Das Ausländerzentralregistergesetz – was Recht ist

Europarechtlicher und verfassungsrechtlicher Korrekturbedarf beim AZRG

Stand: 14.02.2022

Thilo Weichert
weichert@netzwerk-datenschutz-expertise.de
Waisenhofstraße 41, 24103 Kiel
Karin Schuler
schuler@netzwerk-datenschutz-expertise.de
Kronprinzenstraße 76, 53173 Bonn

www.netzwerk-datenschutzexpertise.de

Inhalt

Das Ausländerzentralregister (AZR) ist die am umfassendsten vernetzte Datenbank der deutschen Verwaltung über in Deutschland lebende Ausländerinnen und Ausländer. Es verbindet die Ausländerbehörden untereinander, aber auch sämtliche Sicherheitsbehörden – Polizeien und Nachrichtendienste – sowie in den jüngsten Jahren zunehmend Behörden aus dem allgemeinen und dem sozialen Bereich. Dieses schon seit Jahrzehnten bestehende Register wurde – ohne dass dies bisher größere öffentliche Aufmerksamkeit gefunden hätte – immer weiter ausgebaut.

Von Anfang an stand das AZR in der Kritik, die Grundrechte der in ihm erfassten Menschen nicht hinreichend zu beachten. Dessen ungeachtet wurden die administrativen Befugnisse zum Datenaustausch über das Register – ohne Rücksicht auf die Betroffenenrechte und zuletzt 2021 – immer wieder erweitert. Dies führte dazu, dass die im Register angelegten Verstöße gegen das Grundrecht auf Datenschutz, aber auch gegen weitere Grundrechte und gegen das Gleichbehandlungsgebot verschlimmert wurden. Durch die Europäisierung des Grundrechtsschutzes und die europäische Datenschutz-Grundverordnung kommt zu den Verstößen gegen das deutsche Grundgesetz die Verletzung von Europarecht hinzu.

Das vorliegende Gutachten stellt die im AZR-Gesetz (AZRG) angelegten Verstöße dar. Angesichts der hohen Komplexität des AZRGs mit seinen vielen Verweisungen ist es eine besondere Herausforderung, die Wirkweise der AZR-Datenverarbeitung verständlich darzustellen und kritisch zu hinterfragen. Mit dem vorliegenden Gutachten sollen zudem Antworten auf die Frage gegeben werden, wie der Kommunikationsbedarf innerhalb der Verwaltung zu Ausländerinnen und Ausländern verfassungs- und europarechtskonform ausgestaltet werden kann. Im Jahr 2021 wurde eine weitere Zentralisierungsrunde der AZR-Datenverarbeitung gestartet. Damit droht eine erneute Vertiefung der informationellen Entrechtung von Ausländerinnen und Ausländern. Zugleich eröffnen sich dabei die Notwendigkeit und die Chance, das AZR auf ein angemessenes, rechtsstaatliches Niveau zu heben.

1 Kleine Geschichte des AZRG

Das Ausländerzentralregister (AZR), in dem alle in Deutschland nicht nur vorübergehend aufhältigen Nichtdeutschen erfasst werden, besteht seit 1953. Nachdem im **Volkszählungsurteil** des Bundesverfassungsgerichts (BVerfG)[1] 1983 festgestellt worden war, dass informationelle Eingriffe, wie sie im AZR erfolgen, einer gesetzlichen Grundlage bedürfen, wurde 1994 das Ausländerzentralregistergesetz (AZRG) verabschiedet und in Kraft gesetzt.[2] Das neue Gesetz wurde damals dahingehend kritisiert, dass es den verfassungsrechtlichen Anforderungen, insbesondere zum Datenschutz, nicht genüge. 1995 wurde gegen das Gesetz eine Verfassungsbeschwerde erhoben. Diese Beschwerde wurde vom BVerfG mit Beschluss vom 10.10.2001 zurückgewiesen, da sie sich direkt gegen das Gesetz

[1] BVerfG 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 419.
[2] BGBl. 1994 I S. 2265.

richtete. Das BVerfG begründete dies damals, das Gesetz könne so nicht angegriffen werden und verwies auf die Ausschöpfung des Verwaltungsrechtswegs, über den konkrete informationelle Eingriffe beanstandet werden müssten. Es gestand aber zu, dass die Beschwerde „durchaus gewichtige verfassungsrechtliche Fragen“ aufwerfe.[3]

Das AZRG wurde bis heute 43mal, teilweise sehr grundsätzlich geändert. Diese **Änderungen** zielten vorwiegend darauf ab, den Umfang der Datenverarbeitung auszuweiten und weiteren Stellen die Speicherung von Daten im AZR und den Abruf daraus zu ermöglichen und zu erweitern. Eine Ausnahme hiervon war ein Gesetz von 2012.[4] Damit wurde ein Urteil des Europäischen Gerichtshofs (EuGH) aus dem Jahr 2008[5] umgesetzt, in dem dieser festgestellt hatte, dass die Datenspeicherung von EU-Staatsangehörigen im AZR diskriminierend sei, weil dadurch Deutsche und sonstige EU-Angehörige ungerechtfertigt unterschiedlich behandelt würden.

Die jüngste Novellierung des AZRG erfolgte mit dem Gesetz zur Weiterentwicklung des Ausländerzentralregisters (AZRWeiterentwG) vom 09.07.2021, durch das die **Zentralisierung** der bisher dezentral bei den Ausländerbehörden geführten Ausländerdateien A im AZR eingeleitet werden soll. Hierfür bedarf es künftig weiterer Gesetzesregelungen. Auch dieses Gesetz war im Rahmen des Gesetzgebungsverfahrens massiv aus europa- und verfassungsrechtlicher Sicht kritisiert und daraufhin – ein wenig – verbessert worden.[6]

Der Regelungsrahmen für das AZRG wird inzwischen nicht nur durch das Grundgesetz (GG) vorgegeben, sondern auch durch die Europäische Grundrechte-Charta (GRCh). Art. 8 GRCh sieht ein Grundrecht auf Datenschutz vor. In Umsetzung dieser Vorgabe wurde 2018 die europäische **Datenschutz-Grundverordnung** (DSGVO)[7] wirksam, die konkretere, zwingende Vorgaben für den informationellen Grundrechtsschutz – auch im AZRG – macht.

Inzwischen haben mehr als **16.000 öffentliche Stellen**, davon ca. 4.000 online, mit mehr als 150.000 Einzelnutzenden Zugriff auf rund 16 Millionen Personendatensätze. Allein im Jahr 2020 führten Behörden im Schnitt etwa 260.000 Datenabfragen pro Arbeitstag im AZR durch.[8] Zum Stichtag 31.07.2021 waren knapp 19 Mio. Personen im allgemeinen Datenbestand des AZR erfasst, von denen gut 11.6 Mio. in Deutschland lebten.[9] Das AZR teilt sich in einen allgemeinen Datenbestand, der in den §§ 2-27 AZRG geregelt ist, und eine Visa-Datei, spezifisch normiert in den §§ 28-33 AZRG.

[3] BVerfG 10.10.2001 – 1 BvR 1970/95, NVwZ 2002, 464; dazu *Weichert* in GK-AufenthG, Vorb AZRG Rn. 34 f. m.w.N.
[4] BGBl. 2012 I S. 2745.
[5] EuGH 16.12.2008 – C-524/06, DVBl. 2009, 171 = MMR 2009, 171 = DÖV 2009, 168.
[6] Deutscher Bundestag, Ausschuss für Inneres und Heimat, 19. Wahlperiode, Wortprotokoll der 137 Sitzung v. 03.05.2021.
[7] Verordnung (EU) 2016/679 v. 27.04.2016, ABl. v. 04.05.2016, L 119/1.
[8] GFF, Das Ausländerzentralregister, 2022, S. 4; BT-Drs. 19/32508, 2 ff., 8; vgl. BT-Drs. 19/17380, S. 4, 36; *Weichert* in GK-AufenthG, Vorb AZRG, Rn. 51.
[9] GFF, Das Ausländerzentralregister, 2022, S. 5, BT-Drs. 19/32508, 2.

Der Ausbau des AZR war geprägt durch immigrationspolitische Entwicklungen, zuletzt durch die verstärkte Einwanderung nach Deutschland im Jahr 2015, und die deshalb für notwendig angesehene Digitalisierung der Ausländerverwaltung. Diese Digitalisierung steht im größeren Kontext normativer Bemühungen zur **Verwaltungsmodernisierung** in Deutschland. Diese Bemühungen wurden im 2021 beschlossenen Registermodernisierungsgesetz (RegMoG)[10] konkretisiert, das auch das AZR einbezieht. Darin ist vorgesehen, zum sichereren Online-Austausch eine Identifizierungsnummer für alle in Deutschland wohnenden Menschen, also auch für alle Ausländerinnen und Ausländer, einzuführen.[11] Die Digitalisierung steht auf der Tagesordnung der 20. Legislaturperiode des Deutschen Bundestags und der Bundesregierung. Der damit versprochene Aufbruch im sog. eGovernment muss sich natürlich am normativen Rahmen des Grundgesetzes und des Europarechts orientieren.

Der **Reformbedarf beim AZR** wird zunehmend erkannt. Die Gesellschaft für Freiheitsrechte (GFF) hat Januar 2022 in einer Studie und einem Rechtsgutachten strukturelle Änderungen beim AZR und eine rechtliche Entschlackung des AZRG eingefordert.[12] Initiativen im Bundestag zeigen, dass dort rechtliche Grundlagen und Praxis des AZR kritisch bewertet werden.[13] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) signalisierte, dass das AZRG überarbeitet werden muss und dabei die Speicherfristen, die Zugriffsregelungen und den Kreis der Zugriffsberechtigten kritisch hinterfragt werden müssen.[14]

*Im Folgenden werden die Regelungen des AZRG **an höherrangigem Recht gemessen**, also am deutschen Grundgesetz (GG), an der europäischen Grundrechte-Charta (GRCh) sowie an der diese Vorgaben konkretisierenden europäischen Datenschutz-Grundverordnung (DSGVO).[15] Bzgl. der ebenso anwendbaren Europäischen Menschenrechts-Konvention (Art. 52 Abs. 3 GRCh) ergeben sich keine Abweichungen zum GG und zur GRCh. Bei der rechtlichen Bewertung sind drei Verarbeitungsphasen zu unterscheiden: 1. die Übermittlung an Daten anliefernden Stellen und deren Speicherung im AZR, 2. Die Übermittlung der gespeicherten Daten an Empfänger, 3. eine Weiterverwendung dieser Daten durch die Übermittlungsempfänger.[16] Die ursprüngliche Datenerhebung und -speicherung der Daten durch die anliefernden Stellen wird nicht näher beleuchtet.*

[10] G. v. 28.03.2021, BGBl. I S. 591.
[11] Identifikationsnummerngesetz (IDNrG) als Teil des RegMoG.
[12] GFF, Das Ausländerzentralregister; *Bäcker*, Bewertung des AZR (GFF-Gutachten), 13.01.2022.
[13] Anfrage der MdB *Jelpke* u.a. und der Fraktion Die Linke v. 20.09.2021, BT-Drs. 32112; Ausschuss für Inneres und Heimat, Wortprotokoll der 137. Sitzung (Protokoll-Nr. 19/137) v. 03.05.2021 mit Beiträgen u.a. von *Lehmann*, *Jelpke* und *Amtsberg*.
[14] Interview mit *Kelber*, www.migazin.de 26.01.2022.
[15] Zu deren Anwendbarkeit auf die aZR-Datenverarbeitung *Weichert* in GK-AufenthaltG, Vorbem. Rn. 40; *Bäcker*, GFF-Gutachten, S. 19 f.
[16] Zur Wechselbezüglichkeit der Verarbeitungsphasen *Bäcker*, GFF-Gutachten, S. 21 f.

*Die folgenden Ausführungen beziehen sich vorrangig auf die Regelungen zum **allgemeinen Datenbestand** des AZR, nicht zu dem Bestand der Visadatei, der in den §§ 28-33 AZRG geregelt ist.*

2 Die Grundrechte

Angesichts der bisherigen qualifizierten Kritik am AZRG und den eingeleiteten weiteren Änderungen im Bereich der Digitalisierung in der Ausländerrechtsverwaltung ist es nötig, eine rechtliche Bestandaufnahme vorzunehmen, um zu vermeiden, dass beim weiteren Vorgehen Fakten geschaffen werden, die mit übergeordnetem Recht nicht vereinbar oder schwer rückgängig zu machen sind.

2.1 Datenschutz – Recht auf informationelle Selbstbestimmung

Mit der Verarbeitung personenbezogener Daten von Nichtdeutschen im AZR erfolgen Eingriffe in das Recht auf informationelle Selbstbestimmung[17], also in das in Art. 8 GRCh garantierte **Grundrecht auf Datenschutz**. Der materielle Gehalt der verfassungsrechtlichen und europarechtlichen Garantie des Grundrechts unterscheiden sich nicht.[18] Das Grundrecht auf informationelle Selbstbestimmung gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Gemäß Art. 8 Abs. 2 GRCh dürfen Daten nur „nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen, gesetzlich geregelten, legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken."

„**Einschränkungen** dieses Rechts auf ‚informationelle Selbstbestimmung' sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken."[19]

Ausländerinnen und Ausländern, also Menschen, die keine deutsche Staatsangehörigkeit haben, steht wie Deutschen das Recht auf informationelle Selbstbestimmung bzw. das Grundrecht auf Datenschutz zu.[20]

[17] BVerfG 15.12.1983 – 1 BvR 209/83 u.a., Volkszählung, NJW 1984, 419.
[18] *Kühling/Raab* in *Kühling/Buchner*, Einführung Rn. 31-41.
[19] BVerfG 15.12.1983 – 1 BvR 209/83 u.a., Volkszählung, NJW 1984, 419.
[20] BVerfG 10.5.1988 – 1 BvR 482/84, 1 BvR 1166/85, Rn. 50, BVerfGE 78, 196 f.; *Huber*, NJW 2013, 2573 f.; *Bäumler*, NVwZ 1995, 239; *Rittstieg*, InfAuslR 1984, 123; *Frankenberg*, FS Simitis, S. 100; *Weichert*, InfAuslR 1989, 1; *ders.*, AZRG, Einführung Rn. 13; *ders.* in *Roßnagel*, Handbuch Datenschutzrecht, 2003, S. 1573.

Viele weitere Grundrechte haben eine informationelle bzw. **digitale Dimension**[21] und damit eine Wechselbeziehung zum Grundrecht auf Datenschutz: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“[22]

Bei der Datenverarbeitung im oder über das AZR ist diese grundrechtliche Dimension immer zu berücksichtigen. Dies gilt wegen ihres informationellen Gehalts für alle **bürgerlichen, politischen und sozialen Grundrechte**. Dies gilt insbesondere auch für die speziellen Rechte, die für Nichtdeutsche bzw. aus europarechtlicher Sicht für Drittstaatsangehörige zur Anwendung kommen, also das Recht auf Asyl (Art. 16a GG, Art. 18 GRCh) sowie der Schutz bei Abschiebung, Ausweisung und Auslieferung (Art. 19 GRCh).

2.2 Insbesondere Grundrecht auf Asyl

Gemäß Art. 16a Abs. 1 GG und Art. 18 GRCh genießen **politisch Verfolgte** Asylrecht. Der Schutz vor politischer Verfolgung ist in internationalen Abkommen konkretisiert, insbesondere im Genfer Abkommen vom 28.07.1951 und dem Protokoll vom 31.01.1967 über die Rechtsstellung der Flüchtlinge. Im Rahmen von Asylverfahren müssen Verfolgte, um ihren Status anerkennen zu lassen, oft detaillierte Informationen über ihre politischen Überzeugungen und Aktivitäten offenbaren, die zugleich von Behörden, Einrichtungen und Einzelpersonen, insbesondere in den Heimatstaaten, als Grundlage für Verfolgungsmaßnahmen verwendet werden können. Geheimdienste der Heimatstaaten sind in Europa und in Deutschland aktiv, um an entsprechende Informationen zu gelangen. Diese besorgen sie sich von anderen Geheimdiensten, verdeckt oder offen, aber auch von sonstigen staatlichen Stellen, etwa indem sie Dolmetscher oder Mitarbeiter bei diesen Stellen einschleusen. Soweit vom AZR Informationen verarbeitet werden, die sich als Grundlage für politische Verfolgung eignen, sind diese besonders schützenswert.[23]

Man kann insofern von der Notwendigkeit eines **Asylgeheimnisses** sprechen, das aus dem grundrechtlich zugesicherten Schutz vor Verfolgung abzuleiten ist. Bei den Angaben eines Flüchtlings zur Begründung seines Asylantrags sowie in Entscheidungen hierzu handelt es sich

[21] *Weichert*, KJ 2014, 25 ff.; *Hoffmann/Luch/Schulz/Borchers*, Die Digitale Dimension der Grundrechte, 2015.
[22] BVerfG 15.12.1983 – 1 BvR 209/83 u.a., Rn. 146, NJW 1984, 422.
[23] *Müller* ZAR 2019, 185; *Frankenberg*, FS Simitis, S.114.

um Informationen über die politische Meinung des Betroffenen, die auch gemäß Art. 9 Abs. 1 DSGVO unter besonderem Schutz stehen.[24]

2.3 Weitere verfassungsrechtliche Aspekte

Besondere Kategorien personenbezogener Daten genießen nach Art. 9 Abs. 1 DSGVO einen erhöhten Schutz. Zu diesen sensitiven Daten zählen u.a. Angaben über politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zur sexuellen Orientierung. Teilweise wird die Ansicht vertreten, dass eine Rechtspflicht zur Angabe eines religiösen Bekenntnisses wegen Art. 140 GG i.V.m. Art. 136 Abs. 3 WRV verfassungsrechtlich verboten ist.[25]

In Art. 9 Abs. 1 DSGVO geschützte Angaben können im AZR enthalten sein, insbesondere in Dokumenten nach § 6 Abs. 5 AZRG, etwa zur Ausweisung oder Untersagung der politischen Betätigung. Angaben zur Religionszugehörigkeit können nach § 3 Abs. 1 Nr. 5 AZRG gespeichert sein. Biometrische Daten sind z.B. die Fingerabdrücke oder ein biometrisch auslesbares Foto (§ 3 Abs. 1 Nr. 5a, Abs. 2 Nr. 1, Abs. 3a Nr. 1 AZRG). Gesundheitsangaben werden nach § 3 Abs. 2 Nr. 10-11 AZRG gespeichert. Die Verarbeitung dieser Daten muss durch ein **erhebliches öffentliches Interesse** gerechtfertigt sein (Art. 9 Abs. 2 lit. g DSGVO).[26] Diese Daten bergen eine besonders hohe Gefahr der Stigmatisierung und der Einschüchterung.[27] Die Bevorratung sensitiver Daten muss an klar konturierte Anlässe und auf hinreichend gewichtige Fälle begrenzt bleiben.[28]

Eine weitere, besonders geschützte Datenart stellen Daten über **strafrechtliche Verurteilungen und Straftaten** (Art. 10 DSGVO) dar. Solche Daten werden systematisch im AZR gemäß § 2 Abs. 2 Nr. 7, 7a, 11 AZRG erfasst.[29] Das AZR wird, wie von Art. 10 DSGVO gefordert, unter behördlicher Aufsicht geführt. Zulässig ist die Verarbeitung zudem nur, wenn geeignete Garantien für die Rechte und Freiheiten der Betroffenen vorgesehen sind.

Berufsgeheimnisse und das Sozialgeheimnis (vgl. § 203 StGB, § 35 SGB I) sind nicht ausdrücklich im Grundgesetz (GG) oder in der GRCh garantiert. Das BVerfG wie auch der EuGH[30] haben aber einen verfassungsrechtlichen Schutz solcher Geheimnisse aus den Grundrechten abgeleitet. Für bestimmte Berufs- und Personengruppen sowie für bestimmte Stellen ist eine besondere Vertraulichkeit Voraussetzung für deren wirksame Tätigkeit. Dem

[24] Netzwerk Datenschutzexpertise, Stellungnahme zum 2. DSVAG, 2 f.; *Weichert* in *Huber*, § 86 Rn. 40, 45; *ders.*, DuD 2002, 424; ausführlich *Wittmann*, Stellungnahme v. 30.04.2021, BT-Innenausschuss, A-Drs. 19(4)820 D, 23 ff.; vgl. BVerwG 30.03.2021 – 1 C 41.20. Rn. 27.
[25] *Hilbrans* in *Hofmann*, § 86 AufenthG, Rn. 17 m.w.N.
[26] EuGH 03.10.2019 – C-70/18, NVwZ-RR 2019, 1066 = ZAR 2020, 111.
[27] *Bäcker*, GFF-Gutachten, S. 22 mit Verweis auf EGMR 04.12.2008 No. 30562/04 u. 30566/04.
[28] *Bäcker*, GFF-Gutachten, S. 22 f. mit vielen Verweisen auf den EuGH und den EGMR.
[29] *Weichert* in *Kühling/Buchner*, Art. 10 Rn. 8a.
[30] EuGH 08.04.2014 – C-293/12 u. C-594/12, Vorratsdatenspeicherung, Rn. 58, NJW 2014, 712.

liegt die Erwägung zugrunde, dass eine Hilfe suchende Person sich einem potenziellen Helfenden nur umfassend anvertrauen wird, wenn sich für sie hieraus keine nachteiligen Folgen ergeben. Dieses Anvertrauen ist für den Helfenden nötig, um adäquat – individuell, kompetent, situationsbezogen und ausreichend – Hilfe leisten zu können. Dies gilt insbesondere, wenn die Hilfe dem Schutz der Unversehrtheit dient und eine staatliche Schutzpflicht besteht, wie dies z.B. im Hinblick auf die Gesundheit gegenüber der Allgemeinheit der Fall ist.[31] Gesteigert wird die Schutzpflicht gegenüber vulnerablen Gruppen und Personen, also solchen, die sich nicht oder nur eingeschränkt selbst schützen können.

Zur Begründung derartiger Geheimnisse wird auf das Recht auf Datenschutz bzw. auf das allgemeine Persönlichkeitsrecht der Person, die Hilfe in Anspruch nimmt, und auf weitere Verfassungsprinzipien verwiesen. Der „Kernbereichs privater Lebensgestaltung“ kann dabei betroffen sein.[32] Die beruflich begründete Vertraulichkeit fällt zudem in den Schutzbereich der Berufsfreiheit des Art. 12 GG und des Art. 15 Abs. 1 GRCh.[33] Die Rechtsprechung gesteht **keine absolute Vertraulichkeit** bei der Hilfstätigkeit zu. Zur Rechtfertigung von informationellen Eingriffen wird aber der Schutz hochrangiger Güter verlangt.[34]

Im Gesundheitsbereich kommt oft das **Patientengeheimnis** (ärztliche Schweigepflicht) zur Anwendung, das auf den Eid des Hippokrates (von 460 bis 370 vor Christus) zurückgeht.[35] Das Patientengeheimnis hat neben dem Datenschutz seine Grundlage im Schutz der Unversehrtheit des Patienten (Art. 2 Abs. 2 S. 1 GG, Art. 3 GRCh), dem Schutz der Berufsausübung des medizinischen Helfers (Art. 12 GG, Art. 15 GRCh)[36] sowie im Sozialstaatsprinzip (Art. 20 GG bzw. Art. 34, 35 GRCh).[37] Die gesellschaftliche Funktion der Berufsgeheimnisse ändert nichts an dem Umstand, dass bei der Auslegung wie der konkreten Anwendung der Regelungen der Individualrechtsschutz bestimmend ist. Sozial- und Patientengeheimnisse können bei der Verarbeitung der in § 3 Abs. 1 Nr. 6, Abs. 2 Nr. 10, 10a, 11 AZRG genannten Daten betroffen sein.

Nichtdeutsche sind insbesondere als **Flüchtlinge** besonders schutzbedürftig. Dies gilt nicht nur im Fall politischer Verfolgung, sondern generell. Sie leben in Deutschland in einer für sie zunächst fremden Kultur, in einer Gesellschaft mit teilweise unbekannten Regeln und Werten, in der nicht ihre Muttersprache gesprochen wird. Die ökonomische, soziale, kulturelle wie auch die familiäre Situation von Flüchtlingen ist oft prekär.

[31] BVerfG 19.11.2021 – 1 BvR 781/21 u.a., Rn. 168 ff.
[32] BVerfG 25.01.2007 – 2 BvR 26/07, NJW 2007, 1865.
[33] BVerfG 12.04.2005 – 2 BvR 1027/02, NJW 2005, 1919.
[34] BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09 Rn. 131-133, NJW 2016, 1788; MVVerfG 18.5.2000 – LVerfG 5/98, NVwZ 2000, 1038; SächsVerfGH 14.5.1996 – Vf. 44-II/94, NJW 1996, 1954 = DuD 1996, 496 f.
[35] *Weichert* DuD 2014, 831.
[36] *Ruffert* in *Callies/Ruffert*, Art. 15 GRCh Rn. 24.
[37] BVerfG 19.7.1972 – 2 BvL 7/71, NJW 172, 2214, *Hatje* in *Schwarze* Art. 339 Rn. 6; *Wegener* in *Callies/Ruffert*, Art. 339 AEUV Rn. 2.

Art. 21 Abs. 1 GRCh verbietet die Diskriminierung „wegen des Geschlechts, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung“. Art. 21 Abs. 2 GRCh erstreckt das **Verbot von Diskriminierung** auf Gründe der Staatsangehörigkeit. Damit wird das Gleichheitsgebot des Art. 3 GG konkretisiert und teilweise ausgeweitet.

2.4 Grundrechtseinschränkungen

Gemäß Art. 52 Abs. 1 GRCh muss jede Einschränkung der Ausübung der in der Grundrechtecharta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheit achten. Einschränkungen dürfen nur unter Wahrung des Grundsatzes der **Verhältnismäßigkeit** vorgenommen werden. Sie müssen notwendig sein und den Gemeinwohlzielen oder den Erfordernissen des Schutzes anderer entsprechen. Bei der Prüfung der Verhältnismäßigkeit muss festgestellt werden, dass der Eingriff, also die informationelle Maßnahme, 1. die Erreichung eines legitimen Zwecks verfolgt, 2. hierzu geeignet und 3. erforderlich ist. Schließlich muss sie sich 4. im Rahmen einer Interessenabwägung im Hinblick auf die damit verbundenen Eingriffe als angemessen erweisen.

Gemäß Art. 52 Abs. 1 GRCh müssen die Grundrechte einschränkende gesetzliche Regelungen hinreichend bestimmt sein. Der **Bestimmtheitsgrundsatz** ist zugleich auch eine Ausprägung des Rechtsstaats- und Demokratieprinzips (Art. 20, 28 Abs. 1 GG), aus dem u.a. das Gebot der Normenklarheit hergeleitet wird: Inhalt, Zweck und Ausmaß der erteilten Eingriffsermächtigung müssen sich direkt aus der Rechtsgrundlage ergeben.

Im Folgenden werden die Regelungen des AZRG an diesen europa- und verfassungsrechtlichen Vorgaben gemessen. Soweit sich hieraus Defizite ergeben, werden Vorschläge zur Behebung dieser Defizite erarbeitet.

3 Verbot umfassender Überwachung

Das BVerfG hat schon früh in Konkretisierung des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein Verbot des Erstellens von **umfassenden Persönlichkeitsbildern** statuiert. Es ist demnach mit der Menschenwürde nicht vereinbar, „wenn der Staat für sich das Recht in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren“.[38] Vor allem bei der Integration automatisierter Informationssysteme entstehe die Gefahr, dass Personendaten zu einem „teilweisen oder weitgehend vollständigen Persönlichkeitsprofil zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend

[38] BVerfG 16.07.1969 – 1 BvL 19/63 Rn. 24, BVerfGE 27, 6, NJW 1969, 1707.

kontrollieren kann“.[39] Dies ist besonders problematisch, wenn die Verarbeitung zwangsweise oder heimlich erfolgt. Nicht erst das Erstellen von solchen Profilen ist untersagt, sondern auch die systematische Datensammlung zu einem Menschen hierfür.[40]

Ursprünglich zielte das AZR auf die Bereitstellung von Informationen vorrangig für aufenthalts- und sicherheitsrechtliche Zwecke. Seit 2016 kamen zunehmend arbeitsrechtliche, soziale und gesundheitsvorsorgende Zwecke hinzu. Die AZR-Speicherung begleitet einen Ausländer von seiner erstmaligen, nicht nur vorübergehenden Einreise bis lange nach seiner Ausreise oder bis zu seinem Tod. Damit eignet sich das AZR als **Instrument zur Erstellung umfassender Persönlichkeitsbilder**.[41] Die Möglichkeiten zur digitalen Dateneinspeisung (§ 7 AZRG) erlauben eine dauernde Aktualisierung der Profile. Umfassende Persönlichkeitsbilder können, insbesondere bei Defiziten hinsichtlich der Richtigkeit und Aktualität der Daten,[42] für die Betroffenen zu massiven Beeinträchtigungen führen. Mit der weitgehend online verfügbaren Abfragemöglichkeit für sämtliche öffentliche Stellen (§§ 5, 14, 22 AZRG) stehen diese Daten zur Profilerstellung umfassend zur Verfügung.

3.1 Verhinderung eines Überwachungsstaates

Mit der Verhinderung umfassender Persönlichkeitsprofile soll nicht nur der individuelle Schutz der einzelnen Menschen bewirkt werden. Vielmehr geht es auch um den Schutz der demokratischen Gesellschaftsordnung, da „Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist“.[43] Es gehört „zur **verfassungsrechtlichen Identität der Bundesrepublik Deutschland**“, dass eine „möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten“ verhindert wird. Die vorsorgliche anlasslose Speicherung muss die Ausnahme bleiben: „Sie darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen.“ Der Gesetzgeber ist verpflichtet, „bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen, schon vorhandenen Datensammlungen“ Zurückhaltung zu üben. Durch vorsorgliche Datenspeicherungen wird „der Spielraum für weitere anlasslose Datensammlungen“ geringer.[44]

Diese Erwägungen sind bei der Datenverarbeitung zu **Menschen mit Migrationshintergrund** von besonderer Bedeutung. Diese Menschen kommen oft aus Staaten, in denen keine freiheitlichen und demokratischen Rechte gewährt werden und in denen keine

[39] BVerfG 15.12.1983 – 1 BvR 209 u.a., Rn. 145, NJW 1984, 421.
[40] BVerwG 21.3.1986 – 7 C 71/83, NJW 1986, 1329. 2330.
[41] So schon 23. TB HDSB 1994, 122; *Frankenberg*, FS Simitis, S. 105.
[42] Derartige Defizite bestehen beim AZR in großem Maße; dazu GFF, Das Ausländerzentralregister, 2022, 12 f.
[43] BVerfG 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 422.
[44] BVerfG 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 Rn. 218, NJW 2010, 839; dazu *Roßnagel* NJW 2010, 1238.

Rechtsstaatlichkeit herrscht. Bei solchen Menschen kommt der Vermittlung der freiheitlichen Werte eine wichtige Funktion zu, um deren Integration zu erleichtern und zugleich die Freiheitlichkeit unserer Gesellschaft zu wahren. Voraussetzung für die Vermittlungen dieser Werte ist, dass diese Menschen entsprechend dieser Werte behandelt werden und dass sie ihre Rechte auch tatsächlich wahrnehmen können.

