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 das
Bundesministerium des Innern, für Bau und Heimat
Referat M5 – Informationstechnik und Statistik im
Bereich Migration und Asyl; soziale Leistungen
Alt-Moabit 140
10557 Berlin

Kiel, den 04.11.2018

Stellungnahme des Netzwerks Datenschutzexpertise

Zum Referentenentwurf des Bundesregierung
Entwurf eines Zweiten Gesetzes zur Verbesserung der Registrierung und des Datenaustauschs zu aufenthalts- und asylrechtlichen Zwecken
Verbändeanhörung zum Referentenentwurf für ein Zweites Datenaustauschverbesserungesetz (2. DAVG) Stand 18.10.2018, Ihre Mail an Verbände vom 18.10.2018, Az. M%-21000/84#3

Sehr geehrte Damen und Herren,

durch eine Rückfrage eines von Ihnen bei der in der Bezugszeile angeschriebenen Verbands hat das Netzwerk Datenschutzexpertise Kenntnis erlangt von dem im Betreff genannten Referentenentwurf. Wegen der hohen datenschutzrechtlichen Relevanz erlauben wir uns, hierzu Stellung zu nehmen.

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, insbesondere dadurch verbessert werden, 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 neuen Regelungsinhalte nennt der Entwurf folgende Aspekte
- Authentisierung von Onlineabrufen vom AZR durch Organisationen statt Einzelpersonen,
- Verwendung der AZR-Nummer in der Kommunikation zwischen beteiligten Stellen,
- erleichterte Weiterverarbeitung abgerufener AZR-Daten,
- verbindliche Festlegung einer technischen Kommunikationsschnittstelle mit dem AZR,
- Erweiterung der Zuständigkeit der Bundespolizei für 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,
- Ausweitung der Speicherung von Identifizierungsdaten zur Durchführung von Abschiebungen,
- zentralisierte Speicherung von Daten zur Förderung der Ausreise.

Der Gesetzentwurf zeichnet sich dadurch aus, dass hinsichtlich der technischen Überwachung von Flüchtlingen eine Ausweitung erfolgt, ohne dass auch nur eine 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 einer 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 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 diese auch administrativen Einfluss erhalten können, sollten Vorkehrungen für den Fall ergriffen werden, dass derartige Daten zur Diskriminierung und Verfolgung von Minderheiten genutzt werden sollen. Dies wurde bisher und wird erneut im vorliegenden Entwurf versäumt.

Im Referentenentwurf sind geht es insbesondere um die Verarbeitung von Daten zu Flüchtlingen, von denen viele wegen **politischer Verfolgung** Anträge auf Asyl und auf Anerkennung einer politischer Verfolgung stellen. Gemäß Art. 9 Abs. 1 DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten grds. untersagt. Hierzu zählen u. a. Daten, aus denen politische Meinungen hervorgehen. Die Ansicht, politische verfolgt zu sein und einen Anspruch auf Asyl nach Art. 16a GG zu haben, stellt selbst eine politische Meinung dar. Selbst der Umstand, einen Asylantrag gestellt zu haben, kann politische Verfolgung begründen. Ebenso handelt es sich bei Angaben des Flüchtlings zur Begründung seines Asylantrags sowie bei den Entscheidungen hierüber 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 darin, dass die AZR-Daten über das AZR selbst oder über abfragende 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.

Gemäß Art. 87 der europäischen Datenschutz-Grundverordnung 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). Die europarechtlichen 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 Ausländer, insbesondere für die erfassten Flüchtlingen, nicht gilt bzw. über die Zwischenschaltung des AZR aufgehoben wird. Art. 6 Abs. 4 DSGVO verbietet bei der personenbezogenen Datenverarbeitung das Verfolgen von Zwecken, die miteinander nicht vereinbar sind. 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).

