



**Stellungnahme der Datenschutzkonferenz zum  
Entwurf eines Zweiten Datenaustauschverbesserungsgesetz (2. DAVG-E)**

*Stand: 28.05.2019*

Das Datenaustauschverbesserungsgesetz vom 2. Februar 2016 (BGBl. I S. 130) bezweckte, Asyl- und Schutzsuchende sowie Ausländer, die unerlaubt nach Deutschland einreisen oder sich unerlaubt aufhalten, frühzeitig zentral zu registrieren und die dabei erfassten Daten im Ausländerzentralregister (AZR) medienbruchfrei denjenigen öffentlichen Stellen zur Verfügung zu stellen, die sie für die Erfüllung ihrer jeweiligen Aufgabe benötigten. Ausweislich der Gesetzesbegründung zum 2. DAVG-E (BT- Drs. 19/8752, Stand: 27. März 2019, S. 1) ist in den Ländern und Kommunen der Bedarf entstanden, die Nutzungsmöglichkeiten des AZR weiter zu entwickeln. Ziel des 2. DAVG-E ist es daher, die Verwaltungsabläufe weiter zu digitalisieren, um eine medienbruchfreie Kommunikation zwischen den Verfahrensbeteiligten zu erreichen, die Abläufe in den öffentlichen Stellen zu beschleunigen und vor allem die Nutzungsmöglichkeiten des AZR zu erhöhen (BT-Drs. 19/8752, S. 33).

Die beabsichtigten Änderungen begegnen erheblichen datenschutzrechtlichen Bedenken. Diese wurden schon in der Anhörung zum Referentenentwurf des Bundesinnenministeriums seitens verschiedener Verbände breit gefächert vorgetragen, allerdings nicht hinreichend berücksichtigt. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat in seiner Stellungnahme an den Innenausschuss des Deutschen Bundestages vom 18. Februar 2019 verschiedene Kritikpunkte aufgeführt, die trotz seiner vorherigen Beteiligung im Gesetzgebungsverfahren bis dato nicht in den derzeitigen Gesetzentwurf eingeflossen sind. Darüber hinaus hat das Netzwerk Datenschutzexpertise in seiner Stellungnahme vom 22. März 2019 massive Bedenken gegen die geplanten Änderungen durch das 2. DAVG-E geäußert. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist mit dieser Stellungnahme- unter Berücksichtigung der eben genannten Stellungnahmen - auf die datenschutzrechtliche Problematik insbesondere der folgenden Vorschriften hin:

1. Durch Artikel 1 Nr. 4 des 2. DAVG-E soll **§ 10 Abs. 4 Satz 2** des Ausländerzentralregistergesetzes (**AZRG**) neu gefasst werden. Bisher regelte dieser Satz, dass die AZR-Nummer neben dem Verkehr mit dem Register darüber hinaus nur für Datenübermittlungen zwischen dem Bundesamt für Migration und Flüchtlinge und den Ausländerbehörden genutzt werden darf. Die AZR-Nummer dient dazu, den Datensatz eines Ausländers aus dem AZR abzurufen; sie ist veränderungsstabil und nur einer bestimmten Person zugeordnet. Der im AZR gespeicherte Datensatz ist dabei äußerst umfangreich und umfasst unter anderem Namen, Geburtsdatum und -ort, Familienstand, Angaben zum aufenthaltsrechtlichen Status, Fingerabdruckdaten, Größe und Augenfarbe, freiwillige Angaben zu Telefonnummer und E-Mailadresse, durchgeführte Gesundheitsuntersuchungen, Schulbildung, Beruf und die Teilnahme an Integrationskursen. Mit der beabsichtigten Änderung des § 10 Abs. 4 Satz 2 AZRG soll die AZR-Nummer nun zur Datenübermittlung zwischen einer Vielzahl anderer Behörden genutzt werden dürfen und damit die Nutzungsmöglichkeit erheblich erweitert werden. Dadurch besteht die Gefahr, wie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in seiner o.g. Stellungnahme darlegte, dass sich die AZR-Nummer immer weiter von ihrer ursprünglichen Nutzung als Ordnungszahl entfernt und sich zu einer unzulässigen Personenkenzahl entwickelt. Das Bundesverfassungsgericht hat schon in seinem Volkszählungsurteil (BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 – zitiert nach: <https://openjur.de/u/268440.html>, Rn. 118) ausgeführt, dass die unbeschränkte Verknüpfung der erhobenen Daten mit den bei den Verwaltungsbehörden vorhandenen, zum Teil sehr sensitiven Datenbeständen oder gar die Erschließung eines derartigen Datenverbundes durch ein einheitliches Personenkenzeichen oder sonstiges Ordnungsmerkmal unzulässig ist, denn eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebensdaten und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger ist auch in der Anonymität statistischer Erhebungen unzulässig (BVerfGE 27, 1 [6]). .