3.2 Nationale Kennziffern

Eine umfassende Überwachung von Menschen wird dadurch erleichtert, dass diesen ein für viele Register und Dateien geltendes **Personenkennzeichen** zugewiesen wird, mit dem Daten aus unterschiedlicher Herkunft, die für unterschiedliche Zwecke erhoben wurden, zusammengeführt werden können. Wegen dieser Eignung zur Totalkontrolle von Menschen wurden solche Kennzeichen in Deutschland verfassungsrechtlich lange Zeit als unzulässig angesehen. Das Verbot zielte darauf ab, die Erstellung von umfassenden Persönlichkeitsprofilen zu verhindern.[45] Rechtlicher Hintergrund dieses Verbots sind die historischen Erfahrungen in Deutschland mit solchen Kennzeichen. Die Verfolgung und teilweise die Ermordung von Menschen im Nationalsozialismus basierte auf einer solchen zentralen einheitlichen Erfassung.[46] Für Überwachungs- und Kontrollzwecke wurde in der ehemaligen DDR eine Personenkennzahl (PKZ) verwendet, mit der die Daten aus verschiedenen Verwaltungs- und Lebensbereichen zusammengeführt wurden.[47]

Entsprechende negative Erfahrungen der staatlichen Überwachung und Unterdrückung mit einer zweckübergreifenden **nationalen Kennziffer** bestehen in anderen EU-Mitgliedstaaten nicht. Solche Kennziffern kommen dort teilweise schon seit vielen Jahren zum Einsatz. Sie dienen der einfachen Identifikation von Personen und zur technisch-organisatorischen Vereinfachung bei der Kommunikation zwischen Behörden oder im Geschäftsverkehr. Sie werden nun in Art. 87 DSGVO ausdrücklich erlaubt, aber, um ihren Missbrauch zu verhindern, „nur unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung“ (Art. 87 S. 2 DSGVO). Von einer nationalen Kennziffer ist auszugehen, wenn sie in einem Mitgliedstaat umfassend zum Einsatz kommt.[48]

3.3 AZR-Nummer

Gemäß § 3 Abs. 1 Nr. 2 wird zu jeder im AZR gespeicherten Person „das Geschäftszeichen der Registerbehörde (AZR-Nummer) gespeichert. Das Zeichen dient der eindeutigen Identifizierung des Betroffenen. Mit ihr ist außer der Verweisinformation die Aussage verbunden, dass der Betroffene keine deutsche Staatsangehörigkeit hat und dass Daten über ihn im AZR gespeichert sind. Die AZR-Nummer enthält: Tagesdatum der ersten Speicherung

[45] *Kirchberg* ZRP 1977, 137 ff.; *Weichert* RDV 2002, 170; *Bizer*, DuD 2004, 45; *Weichert* in *Däubler u.a.*, Bundesdatenschutzgesetz, 5. Aufl. 2016, Einleitung Rn. 47 f.
[46] *Weichert* in GK-AufenthG, Vorb AZRG Rn. 1 f.
[47] *Bizer* DuD 2004, 45; *Weichert* RDV 2002, 172 m.w.N.
[48] *Weichert* in *Kühling/Buchner*, Art. 87 Rn. 9, 12

und eine laufende Nummer nach der zeitlichen Reihenfolge der Speicherung an diesem Tag. Es handelt sich also um eine nur begrenzt „sprechende Nummer".[49] Die AZR-Nummer wird bei der erstmaligen Übermittlung von Daten zu einer Person, über die noch kein Datensatz vorhanden ist, vergeben. Ist die AZR-Nummer einer Stelle bekannt, die mit dem AZR wegen eines Ausländers kommuniziert, so muss sie angegeben werden (§ 10 Abs. 2 S. 1 AZRG). So soll die Inanspruchnahme des „Ähnlichenservices" (§ 10 Abs. 3 AZRG) vermieden werden, bei dem es beim Vorhandensein von ähnlichen Angaben zu mehreren Personen zu einer Datenübermittlung bzgl. all dieser Personen kommt. Das AZR hat programmtechnisch sicherzustellen, dass eine fehlerhafte Nutzung der AZR-Nummer erkannt wird (§ 2 Abs. 2 AZRG-DV). Der AZR-Nummer kommt als **Zuordnungsinstrument** eine wichtige Konzentrationsfunktion zu. Alle anfragenden öffentlichen Stellen erhalten nach § 14 Abs. 1 AZRG die Nummer übermittelt. Dies wird im Interesse einer schnellen und zweifelsfreien Identifizierung durch diese Behörden für notwendig angesehen.[50]

Die AZR-Nummer kommt im Umgang mit Daten von Nichtdeutschen in praktisch **allen Behörden in Deutschland** zum Einsatz, soweit diese mit dem AZR bzw. dem Bundesamt für Migration und Flüchtlinge (BAMF) kommunizieren. Dies sind nicht nur Ausländer- und Asylbehörden, sondern auch Sicherheitsbehörden sowie Sozialleistungsträger.

Die AZR-Nummer darf nur im **Verkehr zwischen den genannten Stellen** genutzt werden (§ 10 Abs. 4 S. 1 AZRG). Damit soll vermieden werden, dass die AZR-Nummer als allgemeines Personenkennzeichen verwendet wird. Anderen als öffentlichen Stellen soll die AZR-Nummer nicht zur Verfügung stehen. Ob diese Vorkehrung zur Verhinderung der beliebigen Verknüpfbarkeit geeignet ist, war von Anfang an umstritten.[51] Die erlaubte Kommunikation beschränkt sich nicht auf eng definierte Zwecke. Die AZR-Nummer wird nicht nur in einem Zweckzusammenhang genutzt, sondern ist von „allgemeiner Bedeutung".[52]

Solange sich die Verwendung noch weitgehend auf asyl- und aufenthaltsrechtliche Zwecke beschränkte, konnte davon ausgegangen werden, dass es sich bei der AZR-Nummer um eine administrative Ordnungsnummer handelt, auch wenn diese für Sicherheitszwecke zum Einsatz kam.[53] Mit den Gesetzesänderungen im DAVG und dem 2. DAVG 2016 und 2019 wurde die AZR-Nummer aber zum **Zuordnungsmerkmal für praktische alle öffentlichen Stellen**, die mit einem Ausländer zu tun haben, insbesondere auch für die Arbeits-, die Sozial- und die Gesundheitsverwaltung.[54]

[49] § 2 Abs. 1 S. 2 AZRG-DV, *Weichert* in *Kühling/Buchner*, Art. 87 Rn. 16.
[50] *Streit/Heyder*, AZR-Gesetz, § 3 Rn. 4.
[51] *Weichert*, AZRG1998, § 3 Rn. 6; *Scheuerer* in *Appel/Hummel*, Vorsicht Volkszählung, 3. Aufl. 1987, S. 174; *Weichert* Bürgerrechte & Polizei [CILIP] Nr. 31 [3/1988], 25; *ders*, InfAuslR 1989, 6 f.; *Frankenberg*, FS Simitis, S. 105 f.
[52] *Weichert* in *Kühling/Buchner*, Art. 87 Rn. 11, 22
[53] So noch *Weichert* in *Kühling/Buchner*, 2. Aufl. 2018, Art. 87 Rn. 22
[54] 27. TB BfDI 2017-2018, Kap. 9.1.1, S. 65; Netzwerk Datenschutzexpertise, Stellungnahme 2. DAVG, 5 f.

Die Nutzung der AZR-Nummer ist in vielen **Gesetzen** ausdrücklich vorgesehen. Die Duldungsbescheinigung und die Fiktionsbescheinigung nach §§ 60a Abs. 4, 81 Abs. 5 AufenthG enthalten die AZR-Nummer (§ 87a Abs. 5 AufenthG) ebenso wie die Mitteilungen der Ausländerbehörden an die Meldebehörden (§ 90a Abs. 2 Nr. 6 AufenthG). Sie ist Identifikationszeichen im Register zum vorübergehenden Schutz (§ 91a Abs. 2 Nr. 1e AufenthG). Die AZR-Nummer ist gemäß § 31 Abs. 7 AsylG in Asylentscheidungen zu nennen, nach den §§ 63 Abs. 5 Nr. 3, 63a Abs. 1 S. 1 Nr. 16 AsylG wird sie in die Bescheinigung über die Aufenthaltsgestattung bzw. in die Meldung als Asylsuchender aufgenommen. Sie ist in § 3 Abs. 1 Nr. 17a BMG in der Meldebehörde gespeichert. Selbst im EU-internen Verkehr wird die Nummer genutzt, etwa bei innergemeinschaftlichen Auskünften zur Durchführung der Richtlinie 2003/109/EG (§ 91c AufenthG), der Richtlinie (EU) 2016/801 (§ 91d Abs. 4 S. 2, Abs. 5 S. 3 AufenthG), der Richtlinie 2009/50/EG (§ 91f Abs. 1 S. 3) und der Richtlinie 2014/66/EU (§ 91g Abs. 4 S. 4 AufenthG).

Es ist angesichts der nunmehr gesetzlich erlaubten umfassenden Verwendung der AZR-Nummer davon auszugehen, dass es sich um eine Personenkennzahl sowie um eine nationale **Kennziffer nach Art. 87 DSGVO** handelt.[55]

Geeignete Garantien i.S.v. Art. 87 Abs. 2 DSGVO sind solche, die auf gesetzlicher Grundlage verhindern, dass übermäßig in das Persönlichkeitsrecht von Betroffenen eingegriffen wird. Dazu gehören insbesondere Regelungen zur Transparenz und zur Zweck- und Verwendungsbegrenzung.[56] Eine Zweckbegrenzung war ursprünglich in § 10 Abs. 4 AZRGaF vorgesehen, indem sie nur für die Kommunikation mit dem Register und dem BAFl und den Ausländerbehörden eingesetzt werden durfte. Diese Einschränkung wurde sukzessive aufgegeben, so dass die AZR-Nummer zum Austausch zwischen allen asyl- und aufenthaltsrechtlichen, allen Sicherheitsbehörden, zwischen leistungsgewährenden Behörden und in Bezug auf Flüchtlinge zwischen allen öffentlichen Stellen für Zuordnungszwecke zum Einsatz kommt. Die AZR-Nummer darf nur zusätzlich zu den in § 3 Abs. 1 Nr. 4 AZRG genannten Grundpersonalien verwendet werden (§ 10 Abs. 4 AZRG). Die Beachtung dieser Anforderung wird aber durch keine Kontrollregelung gewährleistet, weshalb diese in der Praxis kaum durchgesetzt werden dürfte.[57] Weitere Beschränkungen der über die AZR-Nummer erschlossenen Daten bestehen nicht. Es fehlen die in Art. 87 S. 2 DSGVO geeigneten Garantien, weshalb die Regelung europarechtswidrig ist. Hierin muss zugleich auch weiterhin ein Verstoß gegen das nationale Verfassungsrecht gesehen werden, das Maßnahmen zur umfassenden Überwachung von Menschen ohne hinreichende Sicherungsmaßnahmen verbietet.

[55] *Weichert* in *Kühling/Buchner*, Art. 87, Rn. 22; ähnlich BfDI, Stellungnahme zu 2. DAVG, 2 f.
[56] *Weichert* in *Kühling/Buchner*, Art. 87 Rn. 15.
[57] *Bäcker*, GFF-Gutachten, 2022, S. 49 lässt dies aber als Garantie genügen.

3.4 ID-Nummer

Mit dem **Registermodernisierungsgesetz** (RegMoG) v. 28.03.2021[58] führt der Bundesgesetzgeber für alle in Deutschland aufhältigen Menschen eine zweckübergreifende einheitliche Identifizierungsnummer (ID-Nummer) ein, die nicht nur für Ausländer, sondern auch für Deutsche registerübergreifend eine sichere Personenzuordnung ermöglichen soll. Die lebenslang gültige ID-Nummer, die identisch mit der Steuer-ID nach § 139b AO ist, wird künftig auch im AZR aufgeführt. Deren Übermittlung an das AZR erfolgt auf der Grundlage des § 6a AZRG. Die generellen Regelungen zur ID-Nummer finden sich im Identifikationsnummerngesetz (IDNrG). Mit diesem Gesetz soll über die Identifikationsnummer (ID-Nummer) in Verwaltungsverfahren die eindeutige Zuordnung zu einer natürlichen Person ermöglicht werden (§ 1 Nr. 1 IDNrG). Dem dient auch die Speicherung im AZR (Nr. 3 Anlage zu § 1 IDNrG).

Mit dem RegMoG wird wurde das AZRG um § 3 Abs. 5 ergänzt. Danach werden im AZR bei Ausländern nach § 2 Abs. 1a und 2 Nr. 1-4, 9, 10, 13, 14, Abs. 3 Nr. 1-4 AZRG zur Erfüllung der Aufgaben nach § 2 IDNrG und zur Erbringung von Verwaltungsleistungen i.S.d. OZG die **Identifikationsnummer (ID-Nummer)**, evtl. eine Auskunftssperre nach dem BMG und das Datum des letzten Verwaltungskontaktes gespeichert. Zugleich wird in § 6 Abs. 1 Nr. 10 AZRG geregelt, dass die Registermodernisierungsbehörde, also das Bundesverwaltungsamt (BVA, § 3 Abs. 1 S. 2 IDNrG), der AZR-Registerbehörde, also dem Bundesamt für Migration und Flüchtlinge (BAMF, § 1 Abs. 1 S. 1 AZRG), in den genannten Fällen die genannten Daten mitteilt, so dass bezüglich des Datenflusses ein „Rückweg“ aus der Verwaltung an das BAMF besteht

Die Regelung des § 3 Abs. 5 AZRG betrifft explizit folgende **Personen**: Asylsuchende, unerlaubt eingereiste oder aufhältige Ausländer (§ 2 Abs. 1a AZRG), Personen mit vorübergehendem Schutz, Betroffene von aufenthaltsrechtlichen Entscheidungen sowie von Einreisebedenken, ablehnte Staatsangehörigkeitsantragsteller, Aussiedler und Vertriebene, ohne Pass Eingereiste, über Visum Eingereiste, für die eine Verpflichtungserklärung abgegeben wurde (§ 2 Abs. 2 Nrn. 1-4, 9, 10, 13, 14 AZRG), nicht ausgeschriebene Unionsbürger (§ 2 Abs. 3 Nrn. 1-4 AZRG). Die Regelung ist irritierend, da in ihr – unjuristisch formuliert - nur Flüchtlinge aufgeführt werden. Aus § 6a AZRG wie aus der Gesetzesbegründung geht aber hervor, dass zu sämtlichen im AZR gespeicherten Personen die ID-Nummer als „optionales Ordnungsmerkmal zur Verfügung“ stehen soll.[59]

Gemäß Art. 22 RegMoG tritt die **Regelung in Kraft**, sobald das Bundesministerium des Innern, für Bau und Heimat im Bundesgesetzblatt bekannt gibt, dass die technischen Voraussetzungen für den Betrieb nach dem Identifikationsnummerngesetz gegeben sind.

[58] BGBl. I S. 591.
[59] BT-Drs. 19/24226 S. 84 f.

Die **Verfassungsgemäßheit des RegMoG** war im Gesetzgebungsverfahren sehr umstritten, da es sich bei der ID-Nummer um ein einheitliches Personenkennzeichen handelt.[60] Konsens besteht aber insofern, dass nach der Einführung der ID-Nummer die Bildung von Teil- und Totalprofilen zu einer Person verhindert werden muss. Dem dient ein sog. 4-Corner-Modell. Das 4-Corner-Modell ist eine IT-Architektur nach dem Prinzip des „Privacy by Design". Kern ist die dezentrale Datenhaltung in getrennten Registern bei gleichzeitiger eindeutiger Zuordenbarkeit über eine zentrale Personenidentifikationsnummer und die kontrollierte Kommunikation über Intermediäre. Der Datenaustausch zwischen Registern erfolgt unter Nutzung folgender Sicherungsmechanismen: Verteilte digitale Zugangselemente (ID-Nummer, Registeradresse und ein Einmal-Sicherheitstoken für jede Übermittlung), eine Rechtsprüfung und Verschlüsselung der Datenübertragung, eine berechtigungsspezifische Datenabfrage sowie Transparenz und Kontrolle (ex-ante und ex-post) der Datenverarbeitung (§ 7 Abs. 2 IDNrG).[61] Es werden zudem mindestens sechs Bereiche nach fachlichen Kriterien gebildet.[62] Die Vermittlungsstellen in diesen Bereichen sollen die Übermittlung auf der Grundlage der ID-Nummer für zwei Jahre protokollieren (§ 9 IDNrG) und kontrollieren. Die Authentizität jedes Datenabrufs soll über technische Verfahren gewährleistet (§ 8 Abs. 3 IDNrG), die Abrufberechtigung durch Stichprobenkontrollen kontrolliert werden (§ 8 Abs. 4 IDNrG). Ausgetauscht werden dürfen mit Hilfe der ID-Nummer nur Basisdaten (Namen, Doktorgrad, Geburtsdaten, Geschlecht, Anschrift, § 4 Abs. 2 IDNrG). Zusätzliche Übermittlungen werden mit dem Gesetz nicht erlaubt, so dass die bisherigen gesetzlichen Zweckbindungsregelungen bzgl. aller weiteren Daten weiterhin gelten sollen.

Gemäß § 9 OZG ist die Etablierung eines **Datencockpits** vorgesehen, der es den Betroffenen ermöglicht, im Nachhinein die über die ID-Nummer durchgeführten Datenübermittlungen nachzuvollziehen und zu kontrollieren. Es sind technische Schutzvorkehrungen vorzusehen (§ 7 Abs. 2 IDNrG). In einer Verordnung sind die Maßnahmen zu konkretisieren (§ 12 IDNrG). Die Registermodernisierungsbehörde ist durch den BfDI zweimal alle zwei Jahre zu kontrollieren (§ 13 IDNrG). Datenschutzverstöße sind strafrechtlich sanktionierbar (§ 17 IDNrG). Ob diese Vorkehrungen als Garantien zur Verhinderung von Persönlichkeitsprofilen genügen, kann hier nicht ausführlich behandelt werden.[63] Sie beschreiben in jedem Fall Maßnahmen, die geeignet und damit erforderlich sind, um auf dieses Ziel hinzuwirken.

[60] Deutscher Bundestag, Wissenschaftlicher Dienst, Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines Registermodernisierungsgesetzes (Ausarbeitung WD 3 – 3000 – 196/20).

[61] *Parycek/Hunt/Thapa*, Technische Perspektiven der Registermodernisierung, 08.02.2021, https://www.oeffentliche-it.de/documents/10181/188095/Technische+Perspektiven+der+Registermodernisierung.pdf; *Peuker*, NVwZ 2021, 1167 ff.

[62] Die Entwurfsbegründung nennt exemplarisch Inneres, Justiz, Wirtschaft und Finanzen, Arbeit und Soziales, Gesundheit, Statistik, BT-Drs. 19/24226, 74.

[63] *Von Lewinski/Gülker* DVBl 2021, 633 ff. m.w.N.; kritisch z.B. Konferenz der unabhängigen Datenschutzaufsichtsbehörden, 20.08.2020, Registermodernisierung verfassungskonform umsetzen.

Der Gesetzgeber sieht mit der Einführung einer einheitlichen ID-Nummer ein Instrument vor, das für den Datenaustausch über Nichtdeutsche schon seit langem mit der **AZR-Nummer** besteht. Er hat aber bisher nicht geregelt, ob und inwieweit die AZR-Nummer beibehalten werden soll, nachdem die ID-Nummer in der Praxis eingeführt wurde. Es ist offensichtlich, dass die Notwendigkeit für die AZR-Nummer dann nicht mehr besteht. Angesichts der rechtlichen Problematik der AZR-Nummer (s.o. 3.3) muss diese spätestens nach Einführung der ID-Nummer abgeschafft werden. Anderenfalls bestünde die Gefahr, dass die für die Verwendung der ID-Nummer vorgesehenen Garantien durch die Verwendung der AZR-Nummer ohne Schutzvorkehrungen umgangen würden.

3.5 Reformbedarf bzgl. der AZR-Nummern-Verwendung

Angesichts des zeitlichen Zusammenfallens der Gesetzgebung zum AZRWeiterentwG und zum RegMoG war es naheliegend, die im RegMoG vorgesehenen Garantien auf die AZR-Nummer zu übertragen. Daher hat das Netzwerk Datenschutzexpertise in seiner Stellungnahme vom Mai 2021 zur AZRG-Änderung die Aufnahme eines § 34a vorgeschlagen, um für die Verwendung der AZR-Nummer ein **Datencockpit** vorzusehen, das sich an § 10 OZG orientiert.[64] Damit sollten sich Betroffene nach einer Registrierung Datenübermittlungen mit der eigenen AZR-Nummer anzeigen lassen können.[65] Dadurch würde für die Betroffenen wie für die Allgemeinheit die Transparenz erheblich verbessert. Zugleich würde die Möglichkeit für einen effektiven Rechtsschutz erhöht, um evtl. unzulässige Datenübermittlungen zu erkennen und gerichtlich zu beanstanden. Der Vorschlag wurde vom Gesetzgeber nicht umgesetzt.

Bisher ist die **Datenschutzkontrolle** beim AZR ungenügend. Der BT-Innenausschuss bekräftigte mit Entschließung vom 17.05.2021, dass „eine effektive und regelmäßige datenschutzrechtliche Kontrolle des AZR besondere Bedeutung“ hat. Daher sei der BfDI „bei der datenschutzrechtlichen Kontrolle zu unterstützen, indem das Recht auf präventive Überprüfung von Übermittlungsersuchen weiter verbessert und die Auswertbarkeit der Protokollierung vereinfacht wird“.[66] Durch die Einführung verpflichtender Kontrollen, wie sie z.B. an anderer Stelle gesetzlich vorgesehen sind (§ 13 IDNrG, § 10 Abs. 2 AntiterrordateiG, § 11 Abs. 2 Rechtsextremismusdateigesetz), könnten die Kontrolldefizite verringert werden.

Im RegMoG sind **weitere Maßnahmen** als Garantien für die Betroffenen beim Einsatz der ID-Nummer vorgesehen, die für die Verwendung der AZR-Nummer übernommen werden können. Auch diese Maßnahmen sind in Bezug auf die AZR-Nummer nicht gesetzlich geregelt worden.

[64] Netzwerk Datenschutzexpertise, Stellungnahme v. 24.04.2021, BT-Innenausschuss, A-Drs. 19(4)820 C, 8.
[65] Der Bedarf hieran wurde im BT-Innenausschuss festgestellt: A-Drs. 19(4)851 Nr.II 4, BT-Drs. 19/29820, S. 29.
[66] A-Drs. 19(4)851 Nr.II 4, BT-Drs. 19/29820, S. 29.

3.6 Ausländische Personenidentitätsnummer

Die ausländische Personenidentitätsnummer (CNP-Nummer – Code Numeric Personal) wurde als Identifikationsmerkmal mit G. v. 9.7.2021[67] erstmals in das AZR und generell im deutschen Recht eingeführt (§ 3 Abs. 1 Nr. 5b AZRG). Mit ihr soll die Identitätsfeststellung in Fällen einer Namensänderung oder einer Identitätstäuschung, etwa zur Bekämpfung von Leistungsmissbrauch ermöglicht werden. Mit ihr sollen Abfragen in Fahndungssystemen vorgenommen werden können.[68] Über sie lassen sich vielfältige **Datenbestände in einem Herkunftsland** erschließen; deutsche Daten können mit solchen des Herkunftslandes zusammengeführt werden. Diese Möglichkeit wird insbesondere Sicherheitsbehörden eröffnet (§ 6 Abs. 1 Nr. 2, 4 ff. AZRG, § 6 Abs. 2 S. 3 Nr. 1, 2, 44, 4a, 5, 5a AZRG). Diese können die CNP-Nummer vom AZR erhalten und weiterverarbeiten (§§ 15, 20 AZRG) und potenziell an Behörden in Drittstaaten übermitteln. Genutzt werden kann die CNP-Nummer im Rahmen von Ersuchen nach § 5 AZRG – für alle öffentlichen Stellen (§ 6 Abs. 4 AZRG-E).[69] Sie dient zudem der Datenbeschaffung und der Zuordnung durch Zoll- und Sozialbehörden (z.B. § 17 Abs. 1 Nr. 5a AZRG). § 26 AZRG schließt gesetzlich nicht aus, dass sich Behörden, insbesondere Sicherheitsbehörden des Heimatlands, über die CNP-Nummer aus dem AZR stammende sensitive Daten von Staatsangehörigen beschaffen, um diesen zu schaden.[70]

Auch bei den ausländischen Personenidentitätsnummern handelt es sich um **nationale Kennzeichen** i.S.v. Art. 87 DSGVO. Diese Regelung ist anwendbar, wenn eine Ziffer eines ausländischen Staates, auch von außerhalb der EU, als Personenkennziffer innerhalb der EU zur Anwendung kommt. Die Nutzung dieser Nummer erhöht das Risiko massiv, dass Daten aus dem Ausland am Betroffenen vorbei erhoben oder dorthin übermittelt werden. Für die Beschaffung der Nummer durch deutsche Behörden genügt deren Erforderlichkeit. Gemäß Art. 87 S. 2 DSGVO ist die Verwendung solcher Nummern nur „unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person“ zulässig. Diese sind insbesondere bei einer Verwendung durch Sicherheitsbehörden, die einen internationalen Datenaustausch praktizieren, geboten.

Eine solche Garantie könnte darin bestehen, dass vor jeder Übermittlung durch das AZR oder durch eine andere Stelle, die vom AZR die ausländische Personenidentitätsnummer erhalten hat, an eine ausländische Stelle eine Prüfung erfolgen muss, ob und inwieweit hierdurch eine Gefährdung des Betroffenen oder von ihm nahestehenden Personen verursacht werden kann. Im Rahmen einer solchen **Gefährdungsprüfung** könnte eine Anhörung des Betroffenen vorgenommen werden.

[67] BGBl. I S. 2467.
[68] BT-Drs. 19/28170, 72.
[69] Kritisch Deutsche Vereinigung für Datenschutz, PM v. 09.02.2021, DANA 1/2021, 30.
[70] Anders Antwort Nr. 7 u. 8 der BReg v. 13.04.2021 auf die kleine Anfrage BT-Drs. 19/28123; zu Datenlecks im Ausland GFF, Das Ausländerzentralregister, 2022, 16.

§ 10 Abs. 4a AZRG sieht vor, dass die mit dem AZRWeiterentwG eingeführte ausländische Personenidentitätsnummer nur zum **Zweck der eindeutigen Identifizierung** genutzt werden darf. Diese Regelung wurde im Gesetzgebungsverfahren wegen der Erkenntnis eingefügt, dass ein Datenabgleich auf Grundlage dieser Nummer zu Gefährdungen der Betroffenen führen kann.[71] Diese Regelung betrifft nicht nur das AZR, sondern insbesondere dritte, mit dem AZR kommunizierende Stellen. § 26 S. 2 i.V.m. § 14 Abs. 1 Nr. 1-5 AZRG hat zur Folge, dass die Nummer nicht an Drittstaaten i.S.v. § 1 Abs. 6 S. 2 BDSG übermittelt werden dürfen. Diese Einschränkung ist aber für abrufende Stellen nicht erkennbar und dürfte regelmäßig auch nicht bekannt sein. An Behörden von Mitgliedstaaten der EU darf die Nummer übermittelt werden. Diese sind durch die Verwendungsbeschränkung der §§ 26 Abs. 2, 14 Abs. 1 AZRG nicht gebunden. Es ist kein Verfahren vorgesehen, das die vorgeschriebene Zweckbindung – bei Behörden in Deutschland oder in der EU – sicherstellt.[72] Behörden der Heimatstaaten der Betroffenen können erst recht nicht hierdurch rechtlich gebunden werden. Die gesetzliche Vorkehrung berücksichtigt zudem nicht, dass die eindeutige Identifizierung nur der Primärzweck für einen sekundären Hauptzweck sein kann. Die Identitätsfeststellung dient immer einem Hauptzweck, z.B. der Umsetzung einer ausländerrechtlichen Maßnahme, der Erbringung einer Sozialleistung oder der Strafverfolgung (s.u. 4).

Es fehlt somit an **wirksamen spezifischen Schutzvorkehrungen** bei der Verwendung der ausländischen Personenidentitätsnummer.[73] Deren Einführung verstößt deshalb gegen zwingendes europäisches Recht.

4 Zweckbindung

Zentral für die Wahrung der Freiheitsrechte der Menschen in einer digitalisierten Gesellschaft ist der Zweckbindungsgrundsatz. Die Zweckbindung findet ihre **europarechtliche Grundlage** in Art. 8 Abs. 2 S. 1 GRCh und ihre Konkretisierung in Art. 5 Abs. 1 lit. b DSGVO. Gemäß diesem Grundsatz müssen personenbezogene Daten „für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden“. Die Zweckbindung soll es den Betroffenen ermöglichen, in ihrem Leben in verschiedenen Rollen jeweils eine eigene Identität zu entwickeln und zu entfalten. Sie soll verhindern, dass Persönlichkeitsbilder entwickelt werden, die für die Wahrnehmung und die Behandlung der betroffenen Menschen bestimmend werden.[74]

Der Zweckbindungsgrundsatz ist eng mit dem verfassungsrechtlichen **Bestimmtheitsgebot** (s.u. 6) verbunden. Das Bestimmtheitsgebot wird aus dem Rechtsstaatsgebot (Art. 20 Abs. 3 GG) abgeleitet, wonach hinreichende Bestimmtheit und Klarheit der die Eingriffe

[71] *Lehmann*, BT-Pl.Pro. 19/29902 v. 09.06.2021.
[72] *Bäcker*, GFF-Gutachten, 2022, S. 30.
[73] *Wittmann*, Stellungnahme v. 30.04.2021, BT-Innenausschuss, A-Drs. 19(4)820 D, 19 ff.; *Weichert*, Stellungnahme v. 24.04.2021, BT-Innenausschuss A-Drs. 19(4)820 C, 3; *Petri*, Stellungnahme v. 28.04.2021, BT-Innenausschuss A-Drs. 19(4)820 A 5 f.
[74] *Weichert* in *Däubler u.a.*, Art. 5 Rn. 28.

rechtfertigenden Normen nötig sind. Dies gilt bei einer personenbezogenen Datenverarbeitung insbesondere für den rechtmäßig zu verfolgenden Zweck. Die Regelungen müssen so genau gefasst sein, dass der Betroffene die Rechtslage (Inhalt und Grenzen der Verarbeitung) erkennen und sein Verhalten daran ausrichten kann. Zwar ist die Verwendung unbestimmter Rechtsbegriffe möglich. Es müssen sich aber durch Auslegung objektive Kriterien für deren Anwendung entwickeln lassen. Der Betroffene muss im Ergebnis die Rechtslage mit zumutbarem Aufwand erkennen können. Je intensiver in die Rechte von Betroffenen eingegriffen wird, desto höhere Anforderungen sind an die Bestimmtheit der Regelung und der verwendeten Rechtsbegriffe zu stellen.[75]

Die äußeren Grenzen von **Zweckänderungen** werden in Art. 6 Abs. 4 DSGVO festgelegt. Die Konturen der Zweckbindung werden im ErwGr 50 zur DSGVO näher beschrieben. Zur Beantwortung der Frage nach der Zulässigkeit einer Zweckänderung hat eine zweistufige Prüfung zu erfolgen: Zunächst bedarf es der Feststellung, dass die Zweckverfolgung rechtmäßig ist; im zweiten Schritt ist zu prüfen, ob die Zweckänderung gegen Art. 6 Abs. 4 verstößt. Art. 6 Abs. 4 DSGVO nennt als Kriterien für die **Zweckvereinbarkeit** die Verbindung zwischen Primär- und Hauptzweck (lit. a), den Erhebungskontext und dessen Beziehung zum Verantwortlichen (lit. b), die Sensitivität der Daten (lit. c), die Folgen der Weiterverarbeitung für den Betroffenen (lit. d) und das Vorhandensein geeigneter Garantien (lit. e).