Der Entwurf berücksichtigt teilweise nicht in Bezug auf inhaltliche Regelungen, die Terminologie sowie Verweisungen, dass seit dem 25.05.2018 die europäische **Datenschutz-Grundverordnung** (DSGVO) direkt gültig ist.

Zu folgenden Einzeländerungen 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 Zweck dieser zusätzlichen Angaben wird nicht näher erläutert (S. 39).

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.) Die in der Begründung für die Regelung behauptete Instabilität der Identität bei Asylsuchenden und Asylbewerbern generell (S. 42) wird nicht näher untermauert und ist zu hinterfragen.

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 das AZR zu einer Datendrehscheibe, ohne dass die Zweckbindung noch wirksam überprüft werden kann. Zugleich besteht durch die Weiterübermittlung ohne Rückversicherung im AZR, ob diese Daten noch aktuell und richtig sind, 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. Die in der Begründung (S. 42) aufgestellte Behauptung, die übermittelnde Stelle müsse sich vor der Weitergabe über die Aktualität der Daten vergewissern, findet im Gesetzestext keine Grundlage. Mit der Regelung wird damit strukturell der Grundsatz der Datenrichtigkeit nach Art. 5 Abs. 1 lit. d DSGVO verletzt.

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. 43) 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 generell 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 § 22 Abs. 2 AZRG-E

Die Einrichtung von **automatisierten Abrufmöglichkeiten** sollen künftig nur noch von der Häufigkeit der Übermittlungsersuchen oder deren Eilbedürftigkeit abhängig sein, also, so die Begründung (S. 44), „allen relevanten Behörden" eröffnet werden. 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, 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. 3) wird es für das AZR erheblich schwieriger, missbräuchliche Abrufe systematisch zu erkennen und aufzuklären. Der Verweis auf eine Protokollauswertung durch die insofern oft wenig geschulten abrufenden Stellen (S. 44) stellt keine hinreichende Kontrollvorkehrung dar.

Zu § 34a AZRG

Durch den Verweis bzgl. der **datenschutzrechtlichen Kontrolle** auf den nicht mehr gültigen § 24 Abs. 1 BDSG-alt, der seit Mai 2018 durch Art. 57 DSGVO ersetzt wurde, zeigen die Autoren des Entwurfes ihre beschränkten Kenntnisse in Bezug auf das neue Datenschutzrecht. Die Regelung ist insgesamt überflüssig und sollte gestrichen werden.

Zu § 37 AZRG

Der verwendete Begriff der „Sperrung“ ist durch den der „**Einschränkung der Verarbeitung**“ zu ersetzen (vgl. Art. 18 DSGVO). Der Verweis auf den nicht mehr gültigen § 20 Abs. 5 BDSG-alt läuft ins Leere. Anwendbar ist umfassend Art. 18 DSGVO und verdrängt in jedem Fall § 37 Abs. 1 S. 1 Nr. 1 und S. 2 AZRG. Abs. 2 muss, soll er überhaupt beibehalten werden, der neuen europäischen Rechtslage angepasst werden.

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. 50).

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 § 86a AufenthG-E

Zur **Förderung der Ausreise** sollen an öffentliche sowie private und internationale Stellen Daten weitergegeben werden können. Dazu sollen nach Abs. 1 letzter Anstrich „weitere Angaben zur Person unter Beachtung von Artikel 9 Abs. 1 DSGVO“ gehören. Der Inhalt dieser Regelung ist unklar und erschließt sich auch nicht in der Begründung (S. 53). Er darf aber angesichts der in Art. 9 Abs. 1 DSGVO genannten sensitiven Merkmale nur so verstanden werden, dass die Weitergabe derartiger Merkmale nicht erlaubt ist. Dies sollte explizit und unmissverständlich klargestellt werden.

Zu § 71 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. 56). 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.).

Zu Art. 13 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 (S. 58), sondern eher einer zum Grundrechtsabbau.

Mit freundlichen Grüßen

Dr. Thilo Weichert