Durch die vorgesehene, weitreichende Nutzung der AZR-Nummer zur Datenübermittlung zwischen einer Vielzahl von Behörden, auch außerhalb von aufenthaltsrechtlichen Zwecken, ändern sich die ursprünglichen Zwecke dieser Ordnungsnummer. War diese ursprünglich nur zum Zweck der eindeutigen Adressierung des im AZR gespeicherten Datensatzes und nur in asyl- und aufenthaltsrechtlichem Kontext verwendet worden, entwickelt sie sich durch die geplanten Änderungen zu einem Instrument, das die umfassende Verwaltung der

Daten der betroffenen Ausländer ermöglicht (vgl. Stellungnahme des Netzwerkes Datenschutzexpertise, S. 3). Der Bundesrat hat in seiner Stellungnahme vom 15. März 2019 sogar gefordert, dass die AZR-Nummer zwischen den leistungsgewährenden Behörden auch dann noch verwendet werden darf, wenn schon eine Versicherungsnummer nach dem Vierten Buch Sozialgesetzbuch bekannt ist (BR-Drs. 54/19, Beschluss, S. 2 f.). Dem hat die Bundesregierung in ihrer Gegenäußerung (BT-Drs. 19/8752, Anlage 5, S. 103) zwar widersprochen, das Ansinnen des Bundesrates zeigt aber dennoch deutlich, dass die Länder eine noch weitergehende Ausweitung der Nutzungsmöglichkeiten der AZR-Nummer für erforderlich halten.

Auch wenn die dahinterstehende Intention nachzuvollziehen ist, die betroffene Person in jedweder Situation eindeutig identifizieren zu können, um beispielsweise Leistungsbetrug durch Mehrfachidentitäten zu verhindern, ist zu bedenken, dass das Grundrecht auf informationelle Selbstbestimmung, das auch für die betroffenen Ausländer Geltung beansprucht, einen Eingriff nur gestattet, wenn dieser verhältnismäßig ist. Dies ist in Anbetracht der weitgehenden geplanten Nutzungen kaum denkbar. Die Gefahr, dass sich die AZR-Nummer von ihrer ursprünglichen Nutzung als Ordnungsnummer zu einer unzulässigen Personenkenzahl entwickelt, wird auch in Art. 5 Nr. 5 des 2. DAVG-E deutlich. Dort wird u.a. die Einführung des **§ 63 Abs. 5 Satz 1 Nr. 3 des Asylgesetzes (AsylG)** vorgeschlagen und vorgesehen, dass die AZR-Nummer auch auf der Bescheinigung zur Aufenthaltsgestattung zusätzlich aufgeführt wird. Dadurch wird eine weitere Zusammenführung von Lebensdaten ermöglicht. Auch durch Art. 8 Nr. 1 des 2. DAVG-E, der eine Änderung des Bundesmeldegesetzes (BMG) vorsieht, wird diese Gefahr erneut deutlich. In **§ 3 Abs. 1 Nr. 17 a BMG** ist anstelle der Seriennummer des Ankunftsnachweises nun die Speicherung der AZR-Nummer im Melderegister vorgesehen. Die Seriennummer wird nur noch übergangsweise beibehalten.