Um das Erstellen und das Nutzen von Persönlichkeitsbildern abzuwenden, fordert das BVerfG grundsätzlich eine **strenge Zweckbindung**. Eine Datenverarbeitung ist verfassungswidrig, wenn damit Zwecke verfolgt werden, bei denen tendenziell Unvereinbares miteinander verbunden wird.[76] Beim AZR werden verschiedene Verarbeitungszwecke gebündelt.[77] Es ist daher zu prüfen, ob diese im genannten Sinne tendenziell vereinbar sein können.

Das AZR erfüllt mehrere Funktionen, die vom Gesetzgeber als **Identifizierungsfunktion, Nachweisfunktion und Substitutionsfunktion** bezeichnet werden.[78] Mit dem AZR sollen Ausländer identifiziert werden. Es soll diejenigen Behörden nachweisen, die über nähere Informationen zu einer Person verfügen. Bei Eilentscheidungen, für die eine Anfrage bei der aktenführenden Behörde unvertretbar lange Zeit in Anspruch nähme, soll das AZR diese Behörden ersetzen.[79]

Durch die Übermittlung der Daten an das AZR verlieren diese ihren bisherigen Verwendungszusammenhang und werden **kontextfrei zur weiteren Übermittlung angeboten**.

[75] BVerfG 15.12.1983 – 1 BvR 209/83 u.a., Rn. 101, NJW 1984, 422; *Roßnagel* in *Simitis/Hornung/Spiecker*, Art. 6 Abs. 3 Rn. 29 m.w.N.
[76] BVerfG 15.12.1983 – 1 BvR 209 u.a. Rn. 195, NJW 1984, 422 f., 426.
[77] *Bäumler* DuD 1994, 540; *ders*. NVwZ 1995, 243; *Weichert* InfAuslR 1989, 7.
[78] BT-Drs. 12/6938, 16; *Weichert* InfAuslR 1987, 207 f.
[79] Kritisch hierzu *Weichert*, InfAuslR, 1989, 4.

Die vom AZR zu erfüllenden Informationsfunktionen stellen jedoch keine Zwecke im Sinne des Datenschutzrechts dar.[80]

Die datenschutzrechtlich **relevanten Zwecke** werden beschrieben mit der Durchführung des Ausländer- und Asylrechts, der Strafverfolgung, der Gefahrenabwehr bzw. der sonstigen Aufgabenerfüllung der Daten anliefernden und der abfragebefugten Stellen. Zu den Zwecken im Rahmen von Verwaltungs- und Strafverfahren und in gewissem Umfang privaten Zwecken kommen noch die mit AZR-Daten verfolgten statistischen und planerischen Zwecke (§§ 23 f. AZRG). Der Gesetzgeber verlässt beim AZRG bewusst das Prinzip der „informationellen Gewaltenteilung".[81]

4.1 Allgemeine Normen

Die grundlegende Norm zur Zweckbindung der Nutzung von AZR-Daten enthält § 11 AZRG. § 11 Abs. 1 S. 1 AZRG sieht vor, dass der Datenempfänger bestimmte Daten nur zu dem Übermittlungszweck verwenden darf. Die in § 3 Abs. 1 Nr. 7 i.V.m. § 2 Abs. 2 Nr. 7 u. 7a (Verdächte über bestimmte Straftaten) sowie § 3 Abs. 4 Nr. 7 i.V.m. § 2 Abs. 3 Nr. 7 (terroristische Gefahr geht von Unionsbürger aus) bezeichneten Daten, die im Rahmen von Gruppenauskünften übermittelten Daten (§ 12 AZRG) und übermittelte Dokumente (§ 6 Abs. 5 AZRG) dürfen nur zu dem Zweck verwendet werden, zu dem sie der empfangenden Stelle übermittelt worden sind. Sonstige Daten darf die empfangende Stelle zu einem anderen Zweck verwenden, wenn sie ihr **auch zu diesem Zweck hätten übermittelt werden dürfen** (§ 11 Abs. 1 S. 2).

4.2 Identifizierungsfunktion

Unbestimmte Zwecke sind aus Datenschutzsicht unproblematisch, soweit von der Verarbeitung präzise definierte Angaben zu Sachverhalten betroffen sind, die für die Betroffenen relativ unsensibel sind, wie dies im Melderecht weitgehend der Fall ist. Das Melderecht dient dem Nachweis der Identität und der Wohnung (§ 2 Abs. 1 BMG). Hierfür werden insbesondere folgende Angaben verwendet: Namen, Angaben zu Geburt und Geschlecht, Staatsangehörigkeit, Angaben zu Wohnanschriften und zu Ehegatten/Lebenspartner und Kinder sowie zu Ausweisdokumenten (§ 3 Abs. 1 BMG). Diese Angaben entsprechen in etwa den **Grundpersonalien** und weiteren Personalien in § 3 Abs. 1 Nr. 4, 5 AZRG.

Grunddaten gemäß § 14 Abs. 1 unterliegen keiner spezifischen Zweckbindung (§ 10 Abs. 1 S. 2, vgl. § 11 Abs. 1 S. 3 AZRG). Diese „Zweckfreiheit" geht weiter als im Melderecht und erstreckt sich nicht nur auf die „Grundpersonalien": Nach § 14 Abs. 1 AZRG dürfen auch das Lichtbild, Zu- und Fortzugsdaten, ja sogar das Vorliegen von Übermittlungssperren übermittelt

[80] *Frankenberg*, FS Simitis, S. 102 ff.
[81] BVerfG 15.12.1983 – 1 BvR 209 u.a. Rn. 206, NJW 1984, 428.

werden. Diese gesetzliche Freistellung von der Zweckbindung lässt sich bei den Zu- und Fortzugsdaten nicht mehr allein mit der Identifizierungsfunktion des AZR rechtfertigen; daraus lassen sich Aussagen über die Mobilität ableiten. Anders als im AZRG ist für Übermittlungen aus den Melderegistern eine Zweckangabe erforderlich (§ 34 BMG). Für den Wohnungsnachweis außerhalb des Ausländerrechts kann und sollte ausschließlich auf das Melderecht zurückgegriffen werden. Übermittlungssperren dienen dem Schutz der oder des jeweiligen Betroffenen. Sie signalisieren eine besondere Gefährdung.[82] Eine Freigabe von Daten mit dem Merkmal „Übermittlungssperre“ ohne umfassende Zweckbeschränkung ist unverhältnismäßig. Der Verzicht auf die Verpflichtung, bei Übermittlungsersuchen einen Zweck angeben zu müssen, verstößt gegen die Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO.[83]

Das **Lichtbild** ist zur Identifikation geeignet. Es handelt sich um ein sensitives Datum nach Art. 9 Abs. 1 DSGVO.[84] Durch seine biometrische Auswertbarkeit ohne aktive Beteiligung des Betroffenen, sogar im öffentlichen Raum, besteht ein großes Missbrauchsrisiko. Mit ihm sind auch Identifizierungen außerhalb der Verwaltung möglich.[85] § 10 Abs. 2 S. 2 AZRG erlaubt ausdrücklich die Identifizierung allein mit Hilfe des Lichtbildes. Wegen der Fehleranfälligkeit dieser Form biometrischer Identifizierung besteht das Risiko von Falschzuordnungen, die sogar zur Einbeziehung in strafrechtliche Ermittlungen führen können.[86] Angesichts dieser Risiken bedarf es zusätzlicher Garantien bei einer zweckändernden Nutzung des Lichtbildes (vgl. Art. 9 Abs. 2 lit. g DSGVO). Solche Garantien sind nicht vorgesehen. Daher ist die zweckfreie Nutzung des AZR-Lichtbildes unverhältnismäßig und europarechtswidrig (zur sicherheitsbehördlichen Nutzung s.u. 5.4).

4.3 Vereinbarkeitsprüfung

Bei Daten, deren Inhalt über die verwaltungstechnische Identifizierungsfunktion hinausgeht, müsste bei einer **Prüfung der Zweckvereinbarkeit** der Abfragezweck mit dem ursprünglichen Erhebungszweck der erstmals speichernden Stelle ins Verhältnis gesetzt werden (Art. 6 Abs. 4 lit. a DSGVO). Ein solcher Zweckvergleich wird aber dadurch verunmöglicht, dass die ursprünglichen Erhebungszwecke im AZR nicht dokumentiert sind. Diese können allenfalls aus der Art und der Herkunft der Daten vermutet werden. Zwar sehen die Übermittlungsregelungen des AZR oft Differenzierungen hinsichtlich der Datenarten vor. Diese orientieren sich aber ausschließlich am Informationsbedarf der Übermittlungsempfänger. Eine Zweckvereinbarkeitsprüfung, wie sie von Art. 6 Abs. 4 DSGVO

[82] Zu den Defiziten bei der Einrichtung von Übermittlungssperren GFF, Das Ausländerzentralregister, 2022, 10 mit Verweis auf BT-Drs. 19/32508, 13 f.
[83] *Bäcker*, GFF-Gutachten, 2022, S. 40.
[84] *Weichert* in *Kühling Buchner*, Art. 4 Nr. 14 Rn. 3; *Bäcker*, GFF-Gutachten, 2022, S. 39.
[85] *Weichert* DVBl 2021, 1067 f.,
[86] *Weichert* DVBl 2021, 1070.

gefordert wird, ist nicht vorgesehen, so dass im Ergebnis eine ordnungsgemäße Prüfung von Zweckänderungen nicht durchgeführt werden kann.[87]

Je unbestimmter Datenfelder definiert werden und je mehr mit der Datenverarbeitung in die Rechtssphäre der Betroffenen eingedrungen wird, desto mehr müssen die konkret verfolgten **Verwendungszwecke präzisiert** werden. Die Konkretisierung der Verwendungszwecke erfolgt dabei nicht schon bei der Speicherung im AZR, sondern erst bei der Datenübermittlung zur Erfüllung einer bestimmten Aufgabe. Für die Regelung der Befugnis zur Datenverarbeitung genügt es nicht, dass ausschließlich auf die Erforderlichkeit zur „Erfüllung der gesetzlichen Aufgaben“ verwiesen wird[88], so wie dies im AZRG der Fall ist (§ 10 Abs. 1 S. 1 AZRG).

Mit den AZR-Daten können, wie oben dargestellt, viele verschiedene Zwecke verfolgt werden. Die **Problematik der Multifunktionalität** des AZR versucht der Gesetzgeber dadurch **einzugrenzen**, dass er den Zugriff der Stellen auf bestimmte Datenfelder beschränkt. Für die empfangenden Stellen werden aber nur teilweise konkrete Zweckbestimmungen vorgenommen. Konkrete Zwecke sind z.B. die Durchsetzung einer Abschiebung oder eines Einreiseverbotes oder die Durchführung eines bestimmten Strafverfahrens. Die Aufzählung der Zwecke in § 8 Abs. 3 S. 2 AZRG-DV mit insgesamt 34 sehr allgemein gehaltenen Punkten (von „ausländerrechtliche Aufgabe“ bis „Aufgaben nach dem Sechsten Buch Sozialgesetzbuch“ und „Beratung und Bearbeitung von Einbürgerungsanträgen“) sind dagegen oft viel zu unbestimmt. Das Nutzungsspektrum für die Betroffenen ist so nicht überschau- und vorhersehbar.[89]

In einigen Regelungen wird gefordert, dass bei einer Speicherung oder einer Bereitstellung die **schutzwürdigen Interessen** der Betroffenen zu berücksichtigen sind, ohne nähere Kriterien für die Interessenabwägung zu benennen (§§ 4 Abs. 1 u. 2 S. 1, 6 Abs. 2 S. 2, 22 Abs. 2 AZRG). Bei der konkreten Datenübermittlung wird eine Abwägung grundsätzlich verzichtet (Ausnahme § 24a Abs. 1 S. 1 Nr. 3 AZRG). Diese Regelungen sowie weitere bestehende technische und organisatorische Regelungen (zur Protokollierung, Datenpflege, Datenkorrektur) sind aufgrund ihrer spezifischen Funktionsweise nicht hinreichend geeignet, die durch das AZR eingeräumten Verwendungs- und Verknüpfungsmöglichkeiten wirksam einzuschränken. Auch dies steht im Widerspruch zu der in Art. 6 Abs. 4 DSGVO vorgesehenen Abwägungspflicht, die in Bezug auf sensitive Daten in besonderem Maße besteht (Art. 9 Abs. 2 lit. g DSGVO).

4.4 Suchvermerke zur Aufenthaltsermittlung

Bei den Suchvermerken im AZR gemäß § 5 AZRG handelt es sich um eine Art behördliche Fahndungsausschreibung zum Zweck der **Aufenthaltsfeststellung** und der Ermöglichung

[87] *Bäcker*, GFF-Gutachten, 2022, S. 34.
[88] *Simitis* NJW 1984, 398, 400; *ders* in *Simitis*, BDSG, 5. Aufl. 2003, § 4 Rn. 15.
[89] Ähnlich *Bäcker*, GFF-Gutachten, 2022, S. 35 f., der darauf hinweist, dass das vom BVerfG entwickelte Instrument der „hypothetischen Datenneuerhebung“ (s.u. 5 u. 5.5) generell im AZRG nicht abgebildet wird, soweit das AZR als operative Datengrundlage verwendet wird.

administrativer Maßnahmen gegenüber Ausländerinnen und Ausländern.[90] Es ist zugleich ein dauerndes Übermittlungsersuchen. Bei dieser Aufenthaltsermittlung für öffentliche Stellen im allgemeinen AZR-Datenbestand ist es nicht erforderlich, dass die gesuchte Person schon im AZR registriert ist. Da nach § 2 Abs. 2 Nr. 6 AZRG die Ausschreibung zur Aufenthaltsermittlung ein eigenständiger Speicherungsanlass ist, können Personen über Suchvermerke ins Register aufgenommen werden.

Für die Einstellung eines Suchvermerks und eine Treffermeldung durch das AZR genügt es, dass die Kenntnis des Aufenthalts des Betroffenen **zur Aufgabenerfüllung erforderlich** ist (vgl. § 10 Abs. 1 S. 1 AZRG). Bei der Datenübermittlung zu Suchvermerken nach § 5 AZRG wird auf eine konkrete Zweckbestimmung völlig verzichtet. Nach § 5 Abs. 1 AZRG ist es z.B. einer Schule erlaubt, einen ausländischen Schüler, der seiner Schulpflicht nicht nachkommt, über das AZR zu suchen. Ist einer Behörde der Aufenthalt einer Person nicht bekannt, die gegenüber ihr eine offenstehende Forderung hat, so sind die gesetzlichen Voraussetzungen ebenso erfüllt. Nach der Gesetzesformulierung ist gar der Fall vorstellbar, dass das Scheitern der Zustellung von Post, z.B. eines neuen Jahresprogramms einer öffentlich-rechtlich organisierten Volkshochschule, zur Speicherung eines Suchvermerks führt. Erkenntnisse über die tatsächliche Nutzung des § 5 AZRG sind öffentlich nicht bekannt.

Ausschreibungen zur Feststellung des Aufenthaltes sind auch aufgrund weiterer Gesetze möglich, und zwar als polizeiliche Fahndungsausschreibung für Zwecke der Strafverfolgung (z.B. §§ 131, 131a StPO – Festnahme Aufenthaltsermittlung) und zur Gefahrenabwehr (z.B. § 37 BKAG – polizeiliche Beobachtung und gezielte Kontrolle, §§ 30, 31 BPolG – Fahndung, grenzpolizeiliche Bobachtung). Suchvermerke sind außerdem in den §§ 27–29 BZRG im Bundeszentralregister vorgesehen. Diese sind aber regelmäßig nicht online abrufbar.[91] Während die verfolgten Zwecke in den anderen Ausschreibungsregelungen **gesetzlich festgelegt** sind, trifft dies nicht für das Ersuchen nach § 5 Abs. 1 AZRG zu.

Das Einstellen von Suchvermerken im AZR ist keiner unabhängigen Kontrolle unterworfen, über die eine **Verhältnismäßigkeitsprüfung** durchgeführt werden könnte. Gemäß dem Gesetzeswortlaut kann jeder Mitarbeiter einer öffentlichen Stelle, etwa ein Mitarbeiter einer öffentlichen Bibliothek oder ein Polizeibeamter, einen Suchvermerk initiieren. Suchvermerke sind ohne weitere Prüfung gemäß § 14 Abs. 2 AZRG auf besonderes Ersuchen zu übermitteln. Die Grenze des verfassungsrechtlich noch Zulässigen wird dort überschritten, wo Daten durch nicht näher definierte Stellen bzw. für einen nicht näher definierten Zweck verarbeitet werden. Dies trifft zu bei der „Feststellung eines Aufenthalts“ durch jede denkbare öffentliche Stelle nach § 5 Abs. 1 AZRG, wie gar z.B. die oben erwähnte Volkshochschule. Vorkehrungen zur Verhinderung unberechtigter oder unverhältnismäßiger Suchvermerke sieht das Gesetz nicht vor.

[90] *Schriever-Steinberg* NJW 1994, 3277; 23. TB HDSB 1994, 123.
[91] 13. TB HmbDSB 1994, 98.

5 Verfolgung von Sicherheitszwecken

Der Gesetzgeber hat den Funktionsumfang des AZR im sog. Sicherheitsbereich bewusst von Anfang an weit ausgestaltet.[92] Der historische Hintergrund hierzu ist das ursprüngliche Verständnis des Ausländerrechts als Sicherheitsrecht, nicht etwa als Niederlassungs- und Aufenthaltsrecht.[93] Durch die Speicherung von polizeilichen Fahndungsdaten und nachrichtendienstlichen Suchvermerken gerät noch heute jeder Kontakt von Ausländerinnen und Ausländern mit einer Ausländerbehörde zu einem Kontakt mit einer Außenstelle von Polizei und Nachrichtendiensten. Die Ausländerbehörden erfüllen insbesondere über das AZR eine **sicherheitsbehördliche Hilfsfunktion**.[94] Die Bundesregierung konnte 1995 auf Anfrage über die Wirksamkeit dieser Funktion des AZR keine Angaben machen; Ermittlungserfolge konnten nicht vermeldet werden.[95] Im Jahr 2020 betrug die Anzahl der AZR-Abfragen durch Polizeibehörden und durch Staatsanwaltschaften ca. 12,7 Mio. und hatte sich damit im Vergleich zu 2019 nahezu verdoppelt.[96] Bis heute besteht, soweit ersichtlich, keine Untersuchung, welcher Sicherheitsgewinn durch das AZR erreicht wird und worauf dieser beruht.

Sicherheitsbegründete Speicherungen erfolgen regelmäßig nicht nur im AZR, sondern parallel in weiteren spezifischen **Datenbanken von Sicherheitsbehörden**, insbesondere im polizeilichen Informationssystem (INPOL), im Nachrichtendienstlichen Informationssystem (NADIS) oder im System der Zollverwaltung INZOLL.[97] Es wurde bisher nicht dargelegt, dass und weshalb eine redundante AZR-Speicherung erforderlich sein soll. Teilweise erlangen Sicherheitsbehörden gemäß § 15 Abs. 1 AZRG über das AZR Zugriff auf von anderen Sicherheitsbehörden eingestellte Informationen, ohne dass es im Sicherheitsrecht entsprechende Zugriffe gibt.[98] Eine Erforderlichkeit solcher Zugriffe über den Umweg des Ausländerrechts ist nicht belegt.[99]

§ 15 Abs. 1 AZRG erlaubt Sicherheitsbehörden, **hoch sensible Daten** aus der Migrationsverwaltung für Sicherheitszwecke abzurufen oder abzufragen: finanzielle Leistungsfähigkeit, Religionszugehörigkeit (s.u. 8.2), Angaben über familiäre Bindungen und Bildungsstand, Angaben zur politischen Verfolgung. Die Übermittlung derartiger Daten zur Verfolgung jeglicher Straftaten und zur Abwehr jeglicher Gefahren, ja selbst zur „Verhütung“

[92] *Marx*, BT-PlProt. 12/233 S. 20387; 15. TB LfD Saar 1993/94, 31; vgl. *Streit* BewHi 1996, 232.
[93] *Weichert* in Huber, Vorb §§ 86-91e Rn. 9.
[94] *Bäumler* BewHi 1996, 245 f.; *Schriever-Steinberg* ZAR 1990, 65.
[95] BT-Drs. 13/2683, 4.
[96] GFF, Das Ausländerzentralregister, 2022, S. 8, BT-Drs. 19/32508, 6 ff.
[97] 2. TB SächsDSB 1994, 87; vgl. § 2 Rn. 9, 27; gegen die Verpolizeilichung des Ausländerrechts über das AZR *Weichert*, Bürgerrechte & Polizei [CILIP] Nr. 34 (3/1989), 70; allgemein dazu *Weichert* in *Heldmann*, AuslG, 2. Aufl., §§ 75–80, Rn. 7.
[98] *Streit/Heyder*, AZR-Gesetz, § 15 Rn. 7.
[99] *Frankenberg*, FS Simitis, S. 107 f.

oder „vorbeugenden Bekämpfung“ von Straftaten ohne eine Eingriffsschwelle verstößt offensichtlich in unverhältnismäßiger Weise gegen das Zweckbindungsprinzip.

Gemäß dem vom BVerfG entwickelten Kriterium der „**hypothetischen Datenneuerhebung**“ wäre es für die Rechtfertigung der Datenübermittlung nötig, dass damit Rechtsgüter von hervorgehobenem Gewicht geschützt werden sollen und dass zuvor zumindest ein konkreter Ermittlungsansatz gegeben ist.[100] Derartige Anforderungen werden von § 15 Abs. 1 AZRG bei Sicherheitsbehörden nicht gestellt, weshalb diese Regelungen gegen höherrangiges Recht verstoßen.[101] Entsprechendes gilt grundsätzlich auch für die Übermittlungsbefugnisse an das Zollkriminalamt, wenngleich hier nur enumerativ aufgeführte, wohl aber auch sensitive Daten weitergegeben werden dürfen (§ 17 AZRG).[102]

Bei der Bewertung des AZRG kann nicht auf ein – wie auch immer hergeleitetes – **Recht der Bevölkerung auf Sicherheit** zurückgegriffen werden.[103] Die Nutzung des AZR für Zwecke der Gefahrenabwehr, der Strafverfolgung und für nachrichtendienstliche Zwecke (Sicherheitszwecke) lässt sich von der Erfüllung ausländer- und asylrechtlicher Zwecke trennen. Das Ausländer- und Asylrecht zielt nicht auf die Abwehr wie auch immer gearteter Gefahren ab, sondern konzentriert sich auf die Regelung des Aufenthaltes und damit verbundene Befugnisse. Soweit mit einzelnen ausländer- und asylrechtlichen Regelungen auch Sicherheitszwecke verfolgt werden, ist nichts dagegen einzuwenden. Insofern kann eine beschränkte Speicherung in einer ausländer- und asylrechtlichen Datei erfolgen und eine spezifische Kommunikation stattfinden und unter Beachtung des Verhältnismäßigkeitsgrundsatzes eine Datenübermittlung von und an Sicherheitsbehörden gesetzlich erlaubt sein. Nicht zu rechtfertigen ist aber bei der partiellen Überschneidung von Aufenthalts- und Sicherheitsrecht die umfassende generelle Nutzung des AZR als Sicherheitsregister zu Nicht-Unionsbürgerinnen und -bürgern. Eine fremde Staatsangehörigkeit darf heute angesichts der Globalisierung der personalen Mobilität nicht mehr als Indiz für ein **Sicherheitsrisiko** angesehen werden.

5.1 Speicherung zum Zweck der Kriminalitätsbekämpfung

Gemäß § 2 Abs. 2 Nr. 7 und 7a AZRG werden Nichtdeutsche im AZR gespeichert „bei denen **tatsächliche Anhaltspunkte für den Verdacht** bestehen, dass sie im Geltungsbereich dieses Gesetzes Straftaten nach § 95 Abs. 1 Nr. 8 des Aufenthaltsgesetzes, nach § 30 Abs. 1 oder § 30a Abs. 1 des Betäubungsmittelgesetzes oder nach § 129 oder § 129a, jeweils auch in Verbindung mit § 129b Abs. 1, des Strafgesetzbuches oder mit terroristischer Zielsetzung andere Straftaten, insbesondere Straftaten der in § 129a des Strafgesetzbuches bezeichneten Art, planen, begehen oder begangen haben, oder die durch Straftaten mit terroristischer

[100] BVerfG 10.11.2020 – 1 BvR 3214/15, Rn. 99 f., 112, 117, EuGRZ 2021, 150 f.
[101] *Bäcker*, GFF-Gutachten, S. 41 f.
[102] *Bäcker*, GFF-Gutachten, S. 43.
[103] *Weichert*, Informationelle Selbstbestimmung und strafrechtliche Ermittlung, 1990, S. 32 ff.

Zielsetzung gefährdet sind," und „bei denen tatsächliche Anhaltspunkte für den Verdacht bestehen, dass sie eine Straftat nach § 89a oder § 89b des Strafgesetzbuchs begehen oder begangen haben". Die inzwischen mehrfach erweiterte Vorschrift war von Anfang an aus verfassungsrechtlichen Gründen umstritten.[104] Erkenntnisse über deren praktische Relevanz liegen nicht vor.[105]

Speichervoraussetzung sind **tatsächliche Anhaltspunkte für einen Verdacht**, dass die betroffene Person eine der aufgeführten Straftaten plant, begeht oder begangen hat. Der Begriff ist abzugrenzen von bloßen Vermutungen und „aus der Luft gegriffenen Annahmen".[106] Die Tatsachen müssen nicht auf eine nachgewiesene Straftat verweisen. Ein Anfangsverdacht genügt, aus dem sich die Möglichkeit der Tatbegehung durch den Beschuldigten ergibt.[107] Nach gängiger Rechtsprechung genügt für einen Anfangsverdacht schon eine schwache Tatsachengrundlage. Das Hintereinanderschalten von „Verdacht" und „Anhaltspunkte" wirkt kaum befugniseingrenzend. Das gilt umso mehr, als einige der in § 2 Abs. 2 Nr. 7 AZRG genannten Straftatbestände hinsichtlich ihrer unbestimmten Tatbestandsvoraussetzungen eine weite Anwendung zulassen.[108] Weder die Gesetzesmaterialien noch die Ausführungsbestimmungen geben Anhaltspunkte für eine eingrenzende Auslegung.[109]

Angeliefert werden die Daten zu den Straftatverdächten durch Polizei- und Grenzbehörden (§ 6 Abs. 1 Nr. 2, 4 AZRG). Angesichts des erwähnten weiten Anwendungsbereichs werden Sachverhalte erfasst, die keinerlei Bezug zum Aufenthaltsrecht aufweisen. Tatsächlich stehen diese Daten dann aber im umfassenden **Zugriff für folgende Stellen**: sämtliche Asyl- und Ausländerbehörden, Polizeibehörden, Staatsanwaltschaften (§ 15 AZRG), Gerichte (§ 16 Abs. 2 Nr. 4 AZRG), die Zentralstelle für Finanztransaktionsuntersuchungen (§ 17a Nr. 7 AZRG) Nachrichtendienste (§ 20 AZRG) und Auswärtiges Amt einschließlich deutscher Auslandsvertretungen (§ 21 AZRG). Im Bedarfsfall können diese Daten direkt von allen der genannten Stellen online, d.h. automatisiert im AZR abgerufen werden (§ 22 AZRG).[110] Die abgerufenen Daten dienen nicht nur der Informationsanbahnung oder der Abschätzung von Verdachts- und Gefahrenlagen im Vorfeld von Ermittlungen,[111] sondern auch operativen Zwecken.[112]

[104] *Weichert*, InfAuslR 1989, 3; Änderungsantrag der SPD-Fraktion, BT-Drs. 12/7898, 1.
[105] *Weichert* in GK-AufenthG, § 2 AZRG Rn. 62.
[106] BVerfG 27.07.2005 – 1 BvR 668/04, Rn. 126 f. = BVerfGE 113, 348, 387 = NJW 2005, 2603, 2608 ff., *Graulich* in *Bäcker/Denninger/Graulich*, Handbuch des Polizeirechts, 6. Aufl. 2018, Kap. E. Rn. 149.
[107] BVerfG 29.10.2013 – 2 BvR 389/13, Rn. 16, StV 2014, 388; Überblick bei *Eisenberg/Conen*, NJW 1998, S. 2241, 2244 f.
[108] *Bäcker*, GFF-Gutachten, 2022, S. 24 f.; zu § 129a StGB vgl. z. B. BGH 28.11.2007 – StB 43/07, NJW 2008, S. 86, 88 f.
[109] BT-Drs. 12/6938, 18; Tz. 2.2 .4.1 AZR-VV, dazu *Weichert* in GK-AufenthG, § 2 AZRG Rn. 67 ff.
[110] Siehe die Abrufzahlen von 2019 bis Juli 2021 in BT-Drs. 19/32508, 6 f.; kritisch *Frankenberg*, FS Simitis, S. 109.
[111] Zur Antiterrordatei BVerfG 24.04.2013 – 1 BvR 1215/07, Rn. 105 ff., NJW 2013, 1502 f.; BVerfG 10.11.2020 – 1 BvR 3214/15, Rn. 110, EuGRZ 2021, 151.
[112] *Bäcker*, GFF-Gutachten, 2022, S. 25.

