. 3 AZRG-E
Es ist geplant, die Regelung zu streichen, wonach der automatisierte Abruf „nur von Bediensteten vorgenommen werden“ darf, die „hierzu besonders ermächtigt worden sind“. Damit wird das Missbrauchsrisiko weiter und ohne Not erhöht: Es obliegt ausschließlich den abrufenden Behörden festzulegen, wer Daten vom AZR abruft. Angesichts der (künftigen) Vielzahl der online abfragenden Behörden und der Beliebigkeit der dazu autorisierten Personen ist die Zuverlässigkeit bei der Abfrage der hochsensiblen AZR-Daten nicht mehr gewährleistet. Die in der Begründung genannte Rechtfertigung für die Streichung, die mangelnde Flexibilität bei „Abwesenheiten und Aufgabenveränderungen“ (S. 1), ist vorgeschoben, da es jeder abrufenden Stelle – auch Kommunen – zuzumuten ist, alle abfrageberechtigten Personen zu benennen und entsprechend vom AZR autorisieren zu lassen und für die Abfrage zu authentisieren. Durch die Authentisierung nicht mehr der abfragenden Personen, sondern der **Organisationseinheiten** (S. 4) wird es für das AZR

erheblich schwieriger, missbräuchliche Abrufe systematisch zu erkennen und aufzuklären. Der Verweis auf die Regelungen der DSGVO, des BDSG sowie die Geheimdienstgesetze sowie eine Protokollauswertung durch die insofern oft wenig geschulten abrufenden Stellen (S. 60 f.) stellt keine hinreichende Kontrollvorkehrung dar. Die Streichung dieser Änderung wurde auch vom Bundesratsausschuss aus den genannten Gründen empfohlen (BR-Drs. 54/1/19 Nr. 14).

Der Bundesrat fordert weitere Möglichkeiten des Online-Abrufs im AZR im Zusammenhang mit der **Verteilung von unbegleiteten minderjährigen Flüchtlingen** (BR-Drs. 54/19 – Beschluss, Nr. 5). Es ist nicht nachvollziehbar dargetan, weshalb zusätzlich zu den Jugendämtern auch die Landesverteilstellen direkten Zugang zum AZR benötigen.

Zu § 49 Abs. 6 S. 2, Abs. 8 S. 3 und Abs. 9 S. 3 AufenthG-E, § 16 Abs. 1 S. 2 AsylG-E
Die **Absenkung des Alters** für die Zulässigkeit der Abnahme von **Fingerabdrücken** von derzeit 14 auf 6 Jahre begegnet schwerwiegenden persönlichkeitsrechtlichen Bedenken. Wegen des Wachsens der Kinder sind auch deren Abdrücke Wachstumsprozessen und Änderungen ausgesetzt. Bei der Erfassung solcher Abdrücke bei Kindern bestehen regelmäßig hohe Qualitätsdefizite. Im Entwurf sind keine Nutzungseinschränkungen vorgesehen, so dass die Nutzung dieser Abdrücke durch Sicherheitsbehörden möglich ist. Dadurch laufen die Kinder Gefahr, trotz Strafunmündigkeit in polizeiliche Ermittlungen einbezogen zu werden. Es besteht umgekehrt auch das Risiko, dass diese Fingerabdrücke erheblich später für polizeiliche Ermittlungen und zur Verdachtsgenerierung verwendet werden. Für eine Erforderlichkeit der Absenkung des Alters werden in der Begründung keine Hinweise gegeben. Es ist nicht nachvollziehbar, wie, so die Begründung, mit dieser Maßnahme das Kindeswohl geschützt werden könnte, um „etwaigen Straftaten zu Lasten des Kindes entgegenzuwirken“ (S. 70). Diese Kritik wurde von den Ausschussempfehlungen aufgegriffen, aber vom Bundesrat nicht übernommen (BR-Drs. 54/1/19 Nr. 17).