Darüber hinaus bestehen gravierende Bedenken, dass die geplante Nutzung der AZR-Nummer mit den Vorgaben des Art. 87 Datenschutz-Grundverordnung (DS-GVO) vereinbar ist. Nach Art. 87 DS-GVO können die Mitgliedstaaten näher bestimmen, unter welchen spezifischen Bedingungen eine nationale Kennziffer oder andere Kennzeichen von allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen. In diesem Fall darf die nationale Kennziffer oder das andere Kennzeichen von allgemeiner Bedeutung nur unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person gemäß der DS-GVO verwendet werden. Die

Ausschüsse des Bundesrates hatten dem Bundesrat in ihren Empfehlungen vom 4. März 2019 (BR-Drs. 54/1/19, Empfehlungen, S. 8) in Vorbereitung seiner Stellungnahme nahegelegt, dass im weiteren Gesetzgebungsverfahren diese Frage geprüft werden solle. Aus der Gesetzesbegründung der Bundesregierung sei weder ersichtlich, ob die Bundesregierung den Anwendungsbereich des Art. 87 DS-GVO für eröffnet erachtet, noch ob besondere, von der DS-GVO geforderte Vorkehrungen zum Schutz der Wahrung der Rechte und Freiheiten der betroffenen Ausländer vorgesehen werden. In Anbetracht der angedachten weiten Nutzungsmöglichkeiten kann die AZR-Nummer als nationale Kennziffer oder anderes Kennzeichen von allgemeiner Bedeutung betrachtet werden, sodass entsprechende Garantien für die Wahrung der Rechte und Freiheiten der betroffenen Personen getroffen werden müssten. Diese sind in dem Gesetzentwurf, wie das Netzwerk Datenschutzexpertise in seiner Stellungnahme auf S. 3 bereits erläutert hat, trotz der Risiken, die dem AZR innewohnen, nicht ersichtlich. Als geeignete Garantien kämen insbesondere technische und organisatorische Maßnahmen in Betracht, wie etwa Vorgaben zur Zugriffssicherung der beteiligten Systeme, sowie wirksame Überwachungs- und Kontrollmechanismen. Die Überwachung und Kontrolle der Einhaltung datenschutzrechtlicher Bestimmungen obliegt den Aufsichtsbehörden des Bundes und der Länder. Eine angemessene Kontrolle ist nur mit dem dafür erforderlichen Personal durchführbar. Hieran fehlt es leider. Die Vorgaben des Art. 87 DS-GVO wären somit nicht eingehalten und der neue § 10 Abs. 4 Satz 2 AZRG-E unionsrechtswidrig.

2. Durch Art. 1 Nr. 7 des 2. DAVG-E soll der bisherige **§ 14 Abs. 1 AZRG** geändert werden. Dort werden die Grunddaten definiert, die auf Ersuchen jeder öffentlichen Stelle übermittelt werden dürfen. Zusätzlich zu den dort aufgeführten Angaben soll zukünftig auch die Anschrift im Bundesgebiet bzw. die Erteilung einer Niederlassungserlaubnis oder einer Erlaubnis zum Daueraufenthalt-EU des betroffenen Ausländers übermittelt werden dürfen. In Zusammenhang mit der geplanten Erweiterung der Grunddaten ist kritisch zu sehen, dass die ersuchende Stelle gemäß **§ 10 Abs. 1 Satz 2 AZRG** nicht verpflichtet ist, den Zweck des Übermittlungersuchens anzugeben. Dies ist zwar nicht erst seit der beabsichtigten Änderung des AZRG der Fall. Allerdings wird die fehlende Rechtfertigung bezüglich des beabsichtigten Verwendungszwecks immer brisanter, je mehr der Datenbestand anwächst, der übermittelt wird. Wie die Ausschüsse dem Bundesrat bereits dargelegt haben (BR-Drs. 54/1/19, Empfehlungen, S. 13), steht die fehlende Verpflichtung der

ersuchenden Behörde, den Verarbeitungszweck anzugeben, in Konflikt mit dem Zweckbindungsgrundsatz aus Art. 5 Abs. 1 Buchstabe b DS-GVO. Danach müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben und in einer mit diesen Zwecken zu vereinbarenden Weise weiterverarbeitet werden. Durch die fehlende Verpflichtung zur Angabe des beabsichtigten Verarbeitungszwecks besteht die Gefahr, dass die Daten durch die ersuchende Behörde im Zweifel zu missbräuchlichen Zwecken angefordert werden können, ohne dass dies kontrolliert werden kann und somit der Zweckbindungsgrundsatz unterlaufen wird.