Da weder die Daten eingebenden Stellen noch die abrufenden Stellen einen Bezug zum Aufenthaltsrecht haben müssen, wird das AZR als weitgehend **vom ursprünglichen Zweck losgelöste Datenverteilstelle** genutzt, über die reine Verdachtsdaten selbst für administrative Vorfeldzwecke (Nachrichtendienste) verwendet werden können. Gemäß § 11 Abs. 1 S. 1 AZRG darf die empfangende Stelle die Angaben zum Straftatverdacht „nur zu dem Zweck verwenden, zu dem sie ihr übermittelt worden sind“. Vorkehrungen, dass dies gewährleistet ist, sind nicht vorgesehen. Notwendig wären insofern zumindest eine Pflicht zur entsprechenden Markierung dieser Datenverarbeitung sowie stichprobenweise Kontrollen. Prozedurale Regelungen zur Genehmigung sind auch nicht vorgesehen. Die Betroffenen werden nicht eingebunden, so dass diese Art der Verarbeitung regelmäßig völlig hinter dem Rücken der Betroffenen erfolgt. Derartige Transaktionen sind ein unverhältnismäßiger Eingriff in deren Recht auf Datenschutz.[113]

5.2 Gruppenauskunft (Rasterfahndung)

§ 12 Abs. 1 Nr. 2 AZRG erlaubt die Übermittlung von Daten einer Mehrzahl von nicht namentlich genannten Drittausländern auf Grund von im AZR gespeicherten Merkmalen an die in §§ 15-17 und 20 AZRG genannten Behörden. Diese „Gruppenauskunft“ ist „zulässig, soweit sie erforderlich und angemessen ist a) zur Abwehr von Gefahren für die öffentliche Sicherheit, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für die freiheitliche demokratische Grundordnung oder b) zur Verfolgung eines Verbrechens oder einer anderen erheblichen Straftat, von der auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass sie gewerbs- oder gewohnheitsmäßig, von einem Bandenmitglied oder in anderer Weise organisiert begangen wird, und die Daten auf andere Weise nicht, nur mit unverhältnismäßigem Aufwand oder nicht rechtzeitig erlangt werden können“. Zulässig ist sie auch für den Bundesnachrichtendienst, wenn sie „unter den in § 2 Abs. 1 Nr. 4 des BND-Gesetzes genannten Voraussetzungen erforderlich ist, um im Ausland Gefahren der in § 5 Abs. 1 Satz 3 des Artikel-10-Gesetzes genannten Art rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen“ (§ 12 Abs. 1 Nr. 3 AZRG). Neben den Ausländer- und Asylbehörden kann die Gruppenauskunft von allen Sicherheitsbehörden (also Polizeien, Staatsanwaltschaften, Nachrichtendienste) erlangt werden. Im Sicherheitsrecht wird diese Gruppenauskunft „**Rasterfahndung**“ genannt.

Das Instrument der Gruppenanfragen ist durch die Sicherheitsbehörden in den vergangenen Jahren **vermehrt genutzt** worden. In den Jahren 2018, 2019 und 2020 wurden drei Gruppenauskünfte an das BKA erteilt, drei Gruppenauskünfte an die Bundespolizei und eine Gruppenauskunft an den BND. Zwei Anträge des BKA waren im Jahr 2018 abgelehnt worden.

[113] *Bäcker*, GFF-Gutachten, 2022, S. 3.

Noch in den Jahren 2014, 2015 und 2016 waren keine Gruppenauskünfte durch die genannten Behörden angefordert worden.[114]

Es gelten folgende **Rahmenbedingungen**: „Das Ersuchen ist schriftlich zu stellen, zu begründen und bedarf der Zustimmung des Leiters der ersuchenden Behörde oder eines von ihm für solche Zustimmungen bestellten Vertreters in leitender Stellung“ (§ 12 Abs. 3 AZRG). Nachträglich sind die zuständigen Datenschutzaufsichtsbehörden zu informieren (§ 12 Abs. 4 AZRG). § 11 Abs. 1 S. 1 AZRG sieht vor, dass die empfangene Stelle von Gruppenauskunftsdaten diese „nur zu dem Zweck verwenden (darf), zu dem sie ihr übermittelt worden ist“.

Bei der sicherheitsbehördlichen Gruppenauskunft handelt es sich um einen verdachtslosen informationellen Eingriff. Die Gruppenauskunft zielt darauf ab, Erkenntnisse über einen Verdacht bzw. Verdächtige zu gewinnen (**Verdachtsgewinnungseingriff**). Wegen der Schwere des damit verbundenen Grundrechtseingriffs ist es nötig, dass damit der Schutz hochrangiger Rechtsgüter bei Vorliegen einer konkreten Gefahr verfolgt wird, wobei es sich hierbei um eine Dauergefahr handeln kann. Eine präventive polizeiliche Rasterfahndung ist nur zulässig, wenn die konkrete Gefahr für so hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist. Eine Rasterfahndung im Vorfeld scheidet dagegen aus.[115] § 12 AZRG differenziert nicht bzgl. der bei der erlaubten Gruppenauskunft einbezogenen Merkmale. Das AZR enthält u.a. Daten von hoher persönlichkeitsrechtlicher Relevanz, etwa Angaben über die Religionszugehörigkeit[116], über die Gesundheit, über politische Meinungen. Je mehr derartige Daten in einer Gruppenauskunft einbezogen werden, desto erheblicher ist der damit verbundene Grundrechtseingriff. Die Eingriffsschwere ist auch davon abhängig, welche Folgemaßnahmen die Betroffenen, etwa in Form von unberechtigten Verdächtigungen oder Stigmatisierungen, befürchten müssen.[117]

§ 98a StPO erlaubt einen Datenabgleich von verschiedenen öffentlichen und privaten Stellen. § 12 AZRG zeichnet sich dadurch aus, dass das Zusammenführen von **Daten aus vielen Verwaltungsbereichen** schon im AZR erfolgt ist. Die Daten sind so aufbereitet, dass eine Abfrage bei weiteren Stellen oft nicht erforderlich ist. Die Hemmschwelle für die Durchführung von Abgleichen ist sehr niedrig. Die Gruppenauskunft aus dem AZR-Datenbestand kann mit sicherheitsbehördlichen Rasterfahndungsmaßnahmen kombiniert werden.

[114] GFF, Das Ausländerzentralregister, 2022, S. 8 f. mit Hinweisen auf die Praxis; BT-Drs. 18/18585, 2 f.; BT-Drs. 32508, 9.
[115] BVerfG 04 04.2006 – 1 BvR 518/02, Rn. 118 f., 133, 146; NJW 2006, 1939 ff. = JZ 2006, 906 = RDV 2006, 158 = MMR 2006, 531 = DVBl 2006, 899 = DÖV 2006, 967.
[116] Kritisch dazu *Bäcker*, GFF-Gutachten, 2022, S. 3.
[117] BVerfG 04 04.2006 – 1 BvR 518/02, Rn. 94, 99-102, 108.

Anders als z.B. die Strafprozessordnung (StPO) sieht § 12 AZRG nur geringe verfahrensrechtlichen Grundrechtssicherungen vor. So besteht z.B. kein Richtervorbehalt (vgl. § 98b StPO). Die Gruppenauskünfte nach § 12 Abs. 1 Nr. 2 und Nr. 3 führen zwangsläufig dazu, dass Daten von Personen übermittelt werden, die die gleichen Merkmale aufweisen wie die Person bzw. die Personen, um die es der ersuchenden Stelle letztlich geht, die aber mit dem Ausschreibungsanlass überhaupt nichts zu tun haben. Die Eingriffe haben eine große Streubreite. Hiervon kann ein hoher Einschüchterungseffekt ausgehen.[118] Man muss daher davon ausgehen, dass die sicherheitsbehördliche Gruppenauskunft einen **unverhältnismäßigen Eingriff** in die Rechte ausländischer Betroffener darstellt.[119]

5.3 Sicherheitsbehördliche Suchvermerke

Die in § 20 Abs. 1 AZRG bezeichneten Stellen, also alle bundesdeutschen **Nachrichtendienste** (Verfassungsschutzbehörden des Bundes und der Länder – BfV und LfV, Militärischer Abschirmdienst – MAD, Bundesnachrichtendienst – BND), sowie das **Bundeskriminalamt** (BKA) können nach § 5 Abs. 2 AZRG Suchvermerke im AZR zur Feststellung anderer Sachverhalte als den Aufenthalt speichern lassen.

Der Begriff „**Feststellung anderer Sachverhalte**“ ist uferlos. Dieses „nicht mehr überschaubare Instrument nachrichtendienstlicher Informationsbeschaffung“ stand von Anfang an in der Kritik.[120] Der Gesetzgeber verzichtete durch die Formulierung ausdrücklich darauf, die verfolgbaren Zwecke festzulegen, obwohl dies möglich gewesen wäre, z.B. durch Definition besonderer Bedrohungslagen und der für deren Bekämpfung nötigen Merkmale. Effektiv eingrenzende Verfahrensvorschriften sind nicht vorgesehen, selbst eine nachträgliche Benachrichtigung der Betroffenen nicht. Die grundsätzliche Sichtbarkeit des Suchvermerks für andere öffentliche Stellen (§ 5 Abs. 5 S. 2 AZRG) stellt eine zusätzliche Belastung für Betroffene dar.

Die über den Suchvermerk vermittelte Information kann sich auf jeden im AZR verfügbaren Sachverhalt beziehen. Durch die Aufgabenstellung der Sicherheitsbehörden erfolgt keine erkennbare Eingrenzung. Besonders problematisch ist dies bei den im Vorfeld von Gefahren und Straftaten agierenden Nachrichtendiensten. Die Einschränkung der Suche darauf, dass die Information nicht über allgemein zugänglichen Quellen oder durch eine weniger belastende Maßnahme erhoben werden kann, orientiert sich eher an behördlichen Effektivitätserwägungen. Sie gewährleistet **keine wirksame Verhältnismäßigkeitsprüfung**.[121]

Die Regelung, dass die ersuchende Stelle Aufzeichnungen über das Ersuchen, den Zweck und die rechtlichen Voraussetzungen aufzeichnen müssen (§ 5 Abs. 4 AZRG) ermöglichen allenfalls

[118] BVerfG 04.04.2006 – 1 BvR 518/02, Rn. 117.
[119] *Frankenberg*, FS Simitis, S. 108 f.; *Bäcker*, GFF-Gutachten, 2022, S. 44 f.
[120] Bundesrat: BT-Drs. 12/7520, Nr. 12 S. 6, siehe ebenso *Bäumler* NVwZ 1995, 245; *Schriever-Steinberg* NJW 1994, 3277; *Weichert* InfAuslR 1989, 1, 3.
[121] *Weichert* in GK-AufenthG, § 5 AZRG, Rn. 12 f.; *Bäcker*, GFF-Gutachten, 2022, S. 25 f.

eine nachträgliche Kontrolle und sind angesichts der Praxis nicht oder äußerst selten erfolgender Datenschutzkontrollen ohne erkennbare Wirkung. Die Speicherbefristung des Suchvermerks auf zwei Jahre (§ 5 Abs. 5 S. 1 AZRG) hat **keine wirksame Schutzfunktion**.

Das BVerfG hat festgestellt, dass mit einer Datenverarbeitung nicht „tendenziell **unvereinbare Zwecke**“ verfolgt werden dürfen.[122] Polizeiliche und nachrichtendienstliche Nutzungen sind mit ausländerrechtlichen Nutzungen zumeist dann nicht in Einklang zu bringen, wenn hierbei soziale Ziele, z.B. die Integration der Menschen oder die Familienzusammenführung, verfolgt werden[123] oder wenn ein Patienten- oder Sozialgeheimnis übermittelt wird. Hierin liegt dann zusätzlich ein unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen.[124]

5.4 Verwendung von Fingerabdrücken und Lichtbildern

Gemäß § 3 Abs. 1 Nr. 5a AZRG wird von jedem Nicht-Unionsbürger im AZR ein Lichtbild gespeichert. Von jedem Flüchtling werden zusätzlich die Abdrücke aller 10 Finger verfügbar gemacht (§ 3 Abs: 2 Nr. 1 AZRG). Die Erfassung der Merkmale erfolgt bei Flüchtlingen gemäß § 16 Abs. 1 S. 1 AsylG. Bei Lichtbildern und Fingerabdrücken handelt es sich um **biometrische Daten** zur eindeutigen Identifizierung einer natürlichen Person (Art. 4 Nr. 14 DSGVO), die nach Art. 9 Abs. 1 DSGVO als besonders sensitiv eingestuft sind.

Die Speicherung von **Lichtbildern** war im AZR zunächst nicht vorgesehen. Ab 2002 werden Lichtbilder, also Fotos des Gesichts, in der Visa-Datei gespeichert (§ 29 Abs. 1 Nr. 4 AZRG). Die Speicherung im allgemeinen Datenbestand wurde mit Gesetz vom 19.8.2007 eingeführt.[125] Mit Gesetz vom 20.12.2012 wurde die Speicherung des Lichtbilds von Unionsbürgern ausgeschlossen (§ 3 Abs. 4 AZRG). Das Lichtbild soll die Identitätsfeststellung bei abfragenden Stellen, die einen direkten Kontakt zum Ausländer haben, erleichtern. Voraussetzung für die Erteilung eines Aufenthaltstitels ist die eindeutige Identifizierung (§ 5 Abs. 1 Nr. 1a AufenthG). Das Lichtbild wird vom Gesetzgeber als ein zuverlässiges, weil wenig veränderliches Datum angesehen.[126] Es eignet sich auch zur Überprüfung von Dokumenten, die ein Lichtbild enthalten. Im AZR gespeicherte Lichtbilder können inzwischen mit technischen Mustererkennungsverfahren automatisiert ausgewertet werden.

Die Identifizierung durch ein Lichtbild ist aus **persönlichkeitsrechtlicher Sicht** riskant: Das Gesicht ist in der Öffentlichkeit leicht erfassbar. Mit Hilfe von Gesichtserkennungssystemen lassen sich Lichtbilder automatisiert über Bilddatenbanken abgleichen und zuordnen.[127]

[122] BVerfG 15.12.1983 – 1 BvR 209/83 u.a., Rn. 195, NJW 1984, 426; 14. TB LfD SH 1991–92, 32.
[123] XII. TB LfD Nds. 1993/94, 109.
[124] *Weichert* Bürgerrechte & Polizei [CILIP] Nr. 34 [3/1989], 70.
[125] BGBl. I S. 1970.
[126] *Streit* ZAR 2002, 239 f.
[127] *Petri* in *Simitis/Hornung/Spiecker*, Art. 4 Nr. 14 Rn. 8; *Weichert*, Staatliche Identifizierung, www.netzwerk-datenschutzexpertise.de 08.03.2021, S. 21; *ders*. DANA 1/2021, 11 f., 17; *ders.* DVBl 2021, 1067 f.

Derartige Bilddatenbanken sind als Grundlage für Bildauswertungen im Internet weltweit verfügbar. Lichtbilder werden so zu einem Mosaikstein bei der Rundumüberwachung, und zwar sowohl im öffentlichen Raum als auch in geschlossenen Räumen. Und hierfür werden sie in Überwachungsstaaten auch verwendet.[128] Als Konsequenz kann so ein starker Überwachungsdruck auf die Betroffenen entstehen. Dass es wegen einer weiterhin hohen Fehlerrate bei der automatisierten Bilderkennung immer wieder zu falschen Zuordnungen kommt,[129] ändert nichts an diesem Druck.

Die in § 3 Abs. 2 Nr. 1 u. 2 AZRG genannten **Fingerabdruckdaten** werden im Rahmen der erkennungsdienstlichen Behandlung erhoben und sollen zur Identifizierung auch in späteren Verfahren genutzt werden können. Fingerabdruckdaten haben eine zentrale Identifizierungsfunktion im Ausländerrecht (§ 49 Abs. 1 S. 3 AufenthG, § 16 Abs. 1 S. 1 AsylG). Fingerabdrücke werden europaweit zur eindeutigen Identitätszuordnung genutzt.[130] Bei der ausländerrechtlichen Identifizierung werden grundsätzlich die Fingerabdrücke sämtlicher Finger beider Hände erfasst (Art. 2 Abs. 1 lit. k Eurodac-VO, § 16 Abs. 1 S. 2 AsylG). Sie werden als ein wichtiges Instrument im Bereich der Strafverfolgung eingesetzt, um Tatortspuren Tatverdächtigen zuzuordnen (§ 81b StPO).

Gemäß § 10 Abs. 2 S. 2 AZRG genügen bei „Zweifeln an der Identität des Ausländers“ das Lichtbild oder die Fingerabdruckdaten, um ein **Auskunftsersuchen beim AZR** durchzuführen. Die Berechtigung zur AZR-Datenabfrage haben die Asyl- und Ausländerbehörden sowie die Sicherheitsbehörden einschließlich der Nachrichtendienste (§§ 15, 17, 20 AZRG), die diese Daten auch im automatisierten Verfahren abrufen können (§ 22 AZRG). Gemäß der Regelung des § 5 AZRG ist es den genannten öffentlichen Stellen „zur Erfüllung ihrer Aufgaben“ erlaubt, einen Suchvermerk zur Feststellung des Aufenthaltsortes im AZR zu speichern, wobei das Gesetz es nicht ausschließt, dass dieser Suchvermerk ausschließlich mit dem Fingerabdruck oder dem Lichtbild erfolgt. Sicherheitsbehörden können auf dieser Grundlage auch nach „anderen Sachverhalten“ fahnden (§ 5 Abs. 2 AZRG).

Den Sicherheitsbehörden wird mit den Fingerabdrücken und den Lichtbildern ein umfassendes Fahndungsinstrument in die Hand gegeben, das ursprünglich zur eindeutigen aufenthaltsrechtlichen Identifizierung erhoben wird. Dadurch, dass entgegen der Erforderlichkeit für Identifizierungszwecke alle 10 Finger erfasst werden, besteht eine ideale Abgleichsgrundlage für Tatortspuren im Rahmen der Kriminalitätsbekämpfung. Die biometrischen Merkmale der Betroffenen finden sich nicht nur im AZR, sondern in weiteren Datenbanken, so die Fingerabdrücke z.B. in AFIS und Eurodac, Gesichtsbilder in Ausweisdatenbanken sowie beim BKA.[131] Während Fingerabdrücke bei Eurodac nur zur Verhütung, Aufdeckung oder Untersuchung einer terroristischen oder sonstigen schweren

[128] DANA 1/2020, 68 f. DANA 2/2020, 125 f.
[129] *Wedde* in *Däubler u.a.*, Art. 9 Rn. 32.
[130] Eurodac-VO v. 26.06.2013, Nr. 603/2013, ABl. v. 29.06.2013, L 180/1.
[131] *Weichert* DVBl 2021, 1068.

Straftat genutzt werden dürfen (Art. 5 Abs. 1 Eurodac-VO), gibt es für die biometrischen AZR-Daten keine derartige materiell-rechtliche Beschränkung.

Es bestehen auch keine prozeduralen Schranken gegen die umfassende Verfügbarkeit der biometrischen Identifizierungsdaten für Sicherheitszwecke im AZR. Nicht-EU-Ausländer und Flüchtlinge sind grundsätzlich kein größeres, polizeilich oder geheimdienstlich zu behandelndes, Sicherheitsrisiko als EU-Staatsbürger. Es mag zwar gerechtfertigt sein, dass Sicherheitsbehörden aus aufenthaltsrechtlichen Gründen erfasste biometrische Daten verarbeiten, soweit sie aufenthaltsrechtliche Aufgaben wahrnehmen. Dies legitimiert aber nicht die undifferenzierte Nutzung solcher Daten für generelle Zwecke der Gefahrenabwehr und der Strafverfolgung, selbst wenn sich diese Daten hierfür gut eignen. Im Ergebnis führt die ungenügende Nutzungsbegrenzung zu einer **Zweckunvereinbarkeit**: Die Freiheitsversprechen der GRCh und des GG gelten auch für Nicht-EU-Ausländer. Die Verfügbarkeit biometrischer Identifizierungsdaten für Sicherheitsbehörden erhöht die Gefahr, im Rahmen der Wahrnehmung von Freiheitsrechten erfasst und kontrolliert zu werden und trägt dazu bei, dass aus Angst hiervon auf Freiheitsbetätigungen verzichtet wird.[132]

5.5 Nachrichtendienstliche Nutzung

AZR-Daten von Nicht-EU-Bürgern dürfen gemäß § 20 Abs. 1 S. 1 AZRG an die Verfassungsschutzbehörden des Bundes und der Länder (BfV, LfV), den Militärischen Abschirmdienst (MAD) und den Bundesnachrichtendienst (BND) übermittelt werden, soweit diese „zur Erfüllung der ihnen durch Gesetz übertragenen Aufgaben erforderlich sind, sofern sie nicht aus allgemein zugänglichen Quellen, nur mit übermäßigem Aufwand oder nur durch eine die betroffene Person stärker belastende Maßnahme erhoben werden können“. Das BfV, die LfV, der MAD und der BND werden unter dem Begriff **Nachrichtendienste** zusammengefasst. Diese Stellen zeichnen sich dadurch aus, dass ihnen zwar keine exekutiven Befugnisse zustehen, dass sie aber für die von ihnen zu erfüllenden Aufgaben verdeckt und im Vorfeld von Gefahren oder möglichen Straftaten personenbezogene Daten erheben dürfen und dass sie einer besonderen Geheimhaltung unterliegen. Der Zugriff der Nachrichtendienste auf AZR-Daten wurde sowohl aus rechtspolitischer wie auch aus verfassungsrechtlicher Sicht von Anfang an kritisiert.[133] Dieser Zugriff erstreckte sich zunächst auf alle Nichtdeutschen. Mit G. v. 20.12.2012 wurden wegen der damit verbundenen Diskriminierung von freizügigkeitsberechtigten Unionsbürgern gegenüber Deutschen die Unionsbürger aus der Regelung herausgenommen, da die Nutzung dieser Daten in den dort genannten Fällen nicht zur Durchführung ausländer- oder asylrechtlicher Aufgaben erfolgt.[134]

§ 20 Abs. 1 AZRG macht die Datenübermittlung an Nachrichtendienste vorrangig davon abhängig, ob die Daten zu deren Aufgabenerfüllung nötig sind. Die Regelung, die seit dem

[132] BVerfG 15.12.983 – 1 BvR 209/83, Rn. 94, NJW 1984, 422.
[133] *Weichert* InfAuslR 1987, 213 f.; *ders.* InfAuslR 1989, 6.
[134] BR-Drs. 512/12, 15.

ersten Inkrafttreten des AZRG unverändert geblieben ist, berücksichtigt nicht die inzwischen ergangene Rechtsprechung des BVerfG zur Datenbeschaffung durch Nachrichtendienste. Demgemäß müssen in Rechtsgrundlagen die Voraussetzungen für die Verarbeitung umso enger begrenzt werden, je schwerer die Eingriffe der Ersterhebung und der weiteren Nutzung wiegen. Anlass, Zweck, Umfang und Voraussetzung der Eingriffe müssen **bereichsspezifisch bestimmt und normenklar** geregelt werden.[135]

Gemäß dem sog. **informationellen Trennungsprinzip** gilt, dass operative Polizei- und Verwaltungstätigkeit grundsätzlich von der Tätigkeit der Nachrichtendienste zu trennen ist.[136] Danach dürfen Daten zwischen Nachrichtendiensten und Vollzugsbehörden grundsätzlich nicht ausgetauscht werden. Einschränkungen der Datentrennung und damit ein Datenaustausch sind nur ausnahmsweise zulässig. Es bedarf hinreichend konkreter qualifizierter Eingriffsschwellen und Vorkehrungen.[137] Erfolgt eine informationelle Verflechtung zwischen Nachrichtendiensten und Vollzugsbehörden, so besteht u.a. die Gefahr, dass Nachrichtendienste Zugang zu Informationen erhalten, die nicht für ihre Zwecke bestimmt sind. Dabei ist besonders zu berücksichtigen, dass die nachrichtendienstlichen Vorschriften äußerst allgemein formuliert sind, was eine übermäßige Neigung zur Datenspeicherung und eine eingeschränkte Kontrollmöglichkeit zur Folge hat.[138] Die Tätigkeit von Nachrichtendiensten können für die Betroffenen gravierende Konsequenzen haben, etwa bei Stellenbewerbungen und, in Bezug auf Ausländer, insbesondere durch Datenübermittlungen an Sicherheitsbehörden in Drittländern.

Bei Datenübermittlungen zwischen öffentlichen Stellen ist generell der **Grundsatz der hypothetischen Neuerhebung** anzuwenden. Zulässig sind demnach nur solche Datenerhebungen aus dem AZR, die nach verfassungsrechtlichen Maßstäben auch für den geänderten Zweck erhoben werden dürften. Die nachrichtendienstliche Nutzung der ARZ-Daten muss gegenüber der ursprünglichen Verwendung gleichwertig sein, wobei wegen der gesteigerten Belastungswirkung durch die erhebliche persönlichkeitsrechtliche Relevanz auch gesteigerte Anforderungen gelten. Eingriffsschwellen müssen hinreichend gesetzlich konkretisiert werden.[139] Diesen Anforderungen genügt § 20 AZRG nicht: Er ermöglicht einen praktisch unbeschränkten Zugriff der Geheimdienste auf AZR-Daten zur Aufgabenerfüllung, ohne dass verlässlich geprüft wird, ob der Zweck der Ersterhebung der Daten auch die Verwendung durch geheimdienstliche Stellen rechtfertigt. Ob der Nachrichtendienst die Daten hätte direkt erheben dürfen, wird nicht geprüft. Die Eingriffstiefe ist angesichts der

[135] BVerfG 10.11.2020 – 1 BvR 3214/15, Rn. 98 m.w.N., NJW 2021, 690 = EuGRZ 2021, 150; *Bäcker*, GFF-Gutachten, S. 43 f.
[136] BVerfG 10.11.2020 – 1 BvR 3214/15, Rn. 101 ff.
[137] BVerfG 24.3.2013 – 1 BvR 1215/07, Rn. 123, NJW 2013, 1505; BVerfG 10.11.2020 – 1 BvR 3214/15, Rn. 101 ff., NJW 2021, 690.
[138] BfDI, Stellungnahme 2. DAVG, 8 f.; kritisch schon 15. TB BfD 1993/93 [BT-Drs. 13/1150], 18; *Denninger* KritV 1994, 236 f.; *Gusy* ZRP 1987, 48 ff.
[139] BVerfG 10.11.2020 – 1 BvR 3214/15, Rn. 99 f., 112, 117, EuGRZ 2021, 150 f.; *Bäcker*, GFF-Gutachten, 2022, S. 35 f.

teilweise hohen Sensitivität bzgl. der AZR-Daten sehr unterschiedlich, weshalb gesetzlich ein Prozessschritt vorgesehen werden müsste, bei dem die Verhältnismäßigkeit der konkreten Übermittlung und die hypothetische Direkterhebungsbefugnis durch eine unvoreingenommene Stelle geprüft und bestätigt wird.

Die Übermittlung von AZR-Daten an Nachrichtendienste setzt voraus, dass die vom AZR zu übermittelnden Daten nicht aus allgemein zugänglichen Quellen, nur mit übermäßigem Aufwand oder nur durch eine den Betroffenen **stärker belastende Maßnahme** erhoben werden können. Diese Regelung entspricht § 18 Abs. 3 S. 1 BVerfSchG und gilt für alle Formen der Datenbeschaffung durch Nachrichtendienste des Bundes (§ 10 Abs. 2 MADG, § 8 Abs. 3 S. 1 BNDG). Sie stellt, gerade in hoch invasiven informationellen Bereichen, keine wirksame Einschränkung dar. Die Regelung lässt offen, wann eine weniger belastende Eingriffsmaßnahme angenommen werden kann. Die in § 20 Abs.1 S. 1 AZRG vorgesehenen Einschränkungen stellen weder eine wirksame materielle noch eine prozessuale Hürde dar.

Nach § 20 Abs. 2 AZRG haben die Nachrichtendienste **Aufzeichnungen** über das Ersuchen, den Zweck und die weiteren Übermittlungsvoraussetzungen (§ 20 Abs. 1 S. 1 AZRG) zu führen. § 13 Abs. 3 AZRG regelt, dass Abrufe der Nachrichtendienste ausschließlich von diesen entsprechend § 6 Abs. 3 S. 2 bis 5 BVerfSchG zu protokollieren sind. Die 2019 eingeführte Regelung soll dem Geheimhaltungsbedarf der Nachrichtendienste Rechnung tragen. Angesichts der kumulierten Zusammenführung von Personendaten bei den Nachrichtendiensten (und dem damit eingeschlossenen Schadenpotenzial bei unberechtigtem Informationszugang) sei es, so die Gesetzesbegründung, geboten, diese Protokolldaten als Verschlusssache höher als „Nur für den Dienstgebrauch“ einzustufen, was umfassende Schutzanforderung im AZR mit massiven Kostenfolgen nach sich ziehen würde, ggf. mit Performanceeinschränkungen durch andere Bedarfsträger. Eine Kontrolle der Abrufe erfolge sachgerecht im Zusammenhang mit der Kontrolle der abrufenden Stelle, was durch die dortige Protokollierung unterstützt werde.[140]

§ 13 Abs. 3 AZRG hat zur Folge, dass das weiterhin für die Übermittlung mitverantwortliche BAMF als AZR-Behörde **keine Zulässigkeitskontrolle** durchführen kann und dass generell die Prüfung der Zulässigkeit der Abrufe massiv erschwert wird. Hacker, denen es gelingt, unerkannt mit den Zugangsmöglichkeiten der Nachrichtendienste Daten aus dem AZR abzurufen, profitieren ebenfalls von dieser Intransparenz und werden kaum entdeckt. Die Begründung für die Regelung, nämlich die „Vermeidung von Doppelaufwänden“, ist vorgeschoben, da fachgerechte Protokollierungen automatisiert erfolgen können und die damit verbundene Speicherung keinen zusätzlichen menschlichen Aufwand erfordert. Die Begründung ignoriert mit ihrem Hinweis auf die Geheimhaltungsbedürftigkeit der Protokolldaten den Umstand, dass Protokolldaten durch eine enge Zweckbindung ohnehin einer spezifischen Geheimhaltung unterliegen (vgl. § 37 Abs. 1 S. 1 Nr. 2 AZRG). Von

[140] BT-Drs. 19/8752, 55.