Die in der Begründung (S. 70, 72) genannten Einschränkungen, wonach die ED-Maßnahmen nicht dem Kindeswohl entgegenstehen dürfen und die **Kinder- und Jugendhilfe Primat** habe und kein unmittelbarer Zwang angewendet werden dürfe, finden im Gesetzestext keinen Rückhalt.

Zu § 56a AufenthG-E
Im Beschluss des Bundesrats vom 15.03.2019 ist vorgesehen, dass ausreisepflichtige Ausländer mit elektronischer Aufenthaltsüberwachung verpflichtet werden, „ein zur Verfügung gestelltes Mobiltelefon ständig in betriebsbereitem Zustand bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen.“ Diese **Verpflichtung zu dauernden Erreichbarkeit** und die damit verbundene dauernde Kontrollmöglichkeit stellen weitergehende Einschränkungen der Freiheitsrechte der Betroffenen dar. In der Begründung wird darauf hingewiesen, dass diese Maßnahme nicht erforderlich sei. Sie sei aber sinnvoll, für die „gemeinsame elektronischen Überwachungsstelle der Länder (GÜL) mit Sitz in Hessen, um den Ausländer kontaktieren und eventuelle Problemlagen niedrigschwellig lösen zu können.“ (BR-Drs. 54/19 – Beschluss, Nr. 9). Eine Einwilligung der Betroffenen ist nicht vorgesehen. Die vorgesehene Maßnahme ist erklärtermaßen unverhältnismäßig und deshalb verfassungswidrig.

Zu § 73 AufenthG-E
Die Regelung sieht vor, dass im Rahmen von **Zuverlässigkeits- und Sicherheitsüberprüfungen** nach dem AufenthG neben Anfragen beim BKA, beim ZKA sowie bei den deutschen Nachrichtendiensten des Bundes auch Abfragen bei der Bundespolizei standardmäßig erfolgen. Angesichts der vielen dort vorhandenen Informationen, die auf konkrete Kontakte mit der Bundespolizei zurückgehen (S. 51), ohne dass hierbei i. d. R. abgeschlossene Verwaltungsverfahren dokumentiert sind, besteht die Gefahr, dass ungesicherte Informationen einfließen und zum Nachteil der Betroffenen genutzt werden. Angesichts des Austauschs zwischen den Sicherheitsbehörden ist davon auszugehen, dass

relevante Informationen schon bei den bisherigen Anfragen bekannt werden. Es ist nicht erkennbar, weshalb die bisherigen – schon äußerst weit gehenden – Anfragen für valide Überprüfungen nicht ausreichen und eine zusätzliche Anfrage bei der Bundespolizei notwendig ist.

Zu § 31 Abs. 7 AsylG-E
Die **AZR-Nummer** soll künftig auf den Entscheidungen des Bundesamtes für Migration und Flüchtlinge aufgeführt werden, um sie z. B. zur weiteren Verwendung Sozialbehörden zugänglich zu machen (S. 79). Damit wird die Funktion der AZR-Nummer weit über die einer Ordnungsnummer ausgeweitet und zu einer nationalen Kennziffer gemacht, ohne dass die dabei geforderten Vorkehrungen getroffen werden (s. o. A).

Zu Art. 11 Datenaustauschverbesserungsgesetz (DAVG)
Es gibt keinen Anlass, auf eine **Evaluierung** des 1. DAVG bis Ende 2019 zu verzichten. Gerade im Hinblick auf die dort vorgesehenen und im 2. DAVG geplanten weitergehenden Verschärfungen und Eingriffe ins Recht auf informationelle Selbstbestimmung sowie in andere Grundrechte ist eine frühzeitige Bestandsaufnahme notwendig, um möglichst zeitnah evtl. nötige Korrekturen vornehmen zu können. Ein Verschieben der Evaluation ist kein Beitrag zum Bürokratieabbau, wie im Referentenentwurf zu dem vorliegenden Gesetz angegeben, sondern eher einer zum Grundrechtsabbau.

Für Rückfragen und weitere Erläuterungen stehen wir gerne zur Verfügung

Mit freundlichen Grüßen
Dr. Thilo Weichert