3. Durch Art. 1 Nr. 13 Buchstabe a des 2. DAVG-E soll der bisherige **§ 22 Abs. 1 AZRG** insofern geändert werden, als dass der Katalog derjenigen Behörden, die die Daten der Betroffenen aus dem AZR im automatisierten Verfahren abrufen können, um eine beträchtliche Anzahl an Behörden erweitert wird. In seiner Stellungnahme (BR-Drs. 54/19, Beschluss, S. 1f.) bat der Bundesrat zusätzlich zu der bereits geplanten Erweiterung der abrufberechtigten Behörden darum, im weiteren Gesetzgebungsverfahren geeignete Regelungen zu treffen, damit auch die für Integrationsmaßnahmen zuständigen Stellen der Länder und Kommunen die für ihre Arbeit erforderlichen im AZR gespeicherten Daten, auch im automatisierten Verfahren abrufen können. Die Bundesregierung hält diesen Vorschlag ausweislich ihrer Gegenäußerung für erwägenswert (BT-Drs. 19/8752, Anlage 5, S. 103). Allerdings besteht auch dadurch, wie oben bereits dargelegt, die Gefahr, dass die AZR-Nummer, die ja für den automatisierten Abruf benötigt wird, für immer weitergehende Zwecke verwendet wird, als ursprünglich angedacht. Insofern trägt auch diese beabsichtigte Regelung dazu bei, die Gefahr einer Personenkennzahl zu erhöhen. Darüber hinaus ist die Bezeichnung der „für Integrationsmaßnahmen zuständigen Stellen der Länder und Kommunen“ sehr weitgehend und kollidiert insofern mit dem Gebot der Bestimmtheit. Zudem wird es durch die Vielzahl an abrufenden Behörden schwieriger, Missbrauchsfälle aufzuklären. Abschließend soll an dieser Stelle auch auf die Gefahr hingewiesen werden, dass durch die massive Erweiterung der abrufenden Behörden das Prinzip der Datenminimierung gemäß Art. 5 Abs. a Buchstabe c DS-GVO verletzt werden kann. Durch den automatisierten Abruf durch Eingabe der AZR-Nummer ist es möglich, den gesamten, einer eindeutig identifizierbaren Person zugeordneten Datensatz einzusehen bzw. die Daten weiter zu verwenden. In diesem Zusammenhang ist äußerst fraglich, ob der gesamte Datensatz der betroffenen Person für jede Behörde pauschal zur Erfüllung ihrer jeweiligen Aufgaben relevant ist.

4. Bedenken begegnet auch die in Art. 2 Nr. 13 Buchstabe a Doppelbuchstabe dd vorgesehene Änderung des **§ 22 Abs. 1 Satz 1 Nr. 9 AZRG**. Dadurch sollen die Befugnisse der Nachrichtendienste zum Abruf von Daten aus dem AZR im automatisierten Verfahren erheblich erweitert werden. Nach geltendem Recht ist den Verfassungsschutzbehörden und dem Militärischen Abschirmdienst der automatisierte Abruf nur für bestimmte Aufgaben erlaubt. Diese Beschränkungen sollen wegfallen, so dass der Abruf von Daten im automatisierten Verfahren für jede Aufgabe zugelassen wäre. Bei dem Abruf im automatisierten Verfahren handelt es sich im Vergleich zu einem an die registerführende Behörde gerichteten Ersuchen um einen schwerwiegenderen Grundrechtseingriff. Es bedarf hierfür daher einer besonderen Rechtfertigung, die vor allem in der Eilbedürftigkeit des Zugangs zu personenbezogenen Daten und der Häufigkeit der Abrufe liegen kann. Darlegungen hierzu enthält die Begründung des Regierungsentwurfs nur zu der Aufgabe, neben den bislang von der Norm erfassten terroristischen Bestrebungen auch islamistisch-legalistische Bestrebungen zu beobachten. Für alle weiteren Aufgaben der Verfassungsschutzbehörden und des Militärischen Abschirmdienstes enthält die Begründung keine Ausführungen. Die Erforderlichkeit für den erweiterten Zugang zum AZR ist somit für zahlreiche Aufgaben nicht dargelegt. Die verfassungsrechtliche Rechtfertigung kann insoweit nicht festgestellt werden.