„massiven Kostenfolgen“, selbst bei einer gesondert abgeschotteten Protokollierung, kann keine Rede sein.[141] Erheblich höhere Kosten entstehen, wenn wegen unerkannt unzulässigen Datenabfragen nachträglich umfangreiche Untersuchungen durchgeführt und Schäden ausgeglichen werden müssen. Die Spaltung der Abfragedokumentation ist sach- und rechtswidrig.[142]

Das informationelle Trennungsprinzip gilt vor allem für die Möglichkeit des **Online-Datenabrufes** (§ 22 Abs. 1 Nr. 9 AZRG). Die Eingriffstiefe der vorangegangenen Datenverarbeitung und die der geplanten Nutzung werden beim Online-Abruf nicht überprüft. Die Zulässigkeitsprüfung des Datenabrufs beschränkt darauf, ob die Stelle generell zum Datenempfang berechtigt ist (§ 22 Abs. 1 S. 2 AZRG). Die Zulassung von **AZR-Online-Abfragen für die Nachrichtendienste** war schon anlässlich der ersten Gesetzgebung in den 90er Jahren Anlass zur Kritik.[143] Für die damit verbundene partielle Aufhebung des Trennungsprinzips sind konkrete qualifizierte Eingriffsschwellen und weitere technisch-organisatorisch und prozedurale Vorkehrungen nötig. Die Online-Zugriffsmöglichkeit der Nachrichtendienste beeinträchtigt massiv die Vertraulichkeit beim AZR speziell und beim BAMF generell, ohne dass kompensierende Schutzvorkehrungen bestehen.[144] Durch die Verweigerung von statistischen Angaben zur nachrichtendienstlichen Online-Nutzung des AZR ist selbst im Ansatz eine öffentliche Kontrolle unmöglich.[145]

Dieser Beeinträchtigung der Interessen der Betroffenen steht kein gesicherter, ins Gewicht fallender **Nutzen im Bereich der Sicherheit** gegenüber.[146] § 22 Abs. 2 AZRG macht die automatisierte Abfrage durch Nachrichtendienste von der Häufigkeit der Übermittlungsersuchen oder der Eilbedürftigkeit ab. Es ist kaum begründbar, weshalb die Nachrichtendienste statt der Vornahme von Einzelanfragen auf einen Online-Zugriff angewiesen sein sollen. Ein nachrichtendienstlicher Informationsbedarf wird kaum durch Massendatenabfragen zu bedienen sein. Nötig ist vielmehr eine Erforderlichkeitsprüfung im Einzelfall, nicht nur, wie in § 22 Abs. 1 S. 2 AZRG vorgesehen, eine generelle Zulassung durch die obersten Bundes- und Landesbehörden. Die Dienste haben auch keine Befugnis, in Eilfällen gefahrenabwehrend tätig zu werden, weshalb eine Eilbedürftigkeit regelmäßig nicht zu begründen ist. Eine Erforderlichkeits- und Angemessenheitsprüfung ist nicht gewährleistet. Eine Abwägung mit den Betroffeneninteressen erfolgt nicht; die Betroffenen werden nicht beteiligt und auch nicht nachträglich informiert. Mit dem uneingeschränkten Direktzugriff auf sämtliche im AZR gespeicherten Verwaltungsdaten einschließlich der Angaben über

[141] Netzwerk Datenschutzexpertise, Stellungnahme 2. DAVG, 6.
[142] *Bäcker*, GFF-Gutachten, S. 44.
[143] *Frankenberg*, FS Simitis, S. 109 f.; weitere Nachweise bei *Weichert*, AZRG, § 22 Rn. 22.
[144] Kritisch dazu *Jelpke* u.a., BT-Drs. 32112, 1 f.
[145] BReg BT-Drs. 32508, 9.
[146] BVerfG 05.07.1995 – 1 BvR 2226/94, BVerfGE 93, 187 = NStZ 1995, 503.

Asylverfahren, über die Gesundheit oder zu Sozialdaten wird „tendenziell Unvereinbares“ zusammengefügt, was gegen das Trennungsgebot verstößt.[147]

6 Gesetzliche Bestimmtheit

Das aus dem Rechtsstaatsgebot abgeleitete Prinzip der Normbestimmtheit soll den Betroffenen Rechtssicherheit bei der Normanwendung vermitteln. Die Normbestimmtheit ist im Bereich des Datenschutzrechts insbesondere bei den **Zweckangaben der Rechtsgrundlagen** von Bedeutung (s.o. 4). Je präziser eine Datenverarbeitung in einer Verarbeitungsnorm beschrieben wird, desto berechenbarer ist dies für die Betroffenen und desto klarer ist der Normbefehl für die Anwendenden.

Der Gesetzgeber ist gehalten, beim Verfolgen eines bestimmten Zwecks ein Höchstmaß an Bestimmtheit auch in Bezug auf die **Modalitäten der Verarbeitung** zu suchen. Dies erfolgt z.B. durch eine klare Benennung der verarbeiteten Daten, durch eine Präzisierung der Art der Verarbeitung einschließlich deren vorgesehenes Ende (Löschvorgaben), durch eine Eingrenzung der verarbeitenden Stellen (Verantwortliche) sowie durch technische, organisatorische oder prozedurale Vorgaben und Voraussetzungen für eine Verarbeitung. Die Art der AZR-Daten sind in den §§ 2, 3, 29 AZRG präzise festgelegt. Ein hohes Maß an Bestimmtheit besteht auch bei der Benennung der Daten anliefernden (§§ 6, 30 AZRG) und in Bezug auf spezielle abfragende Stellen (§§ 15 ff., 32 AZRG).

Dem gegenüber sind die allgemeinen Befugnisnormen zum Erhalt oder zum Einstellen von Daten äußerst unbestimmt. **Alle öffentlichen Stellen** werden zu Abfragen berechtigt (§ 10 Abs. 1 AZRG). Die Befugnis zur Verarbeitung wird ausschließlich davon abhängig gemacht, dass diese zur Aufgabenerfüllung erforderlich ist. Dies gilt insbesondere auch für das Einstellen von Suchvermerken (§ 5 Abs. 1 AZRG, s.o. 4.4) und für die generelle Abrufbefugnis von Grunddaten nach § 14 AZRG. Materielle oder prozedurale Schranken sind nicht vorgesehen. Dies gilt auch für die Regelungen der §§ 15, 16 AZRG, wonach im Ergebnis sämtliche Sicherheitsbehörden und, nur wenig eingeschränkt, sämtliche Gerichte auf sämtliche im AZR gespeicherten Daten zugreifen dürfen.

6.1 Insbesondere Einreisebedenken

Gemäß § 2 Abs. 2 Nr. 4 AZRG ist eine Speicherung von Daten eines Ausländers zulässig, „gegen deren Einreise Bedenken bestehen, weil die Erteilungsvoraussetzungen nach § 5 Absatz 1 des Aufenthaltsgesetzes nicht vorliegen“. Die Vorschrift stand schon während des Gesetzgebungsverfahrens wegen der **inhaltlichen Unbestimmtheit** des Begriffs der „Bedenken gegen die Einreise“ in der Kritik.[148] Auch nach Aufnahme der Verweisung auf § 5 Abs. 1 AufenthG ist diese Kritik weiterhin berechtigt: Die Tatbestandsmerkmale dieser

[147] *Bäumler* NVwZ 1995, 243; *Weichert* DuD 2002, 428.
[148] *Schriever-Steinberg* ZAR 1990, S. 65, *Weichert* InfAuslR 1989, S. 2.

Vorschrift werden durch die Verweisung zu Tatbestandsmerkmalen des § 2 Abs. 2 Nr. 4 AZRG, so dass dessen rechtsstaatliche Mängel auch für die Verweisungsnorm bestehen.[149] § 5 Abs. 1 AufenthG verstößt wegen der Verwendung unbestimmter Rechtsbegriffe gegen das verfassungsrechtliche Gebot der Normbestimmtheit.[150] Einreisebedenken können schon bei Zweifeln an der wirtschaftlichen Grundlage eines beabsichtigten Aufenthalts bestehen. Ebenso genügen Zweifel an der Identität des Betroffenen oder bei der Annahme spezifischer Ausweisungsgründe. Vage Vermutungen genügen demnach, um Einreisebedenken zu begründen.

Eine Speicherung von Einreisebedenken ist u.a. wegen **nicht nachgewiesener Identität** (§ 5 Abs. 1 Nr. 1a AufenthG) vorgesehen. Für eine personenbezogene Speicherung ist es immer notwendig, die Identität des Betroffenen zu kennen oder zumindest präzise beschreiben zu können. Fehlt es hieran, so ist eine Speicherung nicht sinnvoll. Es ist unklar, welche Voraussetzungen vorliegen müssen, unter denen eine Behörde eine „ungeklärte Identität" feststellen kann.[151]

Dem Tatbestandsmerkmal der **Beeinträchtigung der Interessen der Bundesrepublik Deutschland** in § 5 Abs. 1 Nr. 3 AufenthG kommt eine Auffangfunktion zu. Trotz der Unbestimmtheit des Rechtsbegriffs „Interessen der Bundesrepublik Deutschland" tendiert die Rechtsprechung zu einem weiten Verständnis, weshalb auch diese Verweisung die Gesamtregelung zu unbestimmt sein lässt.[152]

6.2 Sonstige unbestimmte Regelungen

Ein **weiteres Beispiel** für eine übermäßige und deshalb unzulässige Unbestimmtheit ist der Speicheranlass, dass „tatsächliche Anhaltspunkte für den Verdacht" einer Vielzahl von teilweise auch tatbestandlich unbestimmt beschriebenen Straftaten bestehen (§ 2 Abs. 2 Nr. 7, 7a AZRG, s.o. 5.1).[153] Die Befugnis für BKA und Nachrichtendienste nach § 5 Abs. 2 AZRG einen Suchvermerk „zur Feststellung anderer Sachverhalte" im AZR speichern zu lassen, ist angesichts der Weite der Aufgaben und Ermittlungsbefugnisse dieser Stellen zu unbestimmt (s.o. 5.2 u. 5.5).[154] Das Speichermerkmal „Religionszugehörigkeit" (§ 3 Abs. 1 Nr. 5 AZRG) ist zu unbestimmt, da unklar ist, ob damit die Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgemeinschaft, die Teilnahme an einer irgendwie gearteten religiösen Vereinigung oder die individuelle Zuordnung zu einer bestimmten Glaubensrichtung gemeint ist (s.u. 8.2).[155]

[149] *Weichert* in GK-AufenthG, § 2 AZRG Rn. 42.
[150] *Bäuerle* in GK-AufenthG, § 5 AufenthG, Rn. 5 m.w.N. aus der verfassungsgerichtlichen Rspr.
[151] *Funke-Kaiser* in GK-AufenthG, § 5 AufenthG, Rn. 51.
[152] BVerwGE 56, 254, 258 = NJW 1979, 1112, 1113 = DÖV 1979, 291 f.; BVerwGE 61, 105, 108; kritisch *Weichert*, AZRG, § 2 Rn. 20; a.A. *Bäcker*, GFF-Gutachten, 2022, S. 24.
[153] *Bäcker*, GFF-Gutachten, 2022, S. 24 f.
[154] *Weichert* in GK-AufenthG, § 5 AZRG Rn. 11; *Bäcker*, GFF-Gutachten, 2022, S. 25.
[155] *Bäcker*, GFF-Gutachten, 2022, S. 29.

Das Bestimmtheitserfordernis beschränkt sich nicht auf die Befugnisnormen zur Verarbeitung, sondern erstreckt sich z.B. auch auf die **Einschränkung der Betroffenenrechte**. Zu unbestimmt ist die Regelung zur Auskunftsverweigerung, die erlaubt ist, wenn die Daten „ihrem Wesen nach" geheim gehalten werden müssen (§ 34 Abs. 2 Nr. 3 AZRG, s.u. 10.2), zumal insofern nicht einmal eine Interessenabwägung vorgesehen ist.[156]

7 Erforderlichkeit

Personenbezogene Daten dürfen durch öffentliche Stellen ohne Einwilligung der Betroffenen nur insoweit verarbeitet werden, als dies aus überwiegenden Gründen des Allgemeinwohls erforderlich ist (Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO). Nicht zulässig ist die Sammlung personenbezogener **Daten auf Vorrat** zu unbestimmten oder noch nicht bestimmten Zwecken.[157] Alle Stellen müssen sich auf ein Minimum bei der Datenverarbeitung beschränken. Eine Speicherung „für alle Fälle", ohne dass ein aktueller oder zukünftiger Bedarf klar umschrieben wäre, ist nicht erlaubt.[158]

Bei der Prüfung der Erforderlichkeit der Datenverarbeitung ist ein strenger Maßstab anzulegen: Eine Verarbeitung entspricht nur dann dem **Grundsatz der Datenminimierung** (Art. 5 Abs. 1 lit. c DSGVO), wenn eine Datenverarbeitung für zumindest einen konkreten Zweck benötigt wird, wobei die Art der Daten, die Art der Verarbeitungsphasen und -formen, die Qualität und Zahl der beteiligten Stellen wie auch die Gestaltung des Gesamtsystems von Bedeutung sind.[159] Es besteht kein Ermessensspielraum („margin of appreciation") oder eine vom Zweck losgelöste Rechtfertigung durch ein „dringendes soziales Bedürfnis".[160] Eine besondere Herausforderung in Bezug auf eine Differenzierung hinsichtlich der Erforderlichkeit ist gegeben, wenn mit einem Datum, einem Datensatz bzw. einem Datenverarbeitungssystem verschiedene Zwecke verfolgt werden, so wie dies beim AZR der Fall ist.

Es wird immer wieder darauf hingewiesen, dass das AZR **für Ausländer von großem Vorteil** sei.[161] Es führe zu einer erheblichen Beschleunigung der Bearbeitung von Ausländerangelegenheiten, z.B. im Visaverfahren zum Ausschluss von Einreisebedenken, oder wenn der Nachweis des Aufenthaltsrechts zu führen ist. Es eröffne Familienangehörigen im Ausland eine zentrale Anlaufstelle in dringenden Angelegenheiten, z.B. bei Krankheits- oder Todesfällen oder im Fall der Familienzusammenführung, um nach einem im Bundesgebiet lebenden Familienangehörigen zu suchen (vgl. § 25 AZRG). Derartige Vorteile im Einzelfall sind zweifellos zu begrüßen; sie begründen aber nicht die Erforderlichkeit der Speicherung im Rechtssinn bzgl. der umfassenden Eingriffe in das Recht auf informationelle Selbstbestimmung

[156] *Weichert* in *Däubler u.a.*, § 29 Rn. 4; vgl. *Herbst* in *Kühling/Buchner*, § 29 Rn. 7-10.
[157] BVerfG 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 46 f. = NJW 1984, 422; 17. JB LfD Bremen 1994/95, 56.
[158] *Weichert,* vorgänge Nr. 227 [3/2019], 62.
[159] *Roßnagel* in *Simitis/Hornung/Spiecker*, Art. 5 Rn. 67 ff., 129 ff.; *Weichert* in *Däubler u.a.*, Art. 5 Rn. 45 ff.
[160] So aber *Hailbronner* ZAR 2009, 181.
[161] *Streit* DuD, 1994, 560; *Reichert* ZAR 1990, 67.

für alle. Die Nutzungsmöglichkeit des AZR für private Zwecke ist nur ein Nebenprodukt des für öffentliche Stellen vorgehaltenen Datenbestands.

Die **Eilbedürftigkeit** von Entscheidungen, die Ausländer betreffen, rechtfertigt nur eingeschränkt die Verarbeitung im AZR. Ausländer betreffende Entscheidungen sind nicht per se eilbedürftig. Dies mag bei Maßnahmen zur Neuaufnahme von Flüchtlingen sowie bei der Aufenthaltsbeendigung und bei der Einreiseverweigerung der Fall sein. Nur bei einem kleinen Teil der im AZR registrierten Personen besteht die rechtliche Notwendigkeit bzw. Möglichkeit solcher Eilentscheidungen. Dies rechtfertigt es nicht, alle Ausländer undifferenziert zu belasten.

Die melderechtliche Funktion des AZR wird damit gerechtfertigt, bei Nichtdeutschen könnten Meldebehörden ihre Funktion zumeist nicht erfüllen. Die **Kette der Wohnsitzmeldungen** werde bei Ausländern durch zwischenzeitliche Fortzüge ins Ausland unterbrochen. Bei Ausländern seien in der Regel die Informationsquellen untauglich, die den öffentlichen Stellen üblicherweise bei Deutschen für dieselben Verwaltungszwecke zur Verfügung stehen. Das AZR könne Informationslücken schließen, die bei Deutschen in aller Regel nicht gegeben seien.[162]

Die Erforderlichkeit einer „lückenlosen Meldekette“ über das AZR mit der besonderen Mobilität von Ausländern zu begründen, ist nicht stichhaltig.[163] **Die Mobilität von Ausländern** mit einer längeren Aufenthaltsdauer, die ihren Lebensmittelpunkt in der Bundesrepublik haben, unterscheidet sich nicht signifikant von der Deutscher. Von den über 10 Mio. Ausländern leben ca. 3,3 Mio. bereits seit 20 Jahren oder länger im Land; ca. 5 Mio. sind seit mindestens 10 Jahren in Deutschland. Es ist zu vermuten, dass deutsche Staatsangehörige sogar eine höhere internationale Mobilität aufweisen als die ins Bundesgebiet eingewanderten Ausländer.

Der bloße Zweck einer **Erleichterung der administrativen Arbeit** genügt nicht, um erhebliche Grundrechtseingriffe zu rechtfertigen. Erfordernisse der Verwaltungsvereinfachung können nur in begrenztem Maße informationelle Grundrechtseingriffe rechtfertigen.[164] Wohl sind Erwägungen der Wirtschaftlichkeit, des Einsparens von Ressourcen und der Effektivität von Verwaltungshandeln Aspekte, die im Rahmen einer Verhältnismäßigkeitsprüfung zu berücksichtigen sind. Eine verstärkte Digitalisierung von Abläufen und eine Bündelung von Daten und eine Zentralisierung der Zugriffsmöglichkeit können im Rahmen der Bewertung der informationellen Eingriffe von Relevanz sein.[165] Soweit bei anderen Stellen vorhandene Daten benötigt werden, sind diese verfügbar zu machen. Dem dient das AZR.[166] Verwaltungseffektivität darf jedoch andererseits nicht auf Kosten von rechtsstaatlichen und grundrechtlichen Garantien umgesetzt werden. Es ist vielmehr Aufgabe gesetzlicher

[162] *Heyder* ZAR 1994, 154; *Streit*, DuD 1994, 559; *Streit/Heyder*, AZR-Gesetz, 1997, Einf. Rn. 16.
[163] VG Köln 28.11.2002 – 20 K 10510/00 Rn. 72-74; *Frankenberg*, FS Simitis, S. 106 f.
[164] VG Köln 28.11.2002 – 20 K 10510/00, Rn. 107
[165] Vgl. *Hailbronner* ZAR 2009, 180.
[166] BT-Drs. 12/6938, 16; *Weichert* in GK-AufenthG, § 1 AZRG Rn. 19.

Regelungen, effektive Verwaltung so zu praktizieren, dass Grundrechte und Rechtsschutz gewahrt bleiben. Dabei ist zu berücksichtigen, dass eine Zentralisierung von Daten und eine Beschleunigung von Verfahren mit einem Verlust an Betroffenen- und Sachnähe sowie an Entscheidungsqualität verbunden sein können und dass die Missbrauchsgefahr solcher Daten erhöht wird.[167]

Sprachliche Verständigungsprobleme deutscher Behörden mit den Betroffenen werden teilweise zur Legitimation des AZR herangezogen.[168] Derartige Probleme sind bei ausländischen Betroffenen zweifellos durchschnittlich größer als bei Deutschen. Es gibt aber eine Vielzahl von im AZR gespeicherten Personen, welche die deutsche Sprache perfekt beherrschen. Sprachprobleme lassen sich durch die Verwendung einer gemeinsamen Fremdsprache, durch mehrsprachige Angebote sowie mit Hilfe von Dolmetschern beheben bzw. reduzieren. Sie können es jedenfalls nicht generell legitimieren, dass an die Stelle einer Erhebung beim Betroffenen an diesem vorbei eine Erhebung beim AZR erfolgt.

Das AZR wird für die Kontrolle der **Inanspruchnahme öffentlicher Dienstleistungen** eingesetzt. Dies kann aber nicht eine umfassende Speicherung von Daten aus unterschiedlichen Quellen und viele Kontrollzwecke rechtfertigen. Viele der im AZR gespeicherten Ausländer nehmen solche Leistungen nicht in Anspruch. Die Berechtigung zum Bezug von Leistungen kann regelmäßig durch direkte Nachweise von den ursprünglich die Daten erhebenden Stellen authentischer belegt werden. Vorrang vor einer Datenbeschaffung beim AZR oder auch bei anderen Behörden muss die Direkterhebung bei den Betroffenen haben, die durch Vorlage von Dokumenten die nötigen Überprüfungen ermöglicht.[169] Die Erforderlichkeit eines direkten Austausches mit dem AZR muss begründet werden. Ein solcher Grund besteht z.B. bei der Aufnahme und Versorgung neu ankommender Flüchtlinge eher als bei Ausländern, die in die deutsche Gesellschaft voll integriert sind.

7.1 Zentrale Datenverarbeitung

Drittausländer erhalten, anders als Deutsche oder Unionsbürger, die ihr Aufenthaltsrecht aus der Staatsangehörigkeit ableiten können, dieses Recht in aller Regel erst durch besonderen Verwaltungsakt in Form eines Aufenthaltstitels (§ 4 AufenthG). Diese erworbene Rechtsposition kann wieder erlöschen und geändert werden. Vom **Aufenthaltsstatus** hängen eine Vielzahl anderer Entscheidungen ab. Dieser Status muss insofern, evtl. jederzeit und schnell, überprüfbar sein. Wegen der dezentral organisierten Ausländerverwaltung, der Vielzahl von Außenstellen des BAMF, den vielen deutschen Auslandsvertretungen und Grenzbehörden und zahlreichen weiteren Behörden, die Informationen über Drittausländer für die Erfüllung ihrer Aufgaben benötigen, sowie wegen der Tatsache, dass

[167] GFF, Das Ausländerzentralregister, 2022, 14 f.
[168] *Weichert* InfAuslR 1989, 11.
[169] VG Köln 28.11.2002 – 20 K 10510/00, Rn. 77; so gilt im Sozialrecht die Mitwirkungspflicht der Leistungsempfänger, § 60 Abs. 1 SGB I.

aufenthaltsrechtlichen Entscheidungen einer Behörde für die anderen jeweils verbindlich sind, wird das AZR als zentrale bundesweite Informationsstelle für unverzichtbar angesehen.[170]

Ein solches zentrales Melderegister ist aber nicht erforderlich für Ausländer, die seit Jahren ihren Lebensmittelpunkt im Bundesgebiet haben und deren **gesicherter Aufenthaltsstatus** keinen oder kaum noch Änderungen unterworfen ist. Ein sicherer Aufenthalt besteht nicht nur für freizügigkeitsberechtigte Unionsbürger, sondern auch für viele Staatsangehörige aus Drittstaaten.

Es bedarf keiner **zentralen Erfassung** aller Ausländerinnen und Ausländer aus EU-Staaten; Entsprechendes gilt für Drittausländer mit einem gesicherten Aufenthaltsstatus. Für eine derartige zentrale Datenverarbeitungsstruktur wäre eine spezifische Legitimation nötig, die nicht zu erkennen ist.[171] Auch der Umfang der zu jeder Person erfassten Daten ist in Frage zu stellen. Für die Wahrnehmung der meisten vom AZR erfüllten Aufgaben wäre die Speicherung der Identifikationsdaten mit Hinweisen auf die tätig gewordenen Behörden ausreichend.[172]

Bei den Beratungen zum Melderecht im Jahr 1978 plante der Bundesgesetzgeber zunächst „Landesadressregister“ mit 10 Grundangaben zu jeder Person. Von solchen zentralen Registern sah man aus Datenschutzgründen letztendlich ab.[173] 1987 warnten die Datenschutzbeauftragten des Bundes und der Länder davor, das AZR zu einem bundesweiten Melderegister für Nicht-Deutsche zu machen.[174] Die heute, nach 35 Jahren, dort stattfindende, noch massiv erweiterte **zentralisierte Datenspeicherung** geht über das erforderliche Maß noch deutlicher hinaus.

7.2 Verarbeitung von Dokumenten

Die Regelung zur digitalen Verarbeitung von Dokumenten wurde mit dem AZRWeiterentwG v. 09.07.2021[175] eingeführt. Die Regelung tritt am 01.11.2022 in Kraft (Art. 12 Abs. 1 AZRWeiterentwG). Zuvor gilt, dass Begründungstexte von Entscheidungen über Ausweisung, Abschiebung und Einreisebedenken gespeichert sind, die bei Bedarf übersendet werden können. Damit erfolgt schon bisher und absehbar verstärkt eine **parallele zentrale Aktenführung** neben der lokalen in den Ausländer- und Asylbehörden. Begründet wird die Notwendigkeit dieser parallelen und zentralisierten Aktenführung damit, dass die Texte für eilige Entscheidungen umgehend zur Verfügung stehen müssten.[176] Die Dokumente können im automatisierten Verfahren abgerufen werden (§ 22 Abs. 4 AZRG). Eine solche Begründung der Erforderlichkeit war 1994 beim Inkrafttreten des AZRG möglicherweise verständlich. Sie ist es aber nicht mehr heute angesichts der Möglichkeiten dezentraler digitaler

[170] *Streit/Heyder*, AZR-Gesetz, Einf. Rn. 15; *Streit/Srocke* ZAR 1999, 109.
[171] EuGH 16.12.2008 – C-524/06, Rn. 66; weniger kritisch *Bäcker*, GFF-Gutachten, 2022, S. 3.
[172] *Weichert* InfAuslR 1987, 209.
[173] *Mühlbauer*, Einwohnermeldewesen, 1995, S. 108 ff.; 1. TB BfD 1978 (BT-Drs. 8/2460), 15.
[174] IX. TB LfD Nds. 1988, 190.
[175] BGBl. I S. 2467.
[176] BT-Drs. 12/6938, 21.

Kommunikation. Der Zugriff auf zentral gespeicherte Dokumente ist nicht erforderlich, wenn die benötigten Dokumente im Einzelfall von der aktenführenden Behörde digital zur Verfügung gestellt werden können. Dies ist heute der Fall.

Für die Bereitstellung solcher Daten bedürfte es, in den Fällen, dass die Dokumente auch sensitive Daten nach Art. 9 Abs. 1 DSGVO enthalten, eines „**erheblichen öffentlichen Interesses**“ (Art. 9 Abs. 2 lit. g DSGVO). Für eine solche gesteigerte Erforderlichkeit besteht erst recht keine plausible Begründung:

In den zu übermittelnden Dokumenten sind vielfach **sensitive Daten** gemäß Art. 9 Abs. 1 DSGVO enthalten. Dies gilt in BAMF-Dokumenten für „ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit“ sowie für „Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung“. BAMF-Bescheide enthalten oft präzise Angaben über Verfolgungsgründe. Entscheidungen zu aufenthaltsbeendenden Maßnahmen (Ausweisung, Abschiebung, Zurückweisung, Zurückschiebung) basieren zumeist auf einer umfassenden Abwägung aller in § 54 AufenthG genannten Ausweisungsinteressen, etwa strafrechtliche Verurteilungen (vgl. Art. 10 DSGVO) oder sonstigen Rechtsverstößen einerseits und der in den §§ 53 Abs. 2, 55 AufenthG genannten Bleibeinteressen, die auf persönlichen, wirtschaftlichen und sonstigen Bindungen sowie auf Folgen für Familienangehörige und Lebenspartner beruhen können, inklusive Verweise auf psychiatrische oder ärztliche Gutachten oder Berichte von Sozialarbeitern. Für die Dokumentenübermittlung über die Einschränkung oder Untersagung der politischen Betätigung fehlt schon die gesetzliche Grundlage für diesen Speicheranlass. Dokumente zu Einreisebedenken enthalten evtl. existenzielle Informationen über den Betroffenen (s.o. 6.1). Die Regelung macht keinen Unterschied zwischen bestands- oder rechtskräftigen und anfechtbaren Dokumenten. Die Verarbeitung erfolgt außerhalb des Aktenkontextes, so dass als Ergebnis verkürzte, aus dem Zusammenhang gerissene Daten bereitgestellt werden. Die für eine Abwägung nötigen Informationen zur Feststellung der Übermittlungsbefugnis liegen regelmäßig im AZR nicht vor.[177]

Die Betroffenen haben gleichzeitig keine Möglichkeit zur Stellungnahme bzw. zur Gegendarstellung. § 35 AZRG bzw. Art. 16 DSGVO sind nicht anwendbar, da es wegen der Dokumentationsfunktion nicht auf die inhaltliche Richtigkeit der Texte ankommt, sondern auf die richtige Wiedergabe des Dokuments. Bestandskräftige Entscheidungen mögen im Tenor richtig, aber mit falschen Angaben begründet sein. Solche Gründe aus AZR-Dokumenten können ausschlaggebend für weitere Entscheidungen sein. Den Betroffenen ist regelmäßig nicht bewusst, dass die Entscheidungsbegründungen bundesweit als Grundlage für weitere

[177] 23. TB HDSB 1994, 121; 13. TB HmbDSB 1994, 99 ff.; 17. JB LfD Bremen 1994/95, 56; *Bäcker*, GFF-Gutachten, 2022, S. 31; *Schriever-Steinberg* ZAR 1990, 64; *dies.* NJW 1994, 3276; *Weichert* InfAuslR 1987, 209, 214; *ders.* InfAuslR 1989, 3.

Entscheidungen zur Verfügung stehen. Gegen **unrichtige Angaben in Entscheidungen** gibt es kein Rechtsmittel.[178]

Bei den aufgrund von übermittelten Begründungstexten bzw. Dokumenten gefällten Entscheidungen wird der **Anspruch auf rechtliches Gehör** der Betroffenen beschnitten (§ 66 VwVfG). Obwohl die Entscheidung u.U. existentielle Bedeutung für den Betroffenen hat, wird ihm bei einer Eilentscheidung oder auch bei sonstigen Verfügungen der Umstand der Hinzuziehung der Texte nicht mitgeteilt, geschweige denn, dass eine richtige Anhörung erfolgen würde.

Geregelt sein müssten „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ (Art. 9 Abs. 2 lit. g DSGVO). Erfasst werden nicht nur Entscheidungen zugunsten, sondern vor allem zulasten der Betroffenen. Die in § 6 Abs. 5 S. 2 und 3 (neue Fassung) sowie in § 10 Abs. 6 AZRG genannten Maßnahmen sind nicht hinreichend. Zwar ist vorgesehen, dass bei Asylentscheidungen nicht „besondere gesetzliche Verarbeitungsregelungen oder **überwiegende schutzwürdige Interessen** des Ausländers“ entgegenstehen dürfen. Diese völlig unklare und viel zu unbestimmte Regelung gilt aber nicht für sämtliche Dokumente. Selbst für Asyldokumente gibt sie keinen gesicherten Schutz, da durch deren Kontextverlust nicht gewährleistet ist, dass diese Schutzinteressen überhaupt erkennbar sind.

Der Begriff der „**besonderen gesetzlichen Verarbeitungsregelungen**“ in § 6 Abs. 5 S. 2 AZRG ist außerhalb des Ausländerrechts nicht üblich (vgl. aber § 88 AufenthG, § 8 Abs. 1 AsylG). Dazu werden besondere Amts- und Berufsgeheimnisse (vgl. § 203 StGB, Art. 9 Abs. 3 DSGVO), Beratungsgeheimnisse, das Sozialgeheimnis (§ 35 SGB I) oder das Steuergeheimnis (§ 30 AO), strenge Zweckbindungsregelungen, etwa zur Datensicherheit zur Datenschutzkontrolle oder zur Verarbeitung für Forschungszusammenzwecke (Art. 89 Abs. 4 DSGVO), gezählt. Die Regelung entfaltet nur eine eingeschränkte und damit ungenügende Schutzwirkung. So ist deren Beachtung schon durch die ungewöhnliche Terminologie, die nicht auf den besonderen Vertraulichkeits- und Geheimnischarakter hinweist, nicht gesichert. Die mit dem Begriff erfassten „Geheimnisse“ berücksichtigen nicht die wesentlichen schutzwürdigen Betroffeneninteressen.[179]

§ 6 Abs. 5 S. 2 2. HS AZRG (neue Fassung) verlangt zusätzlich, dass Erkenntnisse aus dem **Kernbereich privater Lebensgestaltung** unkenntlich gemacht werden müssen. Die Regelung ist in sich widersprüchlich, da in den Dokumenten gar keine Erkenntnisse aus diesem Kernbereich aufgeführt werden dürften. Insofern droht die Regelung leerzulaufen. Gemäß der

[178] *Schenke/Schenke* in *Kopp*, VwGO, 25. Aufl. 2019, § 113 Rn. 63; zur Fragwürdigkeit der Gesetzesbegründung der umfassenden Dokumentenverfügbarkeit *Wittmann*, Stellungnahme v. 30.04.2021, BT-Innenausschuss A-Drs. 19(4)820 D, 29 ff. sowie *Bäcker*, GFF-Gutachten, 2022, S. 31 ff.
[179] Ähnlich *Bäcker*, GFF-Gutachten, 2022, S. 32.