Hinzu kommt, dass flankierende Maßnahmen, die den Grundrechtseingriff abmildern, ebenfalls eingeschränkt werden sollen. Besondere Bedeutung, gerade bei Datenverarbeitungen, die für die betroffenen Personen nicht transparent sind, kommt der Überprüfbarkeit der Datenverarbeitung zu (dazu BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07, Rn. 214 ff., zitiert nach [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2013/04/rs20130424\\_1bvr121507.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2013/04/rs20130424_1bvr121507.html)). Diese Kontrolle, unter anderem durch unabhängige Datenschutzaufsichtsbehörden, soll die fehlende Transparenz und Nachvollziehbarkeit für die betroffenen Personen kompensieren. Die Grundlage für eine effektive Kontrolle bilden Informationen über die tatsächliche Nutzung der personenbezogenen Daten. Diesem Zweck dient die nach § 13 AZRG vorgeschriebene Protokollierung von Abrufen aus dem AZR. Vor dem Hintergrund der Bedeutung der Protokolldaten ist es nicht nachvollziehbar, dass durch den vorliegenden Entwurf die Protokollierung der Abrufe durch Nachrichtendienste erheblich eingeschränkt werden soll. Nach **§ 13 Abs. 3 AZRG-E** ist vorgesehen, dass die Protokollierung nicht mehr

bei der Registerbehörde, sondern bei der abrufenden Stelle geführt wird. Dadurch wird der Bestand der Protokolldaten insoweit dezentralisiert. Eine zentrale Kontrolle, zum Beispiel der Häufigkeit von Abrufen, oder ein vom Bundesverfassungsgericht für zentrale Datenbestände gefordertes Zusammenwirken der Datenschutzaufsichtsbehörden (BVerfG, a.a.O. Rn. 216) wird dadurch unmöglich. Eingeschränkt wird zudem der Umfang der Protokolldaten. Nach dem geltenden § 13 Abs. 1 AZRG muss der Zweck des Abrufs protokolliert werden. Aus der Angabe des Zwecks muss nach § 13 Abs. 1 Satz 2 AZRG die Erforderlichkeit der Datenübermittlung erkennbar sein. Die Protokollierung der Abrufe durch Nachrichtendienste soll sich nach dem Entwurf nicht mehr nach § 13 AZRG, sondern nach § 6 Abs. 3 Satz 2 bis 5 BVerfSchG richten. Darin sind Angaben zum Zweck der Datenverarbeitung nicht vorgesehen. Die im Entwurf vorgesehene Protokollierung für die Nachrichtendienste bleibt damit insgesamt weit hinter der Protokollierung der Abrufe anderer Stellen aus dem AZR zurück. Gerade angesichts des mit einem Abruf durch Nachrichtendienste verbundenen Grundrechtseingriffs ist diese Einschränkung von Nachvollziehbarkeit und Kontrolle der Datenverarbeitung nicht akzeptabel.

5. Gleichzeitig bestimmt Art. 1 Nr. 13 Buchstabe b des 2. DAVG-E, dass die Anforderungen des **§ 22 Abs. 2 AZRG** für einen solchen Abruf abgesenkt werden. Bisher durfte gemäß § 22 Abs. 2 AZRG ein automatisiertes Abrufverfahren nur eingerichtet werden, soweit es wegen der Vielzahl der Übermittlungsersuchen oder der besonderen Eilbedürftigkeit unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen angemessen ist und die beteiligten Stellen die zur Datensicherung nach § 9 des alten Bundesdatenschutzgesetzes erforderlichen technischen und organisatorischen Maßnahmen getroffen haben. Zukünftig soll das Wort „Vielzahl“ durch das Wort „Häufigkeit“ ersetzt werden und es muss keine „besondere“ Eilbedürftigkeit mehr bestehen. Ausweislich der Gesetzesbegründung (BT-Drs. 19/8752, S. 58) wird mit der Absenkung bezweckt, dass die Zulassung der in Absatz 1 aufgeführten Behörden zum automatisierten Abruf erleichtert werden soll. Der automatisierte Abruf stellt nach Ansicht des Bundesverfassungsgerichts jedoch einen Eingriff von nicht unerheblichem Gewicht dar. Diesem Eingriff fehlt eine Hemm- und Kontrollwirkung, da der Abruf durch Dritte nicht wahrgenommen wird (vgl. BVerfG, Beschluss vom 24. Januar 2012 – 1 BvR 1299/05 –, zitiert nach: [http://www.bverfg.de/e/rs20120124\\_1bvr129905.html](http://www.bverfg.de/e/rs20120124_1bvr129905.html), Rn. 156). Insofern muss der Eingriff verhältnismäßig sein, um gerechtfertigt werden zu können. Da sich die Gesetzesbegründung mit der Erforderlichkeit der Absenkung der

Zulassungsvoraussetzungen aber nicht auseinandergesetzt hat, ist es nicht nachvollziehbar, weshalb es notwendig war, die Anforderungen abzusenken.

6. Zusätzlich zu der Absicht, die Zulassungsvoraussetzungen abzusenken und einer Vielzahl an Behörden den Abruf mittels automatisierten Verfahrens zu ermöglichen, sieht der 2. DAVG-E vor, dass **§ 22 Abs. 3 Satz 3 AZRG** gestrichen wird. Bisher dürfen Abrufe von Daten aus dem Register im automatisierten Verfahren nur von Bediensteten vorgenommen werden, die vom Leiter der abrufenden Stelle hierzu besonders ermächtigt worden sind. Ausweislich der Gesetzesbegründung soll es zukünftig ganzen Organisationseinheiten ermöglicht werden, sich für einen Abruf zu authentisieren, damit flexibel auf die organisatorischen Erfordernisse vor Ort reagiert werden kann (vgl. BT-Drs. 19/8752, S. 58). Wie die Ausschüsse dem Bundesrat in ihren Empfehlungen (BR-Drs. 54/1/19, Empfehlungen, S. 14f.) richtigerweise nahelegen, bedeutet dies eine erhebliche Missbrauchsgefahr, da es nicht mehr länger nur extra hierfür autorisierten Personen, sondern jedem Mitarbeiter der Organisationseinheit möglich ist, den automatisierten Abruf zu tätigen. Insofern sei die beabsichtigte Streichung nicht unterstützenswert. Diese Empfehlung wurde vom Bundesrat leider nicht in seine Stellungnahme übernommen. Da es sich bei den Daten im AZR um teilweise hochsensible Daten handelt, ist eine Abschwächung des Schutzes dieser Daten nicht hinnehmbar. Zwar sieht § 22 Abs. 3 Satz 2 AZRG vor, dass die Registerbehörde die Zulässigkeit der Abrufe durch geeignete Stichprobenverfahren (Protokollierung) oder anlassbezogen überprüft. Jedoch ist es angesichts der Vielzahl der zum automatisierten Abrufverfahren zugelassenen Behörden, die jeweils als Organisationseinheiten zum Abruf berechtigt sind, schwierig, durch Stichproben Missbrauchsfälle zu erkennen. Insofern ist der tatsächliche Wirkungsgehalt dieser Regelung stark anzuzweifeln. Zusätzlich zu der Überprüfung durch die Registerbehörde soll zwar ausweislich der Gesetzesbegründung nicht auf eine personenscharfe Zugriffskontrolle verzichtet werden (BT-Drs. 19/8752, S. 58). Diese muss innerhalb der jeweils abrufenden Behörde organisiert werden. Jedoch dient eine Protokollierung insgesamt nur dazu, im Nachhinein repressiv gegen diejenigen Personen vorzugehen, die missbräuchlich abgerufen haben; sie ist nicht dazu geeignet, einen solchen Missbrauch im Vorfeld präventiv zu verhindern (vgl. auch die Empfehlungen der Ausschüsse, BR-Drs. 54/1/19, S. 14f.). Dies kann nur dadurch geschehen, dass die Authentisierung einzelner, zuverlässiger Personen für einen Abruf des AZR erfolgt.