Rechtsprechung des BVerfG ist der Kernbereich absolut geschützt. Dem Staat und seinen Organen ist es untersagt, in diesen Bereich einzugreifen.[180]

§ 6 Abs. 5 S. 3 AZRG (neue Fassung) verweist auf die Voraussetzungen des § 10 Abs. 6 AZRG (neue Fassung), wonach die automatisiert abrufende Stelle der Registerbehörde bestätigen muss, dass das Dokument „**unerlässlich** ist, weitere Informationen nicht rechtzeitig von der aktenführenden Behörde zu erlangen sind und ihr die Daten, auf die sich die Dokumente beziehen, übermittelt werden dürfen".[181] Es ist nicht geregelt, wie die Registerbehörde die Richtigkeit dieser Erklärung überprüfen soll; tatsächlich ist ihr dies gar nicht möglich.

Die Weiterverarbeitung der vom AZR erlangten Dokumente wird in § 11 Abs. 1 S. 1 AZRG untersagt. Die Nutzung ist nur zum Übermittlungszweck erlaubt. Dieser Zweck kann aber weit reichen (vgl. Tz. 11.1 AZR-VV). Eine Weiterübermittlung wird in der Praxis nicht wirksam verhindert. Das **Weiterverwendungsverbot** ist nicht durch Kennzeichnungs- und Separierungs- geschweige denn Kontrollvorschriften prozedural gewährleistet. Ein Unterlaufen der Zweckbindung wird nicht wirksam verhindert.

Bei dem erlaubten **automatisierten Abruf** gemäß § 22 AZRG wird die Verantwortung für die Zulässigkeit faktisch auf die abrufende Stelle übertragen. Damit die Registerbehörde formal ihre Verantwortung bewahren kann, muss sie sich gemäß § 6 Abs. 5 S. 3 AZRG die positive Rechtmäßigkeitsprüfung durch die abrufende Stelle bestätigen lassen. Die Interessenabwägung wird dorthin verlagert, wo ein starkes Interesse am Abruf besteht. Es ist daher unrealistisch, dass die Abwägung angemessen durchgeführt wird. Denn für die abrufende Stelle stehen die eigenen Interessen an der Erlangung des Dokuments im Vordergrund. Selbst im Zweifelsfall ist der Registerbehörde eine Prüfung oft nicht möglich, da sie mangels Aktenrückhalt keine umfassende Bewertung vornehmen kann.[182]

Gemäß § 26 S. 6 u. 7 AZRG ist die **Auslandsübermittlung** von Dokumenten nach § 6 Abs. 5 AZRG an Behörden und Stellen außerhalb der EU unzulässig. Behörden innerhalb der EU sind darauf hinzuweisen, dass die Dokumente nur zu dem Zweck verarbeitet werden dürfen, zu dem sie übermittelt worden sind und eine Weiterübermittlung der Dokumente an Behörden anderer Staaten nicht erfolgen darf.

Angesichts der umfangreichen Zugriffsmöglichkeiten deutscher Behörden besteht das Risiko, dass insbesondere durch Sicherheitsbehörden Datenübermittlungen ins Drittausland vorgenommen werden, wobei dann vorrangig andere Übermittlungsregelungen anzuwenden sind. Auch für solche Fälle ist zwar eine Weiterübermittlungen unzulässig, da die zwingende

[180] BVerfG 03.03.2004 – 1 BvR 2378/98 u. 1 BvR 1084/99, NJW 2004, 1002 f.; *Baldus*, JZ 2008, 218 ff.; *Bäcker*, GFF-Gutachten, 2022, S. 33; kritisch zur Kernbereichsspeicherung GFF, Das Ausländerzentralregister, 2022, 11; zu den Umsetzungsproblemen BT-Drs. 19/32112 Frage 21.
[181] *Bäcker*, GFF-Gutachten, 2022, S. 47.
[182] *Wittmann*, Stellungnahme v. 30.04.2021, BT-Innenausschuss A-Drs. 19(4)820 D, 32 f); *Petri*, Stellungnahme v. 28.04.2021, BT-Innenausschuss A-Drs. 19(4)820 A, 7 f.; BfDI, Stellungnahme v. 30.04.2021, BT-Innenausschuss A-Drs. 19(4)823, 2.

gesetzliche Vermutung besteht, dass der Übermittlung **schutzwürdige Betroffenenbelange** entgegenstehen. Es ist aber normativ nicht gewährleistet, dass diese gesetzlich geforderte Abwägung durchgeführt wird. Es müsste zumindest geregelt werden, dass eine entsprechende Markierung des Dokuments erfolgt. Diese Problematik besteht selbst bei Empfängern in anderen EU-Staaten.

Die Speicherung von Dokumenten bzw. von Begründungstexten im AZR in der gesetzlich geregelten Form verstößt gegen Art. 5 Abs. 1 DSGVO. Die Verarbeitung muss „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (´**Datenminimierung**´)“ (lit. c). Aus technischen Gründen besteht zumindest heute angesichts der Verfügbarkeit elektronischer Kommunikationsmedien bei allen Beteiligten keine Erforderlichkeit einer zentralen Speicherung mehr. Ein Rückgriff auf die Originalakten genügt und ist erheblich zuverlässiger. Sollten einzelne Informationen aus den Dokumenten erforderlich sein, so sind sie regelmäßig nicht ausreichend, da sich der Kontext der Information zumeist nur aus der Originalakte ergeben kann.[183]

7.3 Amtshilfe durch das BKA

Das Bundeskriminalamt (BKA) leistet gemäß § 1 Abs. 3 S. 1 AZRG Amtshilfe bei der Verarbeitung der nach § 16 Abs. 1 S. 1 AsylG und § 49 AufenthG erhobenen Daten. Die Regelungen beziehen sich auf biometrische, erkennungsdienstliche und sonstige Identifizierungsdaten. Vergleichbare Amtshilfevorschriften bestehen in § 16 Abs. 3, 3a, 4 AsylG und § 89 Abs. 1 AufenthG. Die Amtshilfeverpflichtung des BKA besteht im Asylverfahren bereits seit 1993 und wurde 2007 auf die Daten nach § 49 AufenthG erweitert. Der Begriff der Amtshilfe ist im Datenschutzrecht nicht bekannt; es gibt nur die Verantwortlichkeit und die Auftragsverarbeitung.[184] Praktische Relevanz hat die Regelung insbesondere bei der Speicherung und dem Abgleich der Fingerabdrücke (§ 3 Abs. 2 Nr. 1 AZRG), die in der vom BKA betriebenen Fingerabdruckdatei AFIS-A mit einer recherchierbaren Referenznummer gespeichert werden.

Gemäß § 1 Abs. 3 S. 2 AZRG werden die beim BKA verarbeiteten aus ausländerrechtlichen Gründen verarbeiteten Daten „getrennt von anderen erkennungsdienstlichen Daten gespeichert“ (ebenso § 89 Abs. 1 S. 3 AufenthG, § 16 Abs. 4 AsylG). Tatsächlich besteht weder eine räumliche noch eine organisatorische oder funktionale **Trennung** zwischen AFIS-A (Ausländer) und AFIS-P (Polizei), sondern lediglich eine spezifische technische Markierung.[185] Die gesetzlich vorgesehene Trennung gewährleistet nicht, dass das BKA für die Daten keine Nutzungsbefugnis für die eigenen Zwecke der Gefahrenabwehr und der Strafverfolgung hat. Diese Eigennutzung ist ausdrücklich gesetzlich erlaubt (§ 15 Abs. 1 S. 1 Nr. 5 AZRG, § 89 Abs. 2

[183] *Wittmann*, Stellungnahme v. 30.04.2021, BT-Innenausschuss A-Drs. 19(4)820 D, 31 f.; *Bäcker*, GFF-Gutachten, 2022, 3 f.
[184] Art. 4 Nr. 7, 8 DSGVO; *Weichert* in *Däubler u.a.*, Art. 4 Rn. 86-98.
[185] *Weichert* in *Huber*, AufenthG, 2010, § 89 Rn. 7.

AufenthG, § 16 Abs. 5 AsylG). Tatsächlich nutzt die Polizei AFIS-A unbeschränkt für die eigene Aufgabenwahrnehmung und verstößt damit zugleich gegen das Zweckbindungsprinzip (s.o. 4).

Nach § 4 Abs. 1 VwVfG ist Amtshilfe die unter Behörden geleistete ergänzende Hilfe. Bei der Hilfe des BKA für das BAMF bestimmt das BKA selbständig Mittel und Zwecke der eigenen Verarbeitung. Dies hat zur Folge, dass eine **gemeinsame Verantwortlichkeit** i.S.v. Art. 26 DSGVO vorliegt.[186] Für diese gemeinsame Verantwortlichkeit, mit der eine starke Einflussmöglichkeit des BKA auf die rein ausländerrechtlich begründete Datenverarbeitung einhergeht, besteht inzwischen keine Erforderlichkeit mehr. Historisch war die Amtshilfe des BKA damit begründet, dass sich die technischen Kompetenzen zur Erfassung und Auswertung erkennungsdienstlicher Unterlagen bei der Polizei konzentrierten. Inzwischen kommen Techniken zum Einsatz, die keine polizeilichen Spezialkenntnisse mehr erfordern. Die Amtshilferegelungen verstoßen daher gegen den Grundsatz der Datenminimierung und müssen aufgehoben werden.

7.4 Zehn Fingerabdrücke

Im AZR erfolgt die Speicherung aller 10 Fingerabdrücke von Flüchtlingen (§ 3 Abs. 2 Nr. 1 AZRG). Für den primär verfolgten aufenthaltsrechtlichen Zweck einer eindeutigen Identifizierung wären nicht die Abdruckdaten aller Finger erforderlich. Ausreichend wären hierfür z.B. die Abdruckdaten von einem oder von zwei eindeutig definierten Fingern.[187] Die Nutzung aller 10 Fingerabdrücke für Zwecke der Gefahrenabwehr und Strafverfolgung ist kein originär aufenthaltsrechtlicher Zweck. Darüber erfolgt eine – im Hinblick auf den Großteil der rechtschaffenen erfassten Ausländer – eine unzulässige Zweckänderung (s.o. 4) und eine unzulässige Vorratsdatenspeicherung.[188] Die damit verbundene **Verletzung des Erforderlichkeits- und Verhältnismäßigkeitsgrundsatzes** beschränkt sich nicht auf das AZR, sondern gilt für alle Bereiche des Ausländerrechts, wonach zu Identifikationszwecken immer sämtliche 10 Fingerabdrücke erfasst werden.[189]

7.5 Weitere Regelungen

Im AZR erfolgen Doppel- und Mehrfachspeicherungen von an anderer Stelle verfügbaren Daten. Diese Mehrfachspeicherungen durch die Substitutionsfunktion des AZR im System angelegt (s.o. 4). Sie können gerechtfertigt sein, wenn die jeweilige Mehrfachspeicherung für eine effektive Verwaltungstätigkeit erforderlich ist. Davon kann keine Rede sein, wenn sowohl die Speicher- als auch die Abfragemöglichkeit bei Stellen besteht, die auf sachnähere Informationsquellen zugreifen können. Dies gilt insbesondere für die Informationssysteme der Polizei, die auf Bundesebene in INPOL zusammengeführt sind, sowie für das von den

[186] *Weichert* in GK-AufenthG, § 1 AZRG Rn. 31.
[187] *Weichert* DVBl 2021, 1073.
[188] *Frankenberg*, FS Simitis, S. 104 f.
[189] Ausführlich *Weichert*, Staatliche Identifizierung, www.netzwerk-datenschutzexpertise.de 08.03.2021, S. 35 ff.; *ders.* DVBl 2021, 1069 ff.

Nachrichtendiensten genutzte Nachrichtendienstliche Informationssystem (NADIS). Für die **redundante Zugriffsmöglichkeit** über das AZR besteht keine Erforderlichkeit. Durch diese Zugriffsmöglichkeit besteht die Gefahr von Inkonsistenzen zwischen den erlangten Abfrageergebnissen. Da es sich bei dem AZR um das sachfremdere Register handelt, dürfte hierbei eine höhere Fehlerquote bestehen. Direktzugriffe sind nur auf die Originaldatenquellen zuzulassen. Es gibt keine Hinweise darauf, dass dadurch Informationsdefizite entstehen würden.[190]

Die Erforderlichkeit einer ausnahmslosen Speicherung der **Lichtbilder von allen Drittausländern** gemäß § 3 Abs. 1 Nr. 5a AZRG ist nicht dargetan.[191] Ausländerrechtlicher Hauptzweck des Lichtbildes ist es, die Identität einer Person vor Ort festzustellen. Das AZR selbst hat keinen direkten Betroffenenkontakt. Regelmäßig ist ein Gesichtsabgleich auch vor Ort nicht nötig, wenn die Betroffenen entsprechende Ausweisdokumente vorweisen können. Fehlen diese, so genügt die Lichtbildspeicherung vor Ort, etwa bei der Ausländerbehörde (§ 82 Abs. 5 AufenthG).

Mit dem AZRWeiterentwG v. 9.7.2021[192] wurde in § 3 Abs. 1 Nrn. 5c, 5d AZR die generelle Speicherung von **deutschen Wohnadressen** eingeführt, und zwar mit Ein- und Auszugsdatum (Nrn. 5c, 5d) in Bezug auf sämtliche Nicht-EU-Bürger. Zuvor war eine Speicherung von Wohnadressen nur bei Flüchtlingen vorgesehen. Die Speicherung im AZR erfolgt zusätzlich zu derjenigen bei den Meldebehörden. Begründet wurde die Erweiterung der Adressspeicherung mit der effizienteren Gestaltung des Verfahrensablaufs sowie mit dem formalen Verweis darauf, dass diese Daten auch bei den Ausländerbehörden verfügbar sind.[193] Während es bei Flüchtlingen wegen des zunächst meist öfter erfolgenden Wohnsitzwechsels noch begründbar ist, dass die Adressen zentral gespeichert werden, ist dies bei sonstigen Drittausländern nicht der Fall. Insofern besteht hierfür bei diesen keine Erforderlichkeit.[194]

§ 16 AZRG eröffnet **Gerichten** den Zugriff auf die AZR-Daten und zwar unterschiedslos nicht nur Straf- und Verwaltungsgerichten, sondern auch Zivilgerichten. Dieser Zugriff beschränkt sich nicht auf Grunddaten, sondern ist in einem gestuften Verfahren auf sämtliche AZR-Daten möglich, wobei insofern – als einzige Verfahrenssicherung – die „Erforderlichkeit“ aktenkundig gemacht werden muss (§ 16 Abs. 2, 3 jeweils S. 2 AZRG). Die generelle Erforderlichkeit hierfür ist nicht dargetan. Dies gilt selbst für Straf- und Verwaltungsgerichte, da in deren Verfahren Behörden eingebunden sind, die einen AZR-Zugang haben und den Gerichten die erforderlichen Informationen beibringen können.

[190] *Weichert* in GK-AuflR, § 2 AZRG, Rn. 72-74.
[191] 21. TB BfDI 2005-2006, Kap. 7.1.1, S. 94 f.; a.A. *Bäcker*, GFF-Gutachten, 2022, S. 26, der fälschlich von einer „begrenzten Sensibilität“ ausgeht.
[192] BGBl. I S. 2467.
[193] BR-Drs. 186/21, 79.
[194] *Petri*, Stellungnahme v. 28.04.2021, BT-Innenausschuss, A-Drs. 19(4)820 A, 6; *Bäcker*, GFF-Gutachten, 2022, S. 3, 30 f.

7.6 Datenlöschung

Eine spezifische Ausgestaltung des Erforderlichkeitsgrundsatzes ist es, dass Daten zu löschen sind, wenn sie für die verfolgten Zwecke nicht mehr notwendig sind (Art. 17 Abs. 1 lit. a DSGVO). Damit wird nicht nur dem Prinzip der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) entsprochen, sondern auch dem Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e). Die Betroffenen haben unter den in Art. 17 DSGVO genannten Voraussetzungen einen Anspruch auf Datenlöschung. Unabhängig von der Umsetzung dieses Betroffenenrechts ist der Verantwortliche verpflichtet, nicht mehr erforderliche Daten **von sich aus zu löschen**.[195]

§ 36 AZRG setzt die Löschverpflichtung einfachgesetzlich durch die Vorgabe um, dass Daten nach Fristablauf zu löschen sind; die **Löschungsfrist** wird von der übermittelnden Stelle mitgeteilt. Die Eintragung eines Löschdatums ist bisher kein Pflichtfeld im AZR-Datensatz und wird häufig versäumt bzw. unterlassen. Dem Evaluierungsbericht des Bundesinnenministeriums (BMI) ist zu entnehmen, dass Löschfristen im AZR regelmäßig nicht eingehalten werden. Eine automatisierte Löschung nach Fristablauf erfolgt bisher nur in Bezug auf Gesundheitsdaten.[196] Speicherfristen beim allgemeinen Datenbestand sind in den § 18 AZRG-DV festgelegt. Nach § 18 Abs. 1 AZRG-DV wird der gesamte Datensatz eines Ausländers spätestens nach Ablauf von 10 Jahren nach seiner Ausreise gelöscht. Ansonsten erfolgt die Löschung nach Ablauf von 5 Jahren nach dem Tod. Die Regelungen und deren Umsetzung führen dazu, dass in Deutschland zum Stichtag 31.07.2021 11.607.351 Personen lebten, im AZR aber 18.998.769 Personen erfasst waren.[197]

Die bestehenden Regelungen gewährleisten nicht die **technische und organisatorische Umsetzung** der Löschpflichten; dem Erfordernis einer frühestmöglichen Löschung wird so in der Praxis nicht entsprochen.

8 Verhältnismäßigkeit im engeren Sinne

Gemäß Art. 52 Abs. 1 S. 2 GRCh dürfen Einschränkungen in die Grundrechte nur unter Wahrung des Grundsatzes der Verhältnismäßigkeit vorgenommen werden. Sie müssen notwendig sein (s.o. 7) und den von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten Anderer tatsächlich entsprechen. Als Kriterien für die Verhältnismäßigkeit ist neben der Geeignetheit und Erforderlichkeit zur Zielerreichung, die Angemessenheit des Eingriffs zu prüfen.

8.1 Angemessenheit allgemein

Im AZR erfolgt die Speicherung von Daten zur Identifizierung einer Person und zu einer **Vielzahl von Lebenssachverhalten** (Aufenthaltsstatus, Straftaten, Einreisebedenken, politische Betätigung). Praktisch alle öffentlichen Stellen, die mit den Betroffenen zu tun

[195] *Däubler* in *Däubler u.a.*, Art. 17 Rn. 2; *Herbst* in *Kühling/Buchner*, Art. 17 Rn. 8 f.
[196] BMI, BT-Drs. 19/17380, 32 f; GFF, Das Ausländerzentralregister, S. 12.
[197] BT-Drs. 19/32508, 2.

haben und bei denen die Ausländereigenschaft eine Rolle spielt, sind zur Anlieferung von Angaben befugt oder gar verpflichtet (§ 6 AZRG). Durch die Speicherung von Begründungstexten werden zusätzlich zu den formatierten Daten Angaben bis hinein in den persönlichen und intimen Bereich gespeichert und zum allgemeinen Abruf bereitgehalten.[198]

Um die Verhältnismäßigkeit der Regelungen des AZRG zu rechtfertigen, wird generell darauf verwiesen, die Möglichkeit der Informationsbeschaffung für andere öffentliche Stellen liege im überwiegenden Allgemeininteresse. Nur so könnten ein effizientes und kostensparendes Verwaltungshandeln sowie **schnelle und sachgerechte Entscheidungen** erreicht werden. Schnelle Informationen kämen auch den Betroffenen unmittelbar zugute.[199] Eine derart pauschale Begründung genügt nicht zur Legitimation der Grundrechtseingriffe. Die Überprüfung der Angemessenheit als Verhältnismäßigkeit im engeren Sinne der konkreten Verarbeitungsprozesse verlangt eine Betrachtung der einzelnen Normen und der Zwecke.

8.2 Speicherung der Religionszugehörigkeit

Die Speicherung der Religionszugehörigkeit gemäß § 3 Abs. 1 Nr. 5 AZRG ist unverhältnismäßig. Es handelt sich hierbei um ein sensitives Datum (Art. 9 Abs. 1 DSGVO, s.o. 2.3). Zulässig wäre die Verarbeitung, wenn hierfür ein erhebliches öffentliches Interesse bestünde und ausreichende Schutzmaßnahmen vorgesehen wären (Art. 9 Abs. 2 lit. g DSGVO). Begründet wird die Speicherung mit der **Terrorismusbekämpfung**. Insbesondere im Zusammenhang mit Gruppenauskünften könne die Religionszugehörigkeit als Auswahlkriterium dienen.[200] Es ist nicht erkennbar, wie die Kenntnis der Religionszugehörigkeit, mit der ein hohes Stigmatisierungs- und Diskriminierungsrisiko verbunden sein kann, für dem genannten primär sicherheitsbehördlichen Zweck angemessen sein könnte.[201] Die Geeignetheit der Speicherung wird dadurch eingeschränkt, dass hierfür die Einwilligung der Betroffenen verlangt wird, und potenzielle religionsmotivierte Gefahrenpersonen ihre Einwilligung wahrscheinlich nicht erteilen.

Das gesetzlich geregelte **Einwilligungserfordernis** ist keine hinreichende grundrechtssichernde Maßnahme. Es ist fraglich ob die Einwilligungen freiwillig erteilt werden (vgl. Art. 4 Nr. 11 DSGVO). In jedem Fall werden diese nicht „in informierter Weise“ abgegeben, da die Nutzungsmöglichkeiten für die Betroffenen nicht ansatzweise absehbar sind.[202] Dies gilt insbesondere für sicherheitsbehördliche Abfragen, mit denen für die Betroffenen zusätzliche, möglicherweise massiv beeinträchtigende operative Eingriffe einhergehen können. Aus diesen

[198] *Schriever-Steinberg* NJW 1994, 3276; *dies.* ZAR 1990, 65; *Weichert* InfAuslR 1989, 7.
[199] *Streit/Heyder*, AZR-Gesetz, Einf. Rn. 15.
[200] BT-Drs. 14/7386, 61.
[201] *Bäcker*, GFF-Gutachten, 2022, S. 28.
[202] Weitergehend *Hilbrans* in *Hofmann*, § 86 AufenthG, Rn. 17 m.w.N., der die Frage nach einem religiösen Bekenntnis generell für unzulässig ansieht.

Gründen kommt auch Art. 9 Abs. 2 lit. a DSGVO als Legitimation für die Speicherung dieses Merkmals nicht in Betracht.[203]

9 Diskriminierungsverbot

Von Anfang an wurde kritisiert, dass die Ausländerregistrierung im AZR gegen den Gleichheitsgrundsatz und das damit verbundene Diskriminierungsverbot (Art. 3 GG, jetzt auch Art. 21 GRCh) verstößt.[204] Ein bundesweites zentrales Register gibt es nur für Ausländer, nicht für Deutsche. Das AZRG knüpft diese Ungleichbehandlung an die **Staatsangehörigkeit**, die nur in begründeten Fällen zur Differenzierung herangezogen werden darf (Art. 21 Abs. 2 GRCh)**.** Das verfassungsrechtliche Gleichheitsgebot verbietet die unterschiedliche Behandlung vergleichbarer Sachverhalte, wenn es keinen sachlichen Grund für die Differenzierung gibt. Die Gleichheitsverbürgungen gelten für alle Menschen, also auch für Ausländer.[205] Es war zunächst umstritten, inwieweit die Differenzierung nach der Staatsangehörigkeit von Art. 3 Abs. 3 GG (Abstammung, Heimat, Herkunft) erfasst wird.[206] Durch die Regelung des Art. 21 Abs. 2 GRCh hat sich dieser Streit erledigt. Aus dem Wortlaut des Art. 21 Abs. 2 GRCh geht nicht hervor, dass dieser nur für Unionsbürger gelten soll.[207]

Zur Begründung der Ungleichbehandlung von Deutschen und Ausländern nach dem AZRG wird vorgebracht, bei der Durchführung ausländer- und asylrechtlicher Vorschriften könne es keine vergleichbaren Sachverhalte für deutsche Staatsangehörige geben; gegen Deutsche könnten keine aufenthalts- und asylrechtlichen Entscheidungen oder Maßnahmen erfolgen, so dass es auch keines zentralen Registers bedürfe. Das AZR habe eine andere Funktion als die dezentralen Meldebehörden, die vorrangig Daten von Deutschen (aber auch von Ausländern) speichern. Die Unterstützung von Behörden durch das AZR habe einen spezifisch **ausländer- bzw. asylrechtlichen Bezug.** Der Gesetzgeber habe im Rahmen des Gleichheitsgrundsatzes einen weiten Gestaltungsspielraum, der mit dem AZRG ausgeschöpft worden sei.[208]

Der an und für sich weite Ermessens- und Gestaltungsspielraum für den Gesetzgeber bei Ungleichbehandlungen wird jedoch eingegrenzt, wenn, wie bei der Datenverarbeitung im AZR, relevante Grundrechtsauswirkungen bestehen.[209] Eine Diskriminierung ist nicht nur gegeben, wenn jemand wegen seiner Staatsangehörigkeit einer sachlich nicht gerechtfertigten körperlichen Sonderbehandlung unterworfen wird. Eine Diskriminierung liegt schon im Vorfeld einer solchen Behandlung vor, nämlich wenn zwecks einer solchen Sonderbehandlung

[203] *Bäcker*, GFF-Gutachten, 2022, S. 27 f.
[204] *Bäumler* NVwZ 1995, 242; *ders.* BewHi 1996, 244, 246; 15. TB LfD Saar 1993/94, 30; 2. TB SächsDSB 1994, 86 f.; dagegen *Streit/Srocke* ZAR 1999, 110 ff.
[205] *Wollenschläger* ZAR 1994, 10 f.; *Frankenberg*, FS Simitis, S. 114 ff.
[206] Nachweise bei *Weichert*, AZRG, Einführung, Rn. 39.
[207] So aber *Bäcker*, GFF-Gutachten, 2022, S. 37.
[208] *Streit/Heyder*, AZR-Gesetz, Einf. Rn. 16.
[209] BVerfG 30.05.1990 – 1 BvL 2/83 u.a., BVerfGE 82, 146; *Bäumler* NVwZ 1995, 239; *Maas* NVwZ 1988, 18 ff.

eine informationelle Erfassung erfolgt, wenn also jemand deshalb schärfer überwacht wird.[210] **Diskriminierung durch Überwachung** erfolgt nicht nur dadurch, dass unnötigerweise mehr Daten als erforderlich gespeichert werden, sondern auch dadurch, dass diese Daten über das erforderliche Maß hinaus verarbeitet, z.B. abgefragt oder übermittelt werden. Dies ist gerade beim AZR mit seinen umfangreichen und schwer eingrenzbaren Abruf- und Verarbeitungsmöglichkeiten der Fall.[211]

Der EuGH stellte 2008 fest, dass die damals erfolgende AZR-Datenverarbeitung eine nicht gerechtfertigte Diskriminierung von sonstigen **Unionsbürgern** gegenüber Deutschen darstellt, soweit diese über die aufenthaltsrechtliche Funktion des AZR hinausgeht.[212] Die Prüfung des EuGH beschränkte sich auf die Frage der Diskriminierung anderer Unionsbürger und betraf nicht Drittstaatsangehörige. Gemäß Art. 21 Abs. 2 GRCh ist aber jede Diskriminierung aus Gründen der Staatsangehörigkeit verboten. Anknüpfungspunkt der Differenzierung im AZR zwischen Unionsbürgern und Drittstaatlern ist die Staatsangehörigkeit.

Diskriminierende Überwachung basiert darauf, dass eine Datenverarbeitung vorgenommen wird, obwohl sie nicht erforderlich ist. Die **Erforderlichkeit einer Datenverarbeitung** lässt sich zwar oft nicht eindeutig feststellen, da eine Datenspeicherung im Hinblick auf einen künftigen Bedarf erfolgt, der wegen seiner Entstehung in der Zukunft nicht präzise festgelegt werden kann. Allerding ist eine Diskriminierung unzweifelhaft gegeben, wenn im Einzelfall die vorgenommene Verarbeitung unter keinen Umständen erforderlich sein kann, etwa weil sie nicht in den Aufgabenbereich einer Behörde fällt. Sie liegt vor, wenn sie „ins Blaue hinein“ und „für alle Fälle“ erfolgt.[213] Zur Rechtfertigung einer Verarbeitung genügt es nicht, dass ein Bedarf irgendwie möglich erscheint. Vielmehr bedarf es hierfür einer gewissen Wahrscheinlichkeit, mit der eine Notwendigkeit angenommen werden kann. Diese Wahrscheinlichkeit kann sich durch Zeitablauf verändern, etwa durch einen langjährigen Aufenthalt in der Bundesrepublik oder in Europa, ohne dass sich ein Bedarf an einer Verarbeitung ergeben hätte (zur fehlenden Erforderlichkeit von Verarbeitungsbefugnissen s.o. 7).

Eine Diskriminierung ist insbesondere dann anzunehmen, wenn eine Verarbeitung **gravierende Folgen** für die Betroffenen haben kann. Dies ist insbesondere bei der Nutzungsmöglichkeit durch Sicherheitsbehörden der Fall. So ist nicht nur bei einem gesicherten Aufenthalt wegen Unionsbürgerschaft von einer Diskriminierung auszugehen[214], sondern auch bei einem gesicherten langjährigen unbescholtenen Aufenthalt. Die Erwägung

[210] EuGH 29.10.1980 – C-22/80 Rn. 9 [Bussac], NJW 1981, 513; *Weichert* in *Heldmann*, AuslG, 2. Aufl. 1993, §§ 75–80 Rn. 7.
[211] VG Köln 28.11.2002 – 20 K 10510/00, Rn. 39.
[212] EuGH 16.12.2008 – C-524/06, NVwZ 2009, 378 = EuZW 2009, 183 = MMR 2009, 171 = DVBl 2009, 171 = ZAR 2009, 197.
[213] BVerfG 02.03.2010 – 1 BvR 256/08 u.a. Rn. 218; *Weichert*, vorgänge Nr. 227 [3/2019], 62.
[214] EuGH 16.12.2008 – C-524/06, Rn. 46, 66, 73.

des Schutzes von öffentlicher Sicherheit und Ordnung kann und darf dann keine Rolle mehr spielen.[215]

Es wurde schon dargestellt, dass die Notwendigkeit einer **lückenlosen Meldekette** zur Begründung der Erforderlichkeit des AZR bei Ausländern, die ihren Lebensmittelpunkt in Deutschland gewählt haben, nicht begründet ist (s.o. 7). Demnach gibt es für diese Personengruppe auch keine Rechtfertigung für die ungleiche Behandlung gegenüber Deutschen.