7. Durch Art. 3 Nr. 2 Buchstabe b und Buchstabe c des 2. DAVG–E soll **§ 49 Abs. 6 Satz 2, Abs. 8 Satz 3 und Abs. 9 Satz 3 AufenthG** dahingehend geändert werden, dass die Altersgrenze, ab der erkennungsdienstliche Maßnahmen zur Überprüfung, Feststellung und Sicherung der Identität des betroffenen Ausländers durchgeführt werden können, von der Vollendung des 14. Lebensjahres auf die Vollendung des sechsten Lebensjahres abgesenkt wird. Ausweislich der Gesetzesbegründung (BT–Drs. 19/8752, S. 3 und 65f.) soll diese Vorschrift das Kindeswohl schützen, indem die Kinder beispielsweise in einem Vermisstenfall aufgrund der Fingerabdrücke eindeutig zugeordnet werden können. In der Gesetzesbegründung wird die Absenkung des Mindestalters mit dem Vorschlag der Kommission gerechtfertigt, bei der Neufassung der EUODAC–Verordnung (COM [2016] 272 final) und der Neufassung der Verordnung über das EU–Visa–Informationssystem (COM [2018] 302 final) die Abnahme von Fingerabdrücken ab der Vollendung des sechsten Lebensjahres zu ermöglichen, da Untersuchungen zufolge ab diesem Alter die Fingerabdruckerkennung mit zufriedenstellender Genauigkeit funktioniert (BT–Drs. 19/8752, S. 65). Im Gegensatz dazu haben die Ausschüsse in ihren Empfehlungen (BR–Drs. 54/1/19, S. 17) aber dargelegt, dass sich die biometrischen Merkmale von Kindern wachstumsbedingt noch ändern und dass regelmäßig Qualitätseinbußen bei der erkennungsdienstlichen Behandlung zu erwarten sind. Bei der Erhebung biometrischer Daten handelt es sich um einen massiven Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Minderjährigen. Allein aufgrund des sehr jugendlichen Alters der betroffenen Kinder sind an eine Rechtfertigung dieses Eingriffes umso höhere Maßstäbe anzulegen. Da bislang die oben genannten Verordnungen mit der abgesenkten Altersgrenze auf EU–Ebene noch nicht beschlossen wurden und es sich lediglich um einen Vorschlag der Kommission handelt, besteht keine Notwendigkeit, mit einer nationalen deutschen Regelung einer eventuellen EU–weiten Normierung vorzugreifen. In Anbetracht der Möglichkeit, dass die erhobenen biometrischen Daten eventuell später unbrauchbar sind, ist ein solcher tiefgreifender Eingriff nicht gerechtfertigt.
  
8. Der Bundesrat hat in seiner Stellungnahme (BR–Drs. 54/19, S. 10f.) angeregt, dass in **§ 56a Abs. 1 AufenthG** ein neuer Satz eingefügt werden soll, der den betroffenen Ausländer dazu verpflichtet, ein zur Verfügung gestelltes Mobiltelefon ständig in betriebsbereitem Zustand bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen. In der Begründung führte er aus, dass das Mobiltelefon zwar für die elektronische Aufenthaltsüberwachung selbst technisch nicht erforderlich sei; die

Möglichkeit einer Sprachverbindung zwischen dem Ausländer und den Mitarbeitern der Überwachungsstelle aber sinnvoll sei, um den Ausländer erreichen und eventuelle Problemlagen lösen zu können. Durch die o. g. Verpflichtung wird ohne Not extrem in die Rechte des betroffenen Ausländers eingegriffen, da sie auf eine ständige Erreichbarkeit des betroffenen Ausländers, zu jeder Tag- und Nachtzeit, abzielt, obwohl er ohnehin schon elektronisch aufenthaltsüberwacht wird. Da der Bundesrat selbst zugegeben hat, dass diese Vorgehensweise nicht erforderlich, sondern nur sinnvoll sei, ist dieses Interesse in der Abwägung mit den betroffenen Interessen des Ausländers als äußerst gering zu bewerten. Ein derart weitgehender Eingriff in dessen Rechte ist mit einer bloß als „sinnvoll“ eingeschätzten Maßnahme nicht zu rechtfertigen. Die Bundesregierung hat in ihrer Gegenäußerung (BT-Drs. 19/8752, Anlage 5, S. 105) den Vorschlag des Bundesrates zwar nicht aufgegriffen und in den Gesetzentwurf einfließen lassen. Dennoch ist aus diesem Ansinnen die bedenkliche Tendenz zu erkennen, den betroffenen Ausländer immer gläserner werden zu lassen.

9. Der Regierungsentwurf sieht in Art. 3 Nr. 5 eine Ausweitung der Zuverlässigkeits- und Sicherheitsüberprüfungen nach **§ 73 AufenthG** vor. Bislang ist die Überprüfung nach § 73 AufenthG zur Feststellung von gesetzlich definierten Versagungsgründen und zur Prüfung von sonstigen Sicherheitsbedenken in bestimmten Verfahren vorgesehen. Der bereits nach geltendem Recht unbestimmte Begriff der sonstigen Sicherheitsbedenken wird durch den Gesetzentwurf weiter aufgeweitet, da die Prüfung von Sicherheitsbedenken auf eine Reihe weiterer ausländer- bzw. asylrechtlicher Verfahren erstreckt werden soll. Ein Maßstab für die Sicherheitsbedenken fehlt im geltenden Recht ebenso wie im vorliegenden Entwurf. Bei dem Verfahren der Zuverlässigkeits- bzw. Sicherheitsüberprüfung handelt es sich um einen erheblichen Grundrechtseingriff. Es werden zahlreiche Behörden eingebunden, neu hinzukommend auch die Bundespolizei, die auf der Grundlage ihrer Datenbestände eine Prüfung und Bewertung vornehmen, ob Sicherheitsbedenken und Versagungsgründe bestehen. Dieses Verfahren ist nicht nur anfällig für Fehler, die zum Beispiel in der Verwechslung von Namen und anderen Identitätsmerkmalen von Personen begründet sein können. Es besteht zudem das Risiko, dass gespeicherte personenbezogene Daten in unverhältnismäßiger Weise verwendet werden. Die Datenbestände der zu konsultierenden Behörden sind vielfältig. Die vorhandenen Daten unterscheiden sich nach der Art und Rolle der betroffenen gespeicherten Person (es sind z.B. Beschuldigte ebenso gespeichert wie Geschädigte, Zeugen oder Kontakt- und Begleitpersonen), nach dem Gewicht des

Anlasses für die Speicherung und nach dem Grad ihrer Verlässlichkeit. Ohne klare gesetzliche Vorgaben für die - zweckändernde - Verwendung dieser Daten für Zwecke der Sicherheits- und Zuverlässigkeitsbewertung ist nicht gewährleistet, dass personenbezogene Daten für eine solche Prüfung verwendet werden, die auf ausreichend gesicherten Erkenntnissen beruhen, für deren Speicherung die betroffene Person einen hinreichenden Anlass gegeben hat und die in einem angemessenen Verhältnis zu dem neuen Zweck der Sicherheits- bzw. Zuverlässigkeitsüberprüfung stehen. Diesen Anforderungen wird § 73 AufenthG in seiner gegenwärtigen und auch in der Fassung des Regierungsentwurfs nicht gerecht.