Die Ungleichbehandlung bei der Unterstützungsfunktion des AZR für andere öffentliche Stellen, die nicht speziell mit der Durchführung ausländer- oder asylrechtlicher Vorschriften betraut sind, wird sachlich damit gerechtfertigt, dass bei Ausländern, die nicht in Deutschland geboren sind, i.d.R. keine Möglichkeit bestehe, beim Geburtsstandesamt Informationen einzuholen.[216] Dieser Nachweis dient insbesondere einer **eindeutigen Identifizierung** der Betroffenen. Diese Überlegung rechtfertigt allenfalls eine Ungleichbehandlung der Ausländer, die nicht in der Bundesrepublik geboren worden sind und beschränkt diese auf die Identifizierungsfunktion des AZR. In den Mitgliedstaaten der EU sowie einer Vielzahl weiterer Staaten bestehen keine nennenswerten Probleme bei der Beschaffung von Geburtsnachweisen. Ist die Identifizierungsfunktion für die EU oder in Deutschland durch anderweitige Vorkehrungen erfüllt, ist der Rückgriff auf ein Geburtsstandesamt und alternativ auf das AZR nicht mehr nötig.

Grundsätzlich ist eine Ungleichbehandlung sachlich begründbar, wenn mit dem AZR ausländer- und asylrechtliche Zwecke verfolgt werden, die am **aufenthaltsrechtlichen Status** von Ausländern bzw. an dem explizit nur Deutschen und Unionsbürgern gewährten Recht auf Freizügigkeit (Art. 11 GG, Art. 45 Abs. 1 GRCh) anknüpfen. Dies gilt auch, wenn vom Aufenthaltsrecht des Ausländers, das über Verwaltungsakt verliehen wird, das aber auch erlöschen bzw. entzogen werden kann, Entscheidungen anderer öffentlicher Stellen abhängen (z.B. Erwerbstätigkeit, Arbeitsaufnahme, Sozialleistungen). Eine Ungleichbehandlung durch AZR-Datenverarbeitung ist unzulässig, wenn die Daten für Entscheidungen herangezogen werden, bei denen es nicht ausdrücklich auf den Aufenthaltsstatus ankommt. Der Umstand, dass im Rahmen einer Ermessensentscheidung auch der Aufenthaltsstatus berücksichtigt werden kann, legitimiert allenfalls in einem besonders zu begründenden Einzelfall die mit einem Grundrechtseingriff verbundene AZR-Datenverarbeitung.

Es ist abwegig, die AZR-Speicherung als **freizügigkeitsfördernd** anzusehen. Das europarechtliche Diskriminierungsverbot bezieht sich nicht nur auf das Verbot der Einschränkung der Freizügigkeit, sondern auf die Beachtung des Gleichheitsgrundsatzes generell. Daher können ARZ-Speicherungen zu Personen mit einem längeren gesicherten

[215] VG Köln 28.11.2002 – 20 K 10510/00 Rn. 66.
[216] *Streit/Heyder*, AZR-Gesetz, 1997, Einf. Rn. 16.

Aufenthalt und unbescholtener Lebensführung einen Verstoß gegen Art. 21 Abs. 2 GRCh und gegen Art. 3 GG darstellen.

In Bezug auf Angehörige anderer EU-Staaten wurden Ungleichbehandlungen im Vergleich zu Deutschen erst nach einer Entscheidung des EuGH aufgehoben.[217] Nicht gerechtfertigte Ungleichbehandlungen zwischen EU-Bürgern und Drittausländern blieben bestehen. Eine **nicht sachlich begründete Ungleichbehandlung** durch das AZRG liegt in folgenden Umständen[218]:

- Anders als für Deutsche wird das AZR nicht dezentral, sondern als bundesweites **zentrales Melderegister** geführt und dadurch werden z.B. von Drittausländern Wohnadressen zentral beauskunftet (§ 3 Abs. 1 Nr. 5c, 5d, s.o. 7.1).

- Die **Multifunktionalität und Zweckunbestimmtheit** des AZR kennt keine Entsprechung bei Datenspeicherungen über Deutsche. Die Nutzung des AZR für andere als ausländer- und asylrechtliche Zwecke ist eine ungerechtfertigte Ungleichbehandlung gegenüber Deutschen. Dies gilt in besonderem Maße für Sicherheitszwecke (s.o. 5),[219] aber auch im Hinblick auf Datenübermittlungen an Luftsicherheitsbehörden und atomrechtliche Aufsichtsbehörden zur Durchführung von Zuverlässigkeitsüberprüfungen (§ 15 Abs. 1 Nr. 3 u. 3a AZRG).[220]

- Mit der **AZR-Nummer** besteht, anders als bei Deutschen, für die Nutzung des AZR außerhalb ausländer- und asylrechtlicher Zwecke ein Instrument zur Zusammenführung persönlicher Daten. Weder die oft ungewöhnliche Schreibweise ausländischer Namen noch eine besondere Mobilität von Ausländern sind ausreichend legitimierende Sachgründe für eine ausnahmslose Nutzung dieser nationalen Kennziffer (s.o. 3.3).

- Die Nutzung des AZR als **besonderes (Vorfeld-)Ermittlungsinstrument** in Zusammenhang mit von Ausländern ausgehender Kriminalität durch Speicherung der Anlässe nach § 2 Abs. 2 Nr. 7, 7a AZRG beruht auf keiner sachlichen Differenzierung (s.o. 5.1).[221]

- **Suchvermerke** nach § 5 AZRG sind gegenüber den meisten Unionsbürgern unzulässig (s.o. 4.4, 5.3).[222]

[217] EuGH 16.12.2008 – C-524/06, NVwZ 2009, 378.
[218] *Frankenberg*, FS Simitis, S. 116 ff.
[219] *Bäcker*, GFF-Gutachten, S. 42 ff.
[220] *Bäcker*, GFF-Gutachten, S. 43.
[221] *Weichert* in GK-AufenthG, § 2 AZRG Rn. 96, 97.
[222] *Weichert* in GK-AufenthG, § 5 AZRG, Rn. 7.

- Die undifferenzierte Übermittlungsmöglichkeit an öffentliche Stellen bzgl. der **Grunddaten ohne Zweckangabe** nach den §§ 10, 14 AZRG ist eine nicht zu rechtfertigende Ungleichbehandlung gegenüber Unionsbürgern.[223]

- **Gruppenauskünfte** nach § 12 AZRG gehen weit über das hinaus, was nach §§ 98a f. StPO, Polizeirecht oder sonstigen Regelungen an Datenabgleich generell zulässig ist (s.o. 5.2). Hierin liegt eine nicht gerechtfertigte Ungleichbehandlung gegenüber EU-Bürgern.[224]

- Eine Übermittlungsmöglichkeit **zwischen Sicherheitsbehörden** über eine Abfrage im AZR nach § 15 Abs. 1 AZRG, ohne dass eine direkte Übermittlung zugelassen ist, besteht nicht in Bezug auf Deutsche und Unionsbürger.[225]

- Die in den §§ 18a, 18b AZRG vorgesehene Datenübermittlung an **Leistungsbehörden** stellt eine ungerechtfertigte Ungleichbehandlung von Ausländern gegenüber Deutschen dar, soweit nicht spezifische ausländerrechtlich relevante Umstände ermittelt werden.[226]

- Nach § 16 erhalten sämtliche **Gerichte** Zugriff auf sämtliche AZR-Daten von Ausländern. Derartige Zugriffe auf die Daten von Deutschen bestehen hingegen nicht.

- Umfassende Online-Zugriffsmöglichkeiten, insbesondere durch sog. Sicherheitsbehörden, nach § 22 AZRG gibt es nicht in Bezug auf deutsche Staatsbürger.[227]

10 Transparenz und sonstige Betroffenenrechte

Art. 8 Abs. 2 S. 2 GRCh spricht jedem Menschen das Recht zu, „Auskunft über die ihn betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken“. Diese Ausgestaltung des Grundrechts auf Datenschutz findet auch im Grundrechtsschutz des Grundgesetzes eine Grundlage: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“[228] Hieraus ergeben sich Transparenzpflichten für die Verantwortlichen und **Rechte der Betroffenen** gegenüber diesen. Die Rechte der Betroffenen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten im AZR sind in der DSGVO insbesondere in den Art. 12-23 geregelt. Das AZRG enthält dazu konkretisierende Regelungen (§§ 34, 35-38).

[223] *Weichert* in GK-AufenthG, § 10 AZRG Rn. 11.
[224] *Bäumler* BewHi 1996, 246; *ders.* NVwZ 1995, 242; *ders*. DuD 1994, 541; *Bäcker*, GFF-Gutachten, 2022, S. 45.
[225] *Bäcker*, GFF-Gutachten, 2022, S. 42.
[226] *Bäcker*, GFF-Gutachten, 2022, S. 46,
[227] *Weichert* in GK-AufenthG, § 22 AZRG Rn. 9.
[228] BVerfG 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 422.

Gemäß Art. 5 Abs. 1 lit. a DSGVO ist es für die Grundrechtskonformität personenbezogener Datenverarbeitung von zentraler Bedeutung, dass diese „in einer für die betroffene Person **nachvollziehbaren Weise**“ erfolgt. Der Transparenzgrundsatz findet in vielen Regelungen der DSGVO seinen Ausdruck, insbesondere im Auskunftsanspruch des Art. 15 DSGVO, der in § 34 AZRG aufgegriffen wird, sowie in den Art. 12-14 DSGVO zu den Informationspflichten.

Neben den Ansprüchen auf Transparenz bestehen grundsätzlich für die Betroffenen folgenden **individuellen Möglichkeiten** der Durchsetzung ihrer Datenschutzrechte:

- Recht auf Berichtigung (Art. 16 DSGVO, § 35 AZRG),
- Recht auf Löschung (Art. 17 DSGVO, § 36 AZRG),
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO, § 37 AZRG),
- Recht auf Unterrichtung (Art. 19 DSGVO, § 38 AZRG),
- Widerspruchsrecht (Art. 21 DSGVO),
- Recht auf Schadenersatz (Art. 82 DSGVO),
- Recht auf Befassung des Datenschutzbeauftragten (Art. 38 Abs. 4 DSGVO),
- Recht auf Beschwerde bei einer Aufsichtsbehörde (Art. 77 DSGVO),
- Recht auf wirksamen gerichtlichen Rechtsbehelf (Art. 78, 79 DSGVO).

10.1 Informationspflichten

Eine Konkretisierung der Art. 12-14 DSGVO erfolgt im AZRG nicht. Diese Regelungen sind direkt auf die Datenverarbeitung im AZR anwendbar. Gemäß Art. 12 Abs. 1 S. 1 DSGVO muss die Information gegenüber den Betroffenen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ erfolgen. Ein wesentlicher Zweck der Information besteht darin, den Betroffenen die Ausübung ihrer Rechte zu ermöglichen (Art. 12 Abs. 2 S. 1 DSGVO).

Die Transparenzfunktion kann bei Ausländern, die zum Zeitpunkt der AZR-Speicherung möglicherweise noch wenig Kontakt mit der deutschen Sprache hatten, durch eine deutschsprachige Information oft nicht erfüllt werden. Angesichts dessen besteht die staatliche Pflicht, die Informationen nach Art. 12-14 DSGVO in der **Muttersprache** vorzunehmen, soweit dies für die verantwortliche Stelle möglich und zumutbar ist.[229] Es dürfte dem BAMF oder den sonstigen informationspflichtigen Behörden schwerfallen, in jeder Muttersprache der Betroffenen die geforderten Informationen zu erteilen. Zumutbarkeit bedeutet, dass das BAMF bei Nichtverfügbarkeit der Muttersprache Vermittlungsversuche in einer anderen Sprache vorzunehmen hat, die für die informationspflichtige Stelle verfügbar und für den Betroffenen verständlich ist.[230] Dies ist oft über eine Weltsprache, etwa Englisch,

[229] *Dix* in *Simitis/Hornung/Spiecker*, Art. 12 Rn. 15.
[230] *Greve* in *Sydow*, Europäische Datenschutz-Grundverordnung, 2017, Art. 12 Rn. 13.

Spanisch oder Französisch möglich und muss dem Betroffenen entsprechend angeboten werden.

Die Speicherung im AZR wird durch eine Übermittlung dritter Stellen bewirkt. Anwendbar ist Art. 14 DSGVO. Die Informationspflicht obliegt dem **Verantwortlichen**, also hier dem BAMF; sie kann aber auch durch die direkt die Daten erhebende und an das AZR übermittelnde Stelle erfüllt werden. In diesem Fall muss sich das BAMF vergewissern, dass die anliefernde Stelle der Informationspflicht genügt (vgl. Art. 15 Abs. 5 lit. a DSGVO).

Keine aktive Informationspflicht besteht nach Art. 14 Abs. 5 lit. c DSGVO, wenn die Erlangung der Information durch **Rechtsvorschriften ausdrücklich geregelt** ist. Dies ist bei der Datenverarbeitung durch das AZR über das AZRG der Fall. Voraussetzung ist aber weiterhin, dass diese Rechtsvorschriften „geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen". Dem Unionsgesetzgeber ging es darum, dass die Betroffenen eine hinreichende Kenntnis von der Datenverarbeitung haben können.[231] Ist die Rechtsvorschrift völlig fremd und ist den Betroffenen wegen ihrer Fremdheit zur deutschen Rechtsordnung die Art der Verarbeitung unbekannt, so wie dies bei dem im AZR gespeicherten Klientel oft der Fall ist, bleibt die Pflicht zur Information der Betroffenen beim Vorliegen einer Rechtsvorschrift bestehen.[232]

Aus dem Vorgesagten ergibt sich, dass das BAMF als verantwortliche Stelle das ihr Zumutbare unternehmen muss, um sicherzustellen, dass die Betroffenen über die Datenverarbeitung im AZR sowie über ihre Datenschutzrechte informiert werden. Diese **Informationspflicht umfasst** Angaben zum Verantwortlichen selbst und dessen Datenschutzbeauftragten, die Zwecke und Datenkategorien sowie hier insbesondere die „Kategorien der Empfänger" (Art. 14 Abs. 1 lit. a-e DSGVO). Als Mindestmaßnahme zum Nachweis der Betroffeneninformation besteht eine Dokumentationspflicht, wie diese im Einzelfall erteilt wurde bzw. prozessual generell erteilt wird. Um spezifische Informationen auf Anfrage erlangen zu können, benötigt der Betroffene zur Datenverarbeitung zumindest Grundinformationen. Besonders wirksam ist ein solches Angebot beim AZR, wenn dem Betroffenen regelmäßig, z.B. einmal im Jahr, eine Übersicht über die erfolgten Datenübermittlungen zur Verfügung gestellt wird.

10.2 Auskunftsanspruch

Der Auskunftsanspruch ist in § 34 AZRG normiert, der in Abs. 1 auf Art. 15 DSGVO verweist. Dadurch erhält der Betroffene die Informationen, die er zur Durchsetzung seiner datenschutzrechtlichen Ansprüche auf Datenkorrektur (Berichtigung, Löschung, Einschränkung der Verarbeitung, §§ 35 bis 37 AZRG) oder auf Schadenersatz (Art. 82 DSGVO) benötigt.

[231] *Dix* in *Simitis/Hornung/Spiecker*, Art. 14 Rn. 27; *Bäcker* in *Kühling/Buchner*, Art. 14 Rn. 65, 67.
[232] Zum alten Recht *Frankenberg*, FS Simitis, S. 110 ff.

Der Antragsteller muss zum Beleg seiner Auskunftsberechtigung gem. § 15 Abs. 2 S. 3 AZRG-DV seine **Identität nachweisen.** Zur Vermeidung von Falschauskünften wird der Antragsteller nach § 34 Abs. 1 S. 2 AZRG verpflichtet, seine Grundpersonalien anzugeben. § 15 Abs. 2 S. 1 AZRG-DV sieht zudem zwingend Schriftlichkeit des Auskunftsantrags vor. Tz. 34.1 AZR-VV sieht den Identitätsnachweis durch Beglaubigung vor. Für den Identitätsnachweis bei der Wahrnehmung der Rechte des Betroffenen muss es nach europäischem Recht dagegen genügen, dass die Identität glaubhaft gemacht wird (Art. 12 Abs. 2 u. 6 DSGVO).[233] Die bestehenden formalen Anforderungen für eine AZR-Auskunft können bei einer wortgetreuen Anwendung die Betroffenen vom Auskunftsanspruch ausschließen, etwa wenn sie nicht über alle Grundpersonalien nach § 3 Abs. 1 Nr. 4 AZRG verfügen oder nicht in der Lage sind, selbst einen schriftlichen Antrag zu stellen oder eine amtliche Beglaubigung vorzulegen.[234]

Nach § 34 Abs. 2 Nr. 2 AZRG wird die Auskunft verweigert, wenn sie die **öffentliche Sicherheit oder Ordnung** gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde (vgl. ebenso § 34 Abs. 1 Nr. 1 i.V.m. § 33 Abs. 1 Nr. 1b BDSG). Angesichts der grundrechtlichen Bedeutung des Auskunftsanspruchs kann ein Verweis auf die öffentliche Ordnung eine Auskunftsverweigerung nicht rechtfertigen.[235] Eine solche Auskunftseinschränkung ist unverhältnismäßig[236] und ist von Art. 23 Abs. 1 DSGVO nicht abgedeckt.[237] Nachteile für das Wohl des Bundes oder eines Landes können nur dann relevant sein, wenn mit ihnen zugleich eine Gefahr für die öffentliche Sicherheit verbunden ist, da nur dies als eigenständiger Ausnahmegrund in Art. 23 Abs. 1 DSGVO aufgeführt ist.[238]

Eine Auskunftsverweigerung ist gemäß dem Gesetz zulässig, wenn die Daten **„ihrem Wesen nach“** geheim gehalten werden müssen. Damit werden Fallgestaltungen erfasst, bei denen insbesondere Drittinteresse betroffen sind, die gesetzlich geschützt wird (z.B. § 1758 BGB, § 61 Abs. 2 PStG). Angesichts der bestehenden großen Unbestimmtheit der Formulierung bei der Einschränkung des Rechts auf informationelle Selbstbestimmung kann die Regelung nicht angewendet werden, wenn es um den Schutz von nicht durch Rechtsvorschrift geregelten öffentlichen Geheimhaltungsinteressen geht.[239]

Stammen die AZR-Daten von deutschen Nachrichtendiensten, den Polizeivollzugsbehörden oder den Staatsanwaltschaften, so muss nach § 34 Abs. 3 AZRG vor der Auskunftserteilung hierfür die **Einwilligung bei diesen Stellen** eingeholt werden. Entsprechendes gilt, soweit Auskunft über diese Stellen oder Gerichte als Datenempfänger gegeben werden soll. Einwilligung bedeutet Zustimmung. Mit der Regelung soll verhindert werden, dass Betroffene

[233] *Ehmann* in *Ehmann/Selmayr*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 15 Rn. 24; *Dix* in *Simitis/Hornung/Spiecker*, Art. 12 Rn. 36.
[234] Zu den praktischen Auskunftsdefiziten beim AZR GFF, Das Ausländerzentralregister, 2022, 11 f.
[235] XII. TB LfD Nds. 1993/94, 110.
[236] *Weichert*, AZRG, § 34 Rn. 18.
[237] *Golla* in *Kühling/Buchner*, § 32 Rn. 13.
[238] *Golla* in *Kühling/Buchner*, § 32 Rn. 14
[239] *Weichert* in *Däubler u.a.*, § 29 Rn. 4-6.

über den Umweg einer AZR-Auskunft Informationen erhalten, die ihnen bei einem entsprechenden Antrag bei der jeweiligen Stelle vorenthalten würden. Den Sicherheitsbehörden soll das Entscheidungsrecht über sie betreffende und von ihnen angelieferte Daten bewahrt bleiben. Ist die Verweigerung der Einwilligung unbegründet bzw. nicht gerechtfertigt, so kann und muss sich die Registerbehörde als Verantwortliche über diesen Umstand hinwegsetzen. Für die Auskunftsverweigerungsgründe kann ausschließlich auf den Rahmen der DSGVO zurückgegriffen werden. Dies geht nicht klar aus dem Gesetzeswortlaut hervor.

10.3 Datencockpit

Ein **Datencockpit** soll es künftig gemäß § 10 OZG Betroffenen ermöglichen, über ein Internetportal Auskünfte zu Datenübermittlungen „unter Nutzung einer Identifizierungsnummer“ (ID-Nummer, § 9 Abs. 1 IDNrG) zu erhalten, die sich aus den Protokollierungen der Übermittlung ergeben. Die nach § 139b AO erstellte ID-Nummer wird nach der Übermittlung durch die Registermodernisierungsbehörde (§ 6a AZRG) im AZR parallel zur AZR-Nummer gespeichert (§ 3 Abs. 5 AZRG). Da eine Datenübermittlung nach § 10 Abs. 2 S. 1 AZRG nicht zwingend durch Identifizierung auf der Grundlage der ID-Nummer, sondern alternativ weiterhin der AZR-Nummer möglich ist, ist auch nach Etablierung des Datencockpits nicht gewährleistet, dass die Betroffenen über dieses Portal Auskunft zu den sie betreffenden Datenübermittlungen erlangen können. Es ist rechtlich geboten, schon vor Einführung des Datencockpits zur ID-Nummer einen solchen zur AZR-Nummer einzuführen. Damit ist zugleich in einem überschaubaren Rahmen die Erprobung eines Datencockpits möglich.[240]

10.4 Widerspruchsrecht

Das **Recht auf Widerspruch** ist im AZRG nicht geregelt und ergibt sich direkt aus Art. 21 DSGVO, da die im AZR erfolgende Verarbeitung auf Art. 6 Abs. 1 lit. e DSGVO beruht. Der Betroffene muss bei der ersten Kommunikation zwischen BAMF und Ausländer auf sein Widerspruchsrecht ausdrücklich hingewiesen werden (Art. 21 Abs. 4 DSGVO, vgl. Art. 14 Abs. 2 lit. c DSGVO). Die betroffene Person kann „aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten“ Widerspruch einlegen. Das BAMF darf dann die Daten im AZR nicht mehr verarbeiten, es sei denn, es „kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen“ (Art. 21 Abs. 1 S. 2 DSGVO).

Kein Widerspruchsrecht besteht, soweit bzgl. der Datenverarbeitung eine rechtliche Verpflichtung besteht (Art. 6 Abs. 1 lit. c DSGVO). Dies gilt für die Datenübermittlung an das

[240] *Weichert*, Stellungnahme v. 24.04.2021, BT-Innenausschuss, A-Drs. 19(4)820 C, 8; tatsächlich bestehen noch keine konkreten Planungen zur Umsetzung des Datencockpits im AZR, BT-Drs. 19/32508, 15.

und die **Speicherung im AZR**, da insofern das AZRG keine Rücksicht auf mögliche schutzwürdige Betroffeneninteressen nimmt, soweit die Daten richtig und zulässig übermittelt wurden. Es besteht ein ausdrücklicher Normbefehl für die Verarbeitung. Dies gilt nicht für falsche, nicht aktuelle oder zu löschende Daten.

Etwas anderes gilt auch für **Übermittlungen aus dem AZR**, für die ein Widerspruch wirksam sein kann. Der Widerspruch des Betroffenen muss sich deshalb auf diese spezifische Form der Verarbeitung beziehen.

Der Widerspruch muss Gründe benennen, die sich aus der **besonderen Situation des Betroffenen** ergeben. Der Betroffene sollte die Gründe so präzise wie möglich darlegen, weshalb die angegriffene Verarbeitung seine Schutzinteressen verletzen. Diese Gründe können in einer individuellen oder familiären Gefährdung liegen, etwa wegen politischer Verfolgung. Unspezifische Einwände gegen eine Übermittlung reichen nicht aus.[241]

10.5 Rechtsschutz

Ausländische Menschen sind häufig der deutschen Sprache nicht oder nur in einem geringen Maße mächtig und 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 Überwachung. Es ist daher wenig erstaunlich, dass sich nur selten ausländische Betroffene an die Datenschutzaufsicht wenden, um ihre Rechte durchzusetzen.[242] Sie haben faktisch, strukturell und kulturell bedingt nur ein sehr begrenzte und manchmal keine Möglichkeit, 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 tatsächlichen Ausgeliefertseins könnte und sollte eine Instanz eingerichtet werden und mit Befugnissen ausgestattet werden, welche die Interessen sowie die Freiheits- und Grundrechte der Nichtdeutschen wahrnehmen kann. Die in den §§ 92-94 AufenthG vorgesehene Einrichtung eines Integrationsbeauftragten hat nur geringe finanzielle und personelle Ressourcen, ist wegen seiner Benennung und seiner hierarchischen Einbindung nicht unabhängig und bzgl. seiner Handlungsmöglichkeiten auf informelle Aktivitäten beschränkt. Es bedarf zusätzlicher, geeigneterer Maßnahmen, um das Grundrecht auf Datenschutz von Nichtdeutschen zu gewährleisten. Hierfür bedarf es einer expliziten gesetzlichen Regelung. Dabei sollte darauf geachtet werden, dass die Einrichtung die Befugnis erhält, **kollektiv Datenschutzverstöße zu reklamieren**.[243] Europarechtlich besteht insofern

[241] *Caspar* in *Simitis/Hornung/Spiecker*, Art. 21 Rn. 7.
[242] 28. TB BfDI 2019, 66.
[243] Art. 80 DSGVO, ausführlich Netzwerk Datenschutzexpertise, Stellungnahme 2. DAVG, 4 f.

eine Grundlage in Art. 80 DSGVO, wofür es aber einer nationalen gesetzlichen Umsetzung bedarf.

11 Spezielle Garantien

Die DSGVO verfolgt das Konzept, dass **besonders intensive Eingriffe** in Grundrechte durch „geeignete Garantien“ oder durch „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ kompensiert werden müssen. Dies gilt für die Verarbeitung sensitiver Daten wie z.B. Gesundheitsdaten oder Angaben über die politische Verfolgung (Art. 9 Abs. 2 lit. g, i DSGVO) sowie für Angaben über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO), für die Datenverarbeitung mit einer nationalen Kennziffer wie der AZR-Nummer (Art. 87 S. 2 DSGVO) oder für privilegierte Datenverarbeitung für Forschungs- und Statistikzwecke (Art. 89 Abs. 1 DSGVO), so wie dies in den §§ 23, 24 und 24a AZRG vorgesehen ist. Entsprechendes gilt nach Art. 6 Abs. 4 lit. e DSGVO), wenn bei der Speicherung der Grundsatz der Zweckbindung aufgehoben wird, so wie dies im AZR generell der Fall ist.

Die Maßnahmen und Garantien haben den Zweck, die besondere Bedrohung, die durch eine spezifische riskante Datenverarbeitung entstehen, soweit zu kompensieren, dass ein angemessenes Verhältnis zwischen Verarbeitungsinteresse und Schutzinteresse der Betroffenen hergestellt wird. Derartige **kompensierende Maßnahmen** müssen sich jeweils an dem besonderen Risiko, das die Garantien nötig macht, orientieren. Es geht darum, dass „Abhilfemaßnahmen“ ergriffen werden, „einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird“ (Art. 35 Abs. 7 lit. d DSGVO).[244]

11.1 Datenschutz-Folgenabschätzung

Wenn die Notwendigkeit für die Durchführung einer **Datenschutz-Folgenabschätzung** besteht, obliegt dem Verantwortlichen, beim AZR also dem BAMF, die Beurteilung, Dokumentation und Verwirklichung der kompensierenden Maßnahmen. Dies ist der Fall, wenn die Verarbeitung „aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ zur Folge hat (Art. 35 Abs. 1 DSGVO). Eine Folgenabschätzung ist u.a. erforderlich, wenn eine „systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen“ oder eine „umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten

[244] Zum alten Recht *Frankenberg*, FS Simitis, S. 113 f.

über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10“ erfolgt (Art. 35 Abs. 3 lit. a u. c DSGVO). Dies ist beim AZR der Fall (s.o. 7.2).

Gemäß Art. 35 Abs. 10 DSGVO besteht die Pflicht zur Durchführung einer Folgenabschätzung nicht, wenn die Verarbeitung auf der Grundlage des Art. 6 Abs. 1 lit. c oder e DSGVO auf einer **nationalstaatlichen Rechtsgrundlage** beruht und „falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte“. Diese Voraussetzungen sind formal beim AZR wegen dem AZRG als Rechtsgrundlage, die auf Art. 6 Abs. 1 lit. c oder e DSGVO zurückgeht, erfüllt. Die Notwendigkeit einer Folgenabschätzung besteht aber nur dann nicht, wenn der Gesetzgeber selbst eine solche Folgenabschätzung vorgenommen hat.[245] Ob dies jeweils der Fall ist, kann der Gesetzesbegründung entnommen werden oder auch der Aufnahme von konkreten risikominimierenden z.B. technischen, organisatorischen oder prozeduralen Anforderungen.[246]

Der Umstand allein, dass ein Gesetzgeber entschieden hat, genügt nicht für die Annahme einer Folgenabschätzung.[247] Dem AZRG ist nicht zu entnehmen, dass von Seiten des **Gesetzgebers eine solche Abschätzung durchgeführt** worden ist. Auch den Gesetzesbegründungen kann nicht im Ansatz Derartiges entnommen werden. Dies gilt sowohl für die Anpassung des AZRG an die DSGVO[248] und ebenso wenig für das 2. DAVG und das AZRWeiterentwG, mit denen eine massive Erhöhung des Risikos für die Betroffenen erfolgt, etwa durch die Privilegierung der Nachrichtendienste beim Datenabruf nach § 20 Abs. 2 AZRG oder durch die generelle Bereitstellung von Dokumenten zum Abruf nach § 6 Abs. 5 AZRG.[249]

In Ermangelung einer gesetzlich vorgenommenen Datenschutz-Folgenabschätzung muss eine solche durch das BAMF durchgeführt werden. Soweit ersichtlich, ist dies bis heute nicht erfolgt. Es handelt sich um einen formellen Verstoß gegen die DSGVO und damit insbesondere auch um eine Verletzung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO.[250] Dieser Verstoß eröffnet dem BfDI die Möglichkeit einer **Sanktionierung** nach Art. 58 Abs. 2 lit. b-g, i, j DSVGO (§ 16 Abs. 1 BDSG). Es ist nicht völlig ausgeschlossen, dass der formelle Verstoß weitergehende Konsequenzen hat, die bis zur Rechtswidrigkeit der Datenverarbeitung gehen können und die einen Lösch- oder Beschränkungsanspruch der Betroffenen nach den Art. 17 Abs. 1 lit. d DSGVO bzw. Art. 18 Abs. 1 DSGVO begründen können.[251]

[245] Kritisch dazu generell *Hansen* DuD 2016, 589.
[246] *Jandt* in *Kühling/Buchner*, Art. 35 Rn. 27.
[247] *Karg* in *Simitis/Hornung/Spiecker*, Art. 35 Rn. 58 f.
[248] BT-Drs. 19/4674.
[249] *Petri*, Stellungnahme v. 28.04.2021, BT-Innenausschuss A-Drs. 19(4)820 A, 8.
[250] *Karg* in *Simitis/Hornung/Spiecker*, Art. 35 Rn. 88.
[251] So EuGH-Vorlagebeschluss des VG Wiesbaden 27.01.2022 – 6 K 2132/19.WI.A Rn. 24-26.

11.2 Technisch-organisatorische Maßnahmen

Gemäß Art. 25 Abs. 1 DSGVO ist das BAMF als Verantwortlicher verpflichtet, „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken (…) geeignete **technische und organisatorische Maßnahmen**“ umzusetzen, „die dafür angelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen“.

Die Erforderlichkeit technisch-organisatorischer Maßnahmen ist in Art. 32 DSGVO geregelt. In Art. 32 Abs. 1 DSGVO werden folgende Vorkehrungen genannt: Pseudonymisierung und Datenverschlüsselung (lit. a), Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer (lit. b), langfristige und andauernde Wahrung der Verfügbarkeit (lit. c), regelmäßige Evaluierung der Maßnahmen (lit. d). Vernichtung, Verlust, Veränderung sowie unbefugter Datenzugang sind zu verhindern (Art. 32 Abs. 2, 4 DSGVO). Das AZRG enthält keine weitergehenden allgemeinen Konkretisierungen. § 22 Abs. 2 BDSG nimmt inhaltlich weitgehend Bezug auf Art. 32 DSGVO und ergänzt den Katalog von Maßnahmen bei der Verarbeitung von sensitiven Daten um die Pflicht zur Protokollierung (Nr. 2), die Sensibilisierung der anwendenden Personen und Stellen (Nr. 3), die Zugangsbeschränkung (Nr. 5) sowie „spezifische Verfahrensregelungen, die im Falle einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung des (Datenschutzrechts) sicherstellen“.[252]

Hinsichtlich der **tatsächlich umgesetzten** technisch-organisatorischen Maßnahmen beim AZR liegen wenig belastbare Informationen vor. Abrufe und Datenänderungen (Meldungen) werden vollständig protokolliert, wobei diese für Kontrollzwecke nur beschränkt auswertbar sind.[253] Jede das Online-Verfahren nutzende Behörde, die an der Kommunikation und am Datenaustausch mit dem AZR teilnimmt, hat ein Zulassungsverfahren zu durchlaufen. Online-Teilnehmer werden durch eine benutzerbasierte Zweifaktor-Authentifizierung identifiziert und erhalten rollenbasierte Berechtigungen. Die Kommunikation und der Datenaustausch erfolgen nach Angaben des BVA gemäß den Standards des Bundesamtes für Informationssicherheit (BSI) und verschlüsselt nach Vorgaben für die Bundesverwaltung.[254] Nähere Angaben hierzu sind bisher nicht bekannt.

[252] *Weichert* DuD 2017, 542.
[253] BfDI, Stellungnahme v. 30.04.2021, BT-Innenausschuss A-Drs. 19(4)823, 2 f.
[254] BVA, Stellungnahmen zum 03.05.2021, BT-Innenausschuss, A-Drs. 19(4)820 B, 3.

12 Das AZRG gemäß übergeordnetem Recht im Wandel

Die Analyse des AZRG ergibt, dass das Gesetz und dessen Umsetzung gegen grundlegende Vorgaben des **Grundgesetzes** und der europäischen **Grundrechte-Charta** sowie gegen die diese Vorgaben umsetzende DSGVO verstoßen. Der Schutz des Grundrechts auf Datenschutz, so wie er vom BVerfG und vom EuGH interpretiert wird, ist nicht gewährleistet. Dies gilt für die grundlegenden Datenschutz-Prinzipien der Zweckbindung, der Bestimmtheit von Grundrechtseingriffen, der Erforderlichkeit und Datenminimierung, der Transparenz bzw. generell der Betroffenenrechte und des Rechtsschutzes.

Diese Verstöße sind im AZRG von Anfang an, also seit 1994, angelegt. In den seitdem erfolgten über 30 Änderungen wurden diese Verstöße immer weiter verschlimmert. Die einzige Korrektur zugunsten Betroffener betrifft eine 2012 vorgenommene Privilegierung von Staatsangehörigen anderer EU-Mitgliedstaaten, die durch ein 2008 ergangenes Urteil des EuGHs erzwungen wurde. Änderungsvorschläge der Verwaltung, also des federführenden Bundesministeriums des Innern bzw. der Bundesregierung, wurden von den jeweiligen Mehrheiten im Bundestag weitgehend kritiklos beschlossen und umgesetzt. Ansätze für ein **verfassungsrechtliches Problembewusstsein** zeigte der Deutsche Bundestag erstmals nach einer Sachverständigenanhörung im Innenausschuss zum AZRWeiterentwG im Mai 2021[255], was zu Änderungen der Regierungsvorlage im Interesse des Betroffenenschutzes führte[256], die grundlegenden Mängel des Gesetzes aber nicht behob.

Dieser Befund ist darauf zurückzuführen, dass die vom AZRG Betroffenen, allen voran die Drittausländer, also die Staatsangehörigen von Nicht-EU-Mitgliedsstaaten, in Deutschland **keine besondere Lobby** haben, dass für die Betroffenen zumeist existenziellere Fragen im Vordergrund stehen und dass sie den ausländerrechtlichen Vollzug und die damit verbundene Datenverarbeitung nicht durchschauen. Datenschutz ist ein Rechtsinstrument moderner westlicher Informationsgesellschaften, zu dem bei dieser Personengruppe häufig trotz ihrer starken Betroffenheit eine kulturelle Distanz besteht.

Diese Rahmenbedingungen unterliegen derzeit einem **grundlegenden Wandel**: Während Ausländerrecht traditionell als spezielles Ordnungsrecht verstanden wurde, führt die Globalisierung der Wirtschaft und des Reiseverkehrs zu einer Entpolizeilichung und einer Fokussierung auf das Aufenthaltsrecht fremder Staatsangehöriger. Die Digitalisierung hat inzwischen die letzten Winkel der Erde erreicht und zugleich weltweit das Bewusstsein für die Notwendigkeit digitaler Grundrechte geschärft. Die Integration der europäischen Staaten verstärkt diese Entwicklung und schafft einen über die nationale Gesetzgebung hinausgehenden rechtlichen Rahmen, der berücksichtigt werden muss. Dabei erweist sich der Umstand, dass digitale Grundrechte in anderen Teilen der Welt keine oder nur eine

[255] Deutscher Bundestag, Ausschuss für Inneres und Heimat, Protokoll-Nr. 19/137, Sitzung am 03.05.2021.
[256] BT-Drs. 19/29820.

untergeordnete Rolle spielen, als Herausforderung. Diese Situation ist ganz besonders Anlass, in Abgrenzung zu autoritären Gesellschaften Grundrechtsorientierung und Rechtsstaatlichkeit als zentrale Bestandteile unserer Verfassungsidentität anzusehen. Das Ausländerrecht und die digitale Ausländerverwaltung stehen insofern besonders im Blick. Hier müssen sich diese Verfassungswerte wegen ihres globalen Bezugs in besonderem Maße bewähren.

Der beschriebene Wandel in der Wahrnehmung des Ausländerrechts und der Grundrechte findet in Deutschland darin seinen besonderen Ausdruck, dass eine **neue Bundesregierung** angekündigt hat, ihre Politik an Themen wie Digitalisierung, Menschenrechtsschutz und Integration neu auszurichten. Zwar wird im Koalitionsvertrag 2021 von SPD, Bündnis 90/Die Grünen und FDP[257] keine Reform des AZR in Aussicht gestellt. Wohl aber bekennt sich die neue Regierungskoalition zu einer Weiterentwicklung der Freizügigkeit in Europa, zu einem Neuanfang in der Integrations- und Migrationspolitik, zu einer Europäisierung der Flüchtlingspolitik und zu einer grundlegenden Reform des Aufenthalts- und Bleiberechts. In diesem Kontext ist es dann unausweichlich, auch eine Reform des AZR vorzunehmen.

Eine solche Reform steht im engen Zusammenhang mit den Plänen der neuen Bundesregierung, die **Digitalisierung der Verwaltung** generell voranzubringen und deren Struktur neu zu ordnen.[258] Bei der geplanten Registermodernisierung kann das AZR nicht außen vor gehalten werden. Vielmehr muss das AZR rechtlich, organisatorisch und informationstechnisch so aufgestellt werden, dass es zum einen in die digitale Verwaltungsstruktur eingebettet wird, zum anderen aber angesichts der kommenden Herausforderungen im Ausländerrecht funktional und entwicklungsfähig ist.

Entwicklungsfähige digitale Verwaltungsstrukturen setzen eine schonungslose, transparente unabhängige **Bestandsaufnahme** voraus. Zwar wurden bei zwei aktuellen Novellen des AZRG Gesetzesevaluationen vorgesehen[259]. Doch sind diese bisher ausschließlich darauf ausgerichtet, die Effizienz neuer Maßnahmen zu messen. Eine grundlegende Bestandsaufnahme und eine umfassende Analyse des AZR ist in den letzten 30 Jahren nicht erfolgt. Daher ist es dringend nötig, eine Gesamtevaluation des AZR vorzunehmen, bevor eine Reform des AZRG begonnen wird. Diese muss ermöglichen, unnötigen Ballast festzustellen und zugleich die Grundrechtswirkungen des Gesetzes und in der Praxis zu untersuchen.

[257] Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und den Freien Demokraten (FDP), Mehr Fortschritt wagen - Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, 2021, S. 137 ff.
[258] Koalitionsvertrag (Fn.195), S. 15.
[259] Art. 13 DAVG v. 02.02.2016, BGBl. I S. 130; 2. DAVG v. 04.08.2019, BGBl. I S. 1131; BMI, Evaluierungsbericht, BT-Drs. 19/17380.

13 AZR-Handlungsbedarf

Unabhängig von den Ergebnissen einer durchzuführenden generellen Evaluierung ergeben sich schon aus der normativen Analyse des AZRG folgende Überarbeitungsbedarfe:

Im Rahmen einer Evaluierung sollte eine umfassende **Datenschutz-Folgenabschätzung** des bestehenden AZR-Verfahrens durchgeführt werden (11.2).

Durch die Europäisierung des Aufenthaltsrechts sollte geprüft werden, ob **freizügigkeitsberechtigte Unionsbürger** weiterhin vom AZRG erfasst sein müssen. Deren Aufenthaltsrecht in Deutschland unterscheidet sich nicht wesentlich von demjenigen deutscher Staatsangehöriger. Insofern kann es genügen, diese Personengruppe – wie Deutsche – ausschließlich melderechtlich zu erfassen (7.1).

Die Verarbeitung der Daten von **Drittausländern mit gesichertem Aufenthalt** bedarf einer umfassenden Reform. Dies gilt zum einen für den zu diesen Personen gespeicherten Datensatz sowie für die Zugriffsmöglichkeit auf diese Daten durch Stellen, die keine ausländer- und asylrechtliche Aufgaben wahrnehmen.

Nach AZR-Einführung der ID-Nummer, für deren Nutzung es Vorkehrungen zum Schutz der Betroffenen gibt, sollte die **AZR-Nummer** entweder ersetzt werden oder in ihrer Funktion auf ein reines Geschäftszeichen reduziert werden. Bis dahin sollte der für die ID-Nummer geplante Datencockpit mit der AZR-Nummer erprobt werden (3.2-3.5, 10.3).

Die **ausländische Personenidentitätsnummer** ist auf ihre Notwendigkeit hin zu überprüfen. Sollten sich tatsächlich Hinweise für deren Notwendigkeit ergeben, so muss der Umgang mit ihr so reguliert werden, dass sich hieraus für die Betroffenen keine zusätzlichen Gefährdungen ergeben. Denkbar sind eine zu dokumentierende Begründungspflicht der Nutzung und eine Markierung mit einem Hinweis auf eine enge Zweckbindung (3.6).

Der Begriff der **Einreisebedenken** ist abschließend, aufzählend und präzise zu bestimmen (6.1).

Bei der Verarbeitung von **Grunddaten** im Rahmen der Identifizierungsfunktion des AZR ist ein gestuftes Verfahren vorzusehen. Alternativ sind diese auf die Grundpersonalien zu beschränken. Darüber hinaus sollte auf die Meldebehörden verwiesen werden. Auch für den Abruf der Grunddaten bedarf es einer Zweckfestlegung (4.2).

Bei potenziell mit der ursprünglichen Datenerhebung in Konflikt stehenden Datenabfragen sind zum Zweck einer **Vereinbarkeitsprüfung** der Sekundärnutzung zumindest ausreichend viele Stichprobenkontrollen unter Rückgriff auf die Originaldaten[260] durchzuführen (4.3).

Die **Bereitstellung von Dokumenten** bzw. Begründungstexten ist auf ihre bisherige Nutzung und die dadurch verursachten Wirkungen in der Verwaltung und für die Betroffenen zu evaluieren. Erweist sich deren Verzichtbarkeit, so sind die Regelungen hierzu zu streichen. Sollte dies nicht möglich sein, so ist zu gewährleisten, dass die Betroffenen über die Bereitstellung sowie über ihre Rechte informiert werden und dass zu deren Schutz prozedurale Vorkehrungen getroffen werden (7.2).

Die Regelung zu den **Suchvermerken** nach § 5 AZRG ist auf ihre bisherige Handhabung, ihre Erforderlichkeit und ihre Wirkung auf die Betroffenen zu evaluieren. Sollte sich dabei herausstellen, dass die Regelung nicht erforderlich ist, so ist sie zu streichen; anderenfalls ist sie materiell und prozedural einzugrenzen (4.4).

Zentrales Anliegen einer AZR-Reform muss es sein, das Register von seinem bisherigen **sicherheitsbehördlichen Ballast** zu befreien. Die weitgehend unbeschränkte Nutzungsbefugnis von AZR-Daten durch Sicherheitsbehörden muss beendet werden (5).

Die Speicherung von **Straftatverdächten** nach § 2 Abs. 2 Nr. 7, 7a AZRG ist ersatzlos zu streichen (5.1, 6.2).

Durch **materiell-rechtliche und prozedurale Vorkehrungen** müssen bei einer sicherheitsbehördlichen Nutzung von AZR-Daten die schutzwürdigen Betroffeneninteressen hinreichend berücksichtigt werden. Dies gilt insbesondere für die Regelungen zu Suchervermerken (5.3, 6.2), zu Gruppenauskünften (Maßnahmen der Rasterfahndung, 5.2) und zum Lichtbild- und Fingerabdruckabgleich (5.4).

Die Verantwortung für die Erhebung und Verarbeitung von identifizierenden Merkmalen (insbesondere Fingerabdrücken) ist vollständig in die Verantwortung des BAMF zu übertragen; die **Amtshilfetätigkeit des BKA** im Ausländerbereich generell ist zu beenden (7.3).

Bei der biometrischen Identifizierung mittels **Fingerabdruck** ist eine Beschränkung auf einen oder zwei Finger (kleiner Finger, Mittelfinger) vorzunehmen (7.4).

Der direkte Zugriff von **Nachrichtendiensten** auf AZR-Daten ist zu evaluieren. Soweit sich dabei ergibt, dass hierüber kein signifikanter Sicherheitsgewinn erzielt wird, sind die Nachrichtendienste von automatisierten Abrufen vollständig auszuschließen. Anderenfalls ist

[260] Zu den Defiziten der bisherigen AZR-Stichprobenkontrollen GFF, Das Ausländerzentralregister, 2022, 14, mit Verweis auf BT-Drs. 19/32508, 10 ff.

durch eine Protokollierung im AZR und eine regelmäßige Kontrolle der Zugriffe sicherzustellen, dass die schutzwürdigen Interessen der Betroffenen gewahrt werden (5.5).

Die Nutzung von AZR-Daten durch **Gerichte** ist zu evaluieren und in jedem Fall zu begrenzen (7.5).

Die Anforderungen an die **Glaubhaftmachung der Identität** bei der Wahrnehmung von Betroffenenrechten ist an die geltende übergeordnete Rechtslage anzupassen (10.2).

Über ein **Datencockpit** sollte den Betroffenen eine Zugangsmöglichkeit zu den zu ihrer Person gespeicherten sowie zu den erfolgten AZR-Abfragen eröffnet werden (10.1, 10.3).

Die **Ausnahmen vom Auskunftsanspruch** sind auf das europarechtlich Zugelassene zu begrenzen (10.2).

Nicht nur im AZRG, sondern im Ausländerrecht generell sollte eine **kollektive Klagemöglichkeit** gegen unzulässige Verfahrensweisen eingeführt werden, die einer unabhängigen Vertretungsinstanz zugewiesen wird (11.3).

14 Abschließende Bemerkungen

Das AZR ist eine der größten Verwaltungsdateien in Deutschland, die zugleich wohl die geringste öffentliche Aufmerksamkeit genießt. Darin werden Menschen gespeichert, in großenteils zu besonders vulnerablen Gruppen gehören. Dies hat weder den Gesetzgeber noch die Verwaltungspraxis davon abgehalten, grundrechtliche und rechtsstaatliche Standards zu ignorieren. Deutschland hat den Anspruch, ein von **Menschenrechten und Toleranz** geprägtes Land zu sein. Um diesem Anspruch gerecht zu werden, muss das AZR aus seinem Schattendasein und aus seiner Verfassungs- und Europarechtswidrigkeit herausgeholt werden.

Um dies zu erreichen, sollte nicht erst darauf gewartet werden, dass ein Betroffener sich durch Instanzen klagt, um letztlich vor einem obersten Gericht auf Bundes- oder europäischer Ebene Recht zu bekommen. Das vorliegende Gutachten hat den Anspruch, die bestehenden Schwachstellen aufzuzeigen und Vorschläge zu machen, wie diese beseitigt werden können. Dies geht nicht ohne eine breite **öffentliche Debatte**. Grundlage dieser Debatte sollte nicht nur das vorliegende Gutachten sein. Diese rechtliche Begutachtung stößt immer wieder dort an Grenzen, wo es darum geht, die gelebte Realität des AZR zu bewerten, von der bisher nur wenig bekannt ist.

Daher sollte die neue Bundesregierung, bevor sie eine Reform des AZRG in Angriff nimmt, zunächst eine unabhängige wissenschaftlich fundierte Bestandsaufnahme der AZR-Praxis vornehmen. Diese muss dann aber ohne großen Verzug in eine umfassende Neukonzeption des AZR münden, mit der eine **Überarbeitung und Modernisierung des AZRG** einhergeht.

Literatur

Bäcker, Matthias, Verfassungs- und unionsrechtliche Bewertung des Ausländerzentralregisters – Rechtsgutachten im Auftrag der Gesellschaft für Freiheitsrechte, 13.01.2022, https://freiheitsrechte.org/home/wp-content/uploads/2022/01/Rechtsgutachten-Auslaenderzentralregistergesetz.pdf

Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hrsg.), Handbuch des Polizeirechts, 6. Aufl. 2018.

Bäumler, Helmut, Kritische Anmerkungen zum Ausländerzentralregister, BewHi 1996, 240-249.

Bäumler, Helmut, Datenschutz für Ausländer, NVwZ 1995, 239

Bäumler, Helmut, Datenschutz für Ausländer, DuD 1994, 540

Bergmann, Jan/Dienelt, Klaus, Ausländerrecht, 13. Aufl. 2020.

Breitkreutz, Katharina/Franßen-de la Cerda, Boris/Hübner, Christoph, Das Richtlinienumsetzungsgesetz und die Fortentwicklung des deutschen Aufenthaltsrechts, ZAR 2007, 341-347.

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), Stellungnahme zum Entwurf eines Zweiten Datenaustauschverbesserungsgesetzes, 18.02.2019, Deutscher Bundestag, Ausschussdrucksache 19(4)271 B.

Callies, Christian/Ruffert, Matthias (Hrsg.), EUV/AEUV, 5. Aufl. 2016.

Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke, EU-DSGVO und BDSG, 2. Aufl. 2020 (Däubler u.a.).

Frankenberg, Günter, Gutachten und Verfassungsbeschwerde gegen das Ausländerzentralregistergesetz (AZRG), Hrsg.: Arbeitsgemeinschaft der Ausländerbeiräte Hessen (AGAH), 1995.

Frankenberg, Günter, Datenschutz und Staatsangehörigkeit, in: *Simon, Dieter/Weiss, Manfred* (Hrsg.), Zur Autonomie des Individuums, Liber Amicorum Spiros Simitis, Baden-Baden 2000, 99-120.

Geffken, Rolf, Ausländerzentralregister und Verfassungsbeschwerde, Informationsdienst zur Ausländerarbeit, 1988, 50-56.

Gemeinschaftskommentar-Aufenthaltsrecht, Hrsg.: *Berlit, Uwe*, Loseblattsammlung, Stand Juni 2021 (GK-AufenthG).

Gesellschaft für Freiheitsrecht (GFF, Hrsg., Autorin *Sarah Lincoln*), Das Ausländerzentralregister – eine Datensammlung ausser Kontrolle, 2022, https://freiheitsrechte.org/home/wp-content/uploads/2022/01/Studie_Auslaenderzentralregister.pdf.

Hailbronner, Kay, Die Speicherung personenbezogener Daten von Unionsbürgern im AZR, ZAR 2009, 178-182.

Heyder, Udo, Zum Gesetz über das Ausländerzentralregister, ZAR 1994, 153-157.

Hofmann, Rainer M., Ausländerrecht, 2. Aufl. 2016.

Huber, Berthold (Hrsg.), Aufenthaltsgesetz, Kommentar, 1. Aufl. 2010.

Huber, Berthold, Die Änderungen des Ausländer- und Asylrechts durch das Terrorismusbekämpfungsgesetz, NVwZ 2002, 787

Jacob, Joachim, Staatsangehörigkeitsdatei, DuD 1997, 68.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung/BDSG, 2. Aufl. 2018.

Mühlbauer, Holger, Kontinuitäten und Brüche in der Entwicklung des deutschen Einwohnermeldewesens, 1995.

Netzwerk Datenschutzexpertise, Stellungnahme zum Gesetzentwurf der Bundesregierung zur Verbesserung der Registrierung und des Datenaustauschs zu aufenthalts- und asylrechtlichen Zwecken (Zweites Datenaustauschverbesserungsgesetz – 2. DAVG) v. 9.5.2019, Deutscher Bundestag Ausschussdrucksache 19(4)271 A.

Parusel, Bernd/Schneider, Jan, Migrationspolitik und Migrationskontrolle – Möglichkeiten und Erkenntnisse der deutschen Visumstatistik, ZAR 2013, 12-19.

Petri, Thomas (Der Bayerische Landesbeauftragte für den Datenschutz). Öffentliche Anhörung zum Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Weiterentwicklung des Ausländerzentralregisters, BT-Drucksache 19/28170; Stellungnahme, v. 28.04.2021, Deutscher Bundestag, Innenausschuss, A-Drs. 19(4)820 A.

Pollähne, Helmut, AZR- Die Totalerfassung der Ausländer, Forum Recht 3/1988, 287-290.

Reichert, Mathias, Das geplante Ausländerzentralregister-Gesetz – Eine Erwiderung, ZAR 1990, 66-68.

Scheuerer, Franz, Immigranten und Flüchtlinge – die gläsernen Menschen, in *Appel, Roland/Hummel, Dieter* (Hrsg.) Vorsicht Volkszählung, 3. Aufl. 1987, S. 171-179.

Schriever-Steinberg, Angelika, Das Ausländerzentralregister, NJW 1994, 3276 f.

Schriever-Steinberg, Angelika, Das geplante Ausländerzentralregister-Gesetz, ZAR 1990, 62-66.

Schriever-Steinberg, Angelika, Nochmals: Das geplante Ausländerzentralregister-Gesetz, ZAR 1990, 68 f.

Schwarze, herausgegeben von *Becker/Ulrich/Hatje, Armin/Schoo, Johann/Schwarze, Jürgen*, EU-Kommentar, 4. Aufl. 2019.

Simitis, Spiros/Hornung, Gerrit/Spieker genannt Döhmann, Indra (Hrsg.), Datenschutzrecht, 2019.

Streit, Christian, Datenschutzregelungen des Ausländerzentralregistergesetzes, DuD 1994, 559-568.

Streit, Christian, Die Auswirkungen des Terrorismusbekämpfungsgesetzes auf die Regelungen zum Ausländerzentralregister, ZAR 2002, 237-241.

Streit, Christian, Der Datenbestand des Ausländerzentralregisters, ZAR 1999, 109

Streit, Christian, Entwicklung, Bedeutung und Rechtsgrundlagen des Ausländerzentralregisters, BewHi 1996, 229-239.

Streit, Christian/Heyder, Udo, Das Ausländerzentralregistergesetz (AZRG), Kommentar 1997

Streit, Christian/Srocke, Frank-Rüdiger, Der Datenbestand des Ausländerzentralregisters, ZAR 1999, 109-118.

Tangermann, Julian, Identitätssicherung und -feststellung im Migrationsprozess, Bundesamt für Migration und Flüchtlinge (Hrs.), 2017.

Weichert, Thilo, Staatliche biometrische Identifizierung auf dem Prüfstand, DVBl. 2021, 1066-1075.

Weichert, Thilo (Netzwerk Datenschutzexpertise), Stellungnahme des Netzwerks Datenschutzexpertise zum Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Weiterentwicklung des Ausländerzentralregisters (AZRWeiterentwG), 24.04.2021, Deutscher Bundestag, Innenausschuss A-Drs. 19(4)820 C.

Weichert, Thilo, Staatliche Identifizierung mit Fingerabdrücken und biometrischen Lichtbildern, 08.03.2021, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2021biometrischeidentifizierung.pdf.

Weichert, Thilo, Datenschutzrecht für Ausländer nach dem 11. September 2001, DuD 2002, 423-428.

Weichert, Thilo, Kommentar zum Ausländerzentralregistergesetz, 1998.

Weichert, Thilo, AZRG – Der 2. Entwurf eines Ausländerzentralregister-Gesetzes, Bürgerrechte&Polizei (CILIP 34), Nr. 3/1989, 67-71.

Weichert, Thilo, Das geplante Ausländerzentralregister-Gesetz – Festschreibung einer verfassungswidrigen Praxis, InfAuslR 1989, 1-11.

Weichert, Thilo, Nochmals: Ausländerzentralregister, InfAuslR 1988, 108 f.

Weichert, Thilo, Ausländerüberwachung - Zum Entwurf eines Gesetzes über das Ausländerzentralregister (AZR-Gesetz), Bürgerrechte&Polizei (CILIP 31), Nr. 3/1988, 20-27.

Weichert, *Thilo*, Das Ausländerzentralregister, InfAuslR 1987, 205-218.

Wittmann, Philipp, Entwurf eines Gesetzes zur Weiterentwicklung des Ausländerzentralregisters Gesetzentwurf der Bundesregierung vom 31.03.2021 (BT-Drs. 19/28170), 30.04.2021, Deutscher Bundestag Innenausschuss A-Drs. 19(4)820 D.

Abkürzungen

ABl.	Amtsblatt der EU
Abs.	Absatz
AFIS	Automatisiertes Fingerabdruckinformationssystem
Art.	Artikel
AsylG	Asylgesetz
AufenthG	Aufenthaltsgesetz
AuslG	Ausländergesetz
AZR	Ausländerzentralregister
AZRG-DV	Durchführungsverordnung zum AZRG
AZRG	Ausländerzentralregistergesetz
AZR-VV	Verwaltungsvorschrift zum AZR
AZRWeiterentwG	AZR-Weiterentwicklungsgesetz
BAMF	Bundesamt für Migration und Flüchtlinge
BDSG	Bundesdatenschutzgesetz
BewHi	Bewährungshilfe (Zeitschrift)
BfD/I	Bundesbeauftragter für den Datenschutz/und die Informationsfreiheit
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKA/G	Bundeskriminalamt/sgesetz
BMG	Bundesmeldegesetz
BMI	Bundesministerium des Innern
BND/G	Bundesnachrichtendienst/-Gesetz
BR-Drs.	Bundesrats-Drucksache
BReg.	Bundesregierung
BT	Bundestag
BT-Drs.	Bundestagsdrucksache
BVA	Bundesverwaltungsamt
BVerfG/E	Bundesverfassungsgericht/Entscheidungssammlung
BVerfSchG	Bundesverfassungsschutzgesetz
BZRG	Bundeszentralregistergesetz
DANA	DatenschutzNachrichten (Zeitschrift)
DAVG	Datenaustausch-Verbesserungesetz
ders.	derselbe
diess.	dieselbe
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVBl.	Deutsches Verwaltungsblatt
EGMR	Europäischer Gerichtshof für Menschenrechte
Einf.	Einführung
ErwGr	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische Grundrechtszeitschrift
FDP	Freie Demokratische Partei
f/f.	fort/folgende
Fn.	Fußnote
G.	Gesetz
GFF	Gesellschaft für Freiheitsrechte
GG	Grundgesetz

GRCh	Europäische Grundrechte-Charta
GK-AufenthG	Gemeinschaftskommentar zum Aufenthaltsgesetz
HDSB	Hessischer Datenschutzbeauftragter
HmbDSB	Hamburgischer Datenschutzbeauftragter
ID	Identifikation
IDNrG	Identifikationsnummerngesetz
InfAuslR	Informationsbrief Ausländerrecht
i.S.v./d.	im Sinne von/des
i.V.m.	in Verbindung mit
JB	Jahresbericht
JZ	Juristenzeitung
Kap.	Kapitel
KJ	Kritische Justiz (Zeitschrift)
KritV	Kritische Vierteljahresschrift
LfD	Landesbeauftragter für Datenschutz
lit.	Buchstabe
MAD/G	Militärischer Abschirmdienst/-Gesetz
Mio.	Millionen
MMR	Multimedia und Recht (Zeitschrift)
MVVerfG	Verfassungsgericht Mecklenburg-Vorpommern
m.w.N.	mit weiteren Nachweisen
Nds.	Niedersachsen
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OZG	Onlinezugangsgesetz
PlProt.	Plenarprotokoll
RDV	Recht der Datenverarbeitung (Zeitschrift)
RegMoG	Registermodernisierungsgesetz
Rn.	Randnummer
RR	Rechtsprechungsreport
S.	Satz oder Seite
SächsDSB	Sächsischer Datenschutzbeauftragter
SächsVerfGH	Sächsischer Verfassungsgerichtshof
SGB	Sozialgesetzbuch
SH	Schleswig-Holstein
s.o.	siehe oben
SPD	Sozialdemokratische Partei Deutschlands
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
s.u.	siehe unten
TB	Tätigkeitsbericht
u.a.	und andere oder unter anderem
v.	von
VG	Verwaltungsgericht
vgl.	vergleiche
VO	Verordnung
Vorb	Vorbemerkung
WRV	Weimarer Reichsverfassung
ZAR	Zeitschrift für Ausländerrecht
z.B.	zum Beispiel

ZRP	Zeitschrift für Rechtspolitik