Kanzlei
Für Aufenthaltsrecht

Jentsch Rechtsanwälte

Kanzlei für Aufenthaltsrecht, Jentsch Rechtsanwälte, Eichendorffstr. 13, 10115 Berlin

Eichendorffstraße 13
10115 Berlin
Telefon (030) 252 987 77 /-78
Telefax (030) 252 987 85
E-Mail kontakt@aufenthaltsrecht.net

Bitte beachten Sie die neuen Bürozeiten:
Mo, Di und Do: 10:00 - 12:00 Uhr
Mo und Do: 15:00 - 17:00 Uhr
Mi und Fr geschlossen

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Graurheindorfer Str. 153

53117 Bonn

vorab per Fax: +49 (0)228-997799-5550
per Post mit EINSCHREIBEN

04.02.2021 D2/39375

Unser Zeichen:
XXX

Beschwerde

des XXX

gegen

die Datenverarbeitung durch das Bundesamt für Migration und Flüchtlinge, Frankenstr. 210, 90461 Nürnberg.

Namens und in Vollmacht des Beschwerdeführers, Vollmacht anbei,

rüge ich die Verletzung der Bestimmungen der Datenschutz-Grundverordnung (DSGVO) durch das Bundesamt für Migration und Flüchtlinge (BAMF) gem. Art. 77 Abs. 1 DSGVO.

Ich rege zugleich an,

dem BAMF gem. Art. 58 Abs. 2 lit. f DSGVO die weitere Durchführung der Datenträgerauswertung zu verbieten.

Gliederung

A. Sachverhalt

Mit der gegenständlichen Beschwerde rügt der Beschwerdeführer, dass das BAMF mit dem Auslesen und Auswerten seines Mobiltelefons seine personenbezogenen Daten unter Verstoß gegen die Vorschriften der DSGVO verarbeitet hat und weiterverarbeitet, nämlich zumindest speichert.

B. Rechtsgrundlagen

Durch das Gesetz zur besseren Durchsetzung der Ausreisepflicht vom 20. Juli 2017 wurde § 15 Abs. 2 Nr. 6 AsylG neugefasst und § 15a AsylG eingeführt. Nach § 15 Abs. 2 Nr. 6 AsylG ist „der Ausländer“ nun verpflichtet, „im Falle des Nichtbesitzes eines gültigen Passes oder Passersatzes (…) auf Verlangen alle Datenträger, die für die Feststellung seiner Identität und Staatsangehörigkeit von Bedeutung sein können und in deren Besitz er ist, den für die Ausführung des Gesetzes zuständigen Behörden vorzulegen, auszuhändigen und zu überlassen“.

Alleiniger Zweck der Datenträgerauswertung ist damit die Feststellung von Identität und Staatsangehörigkeit, nicht etwa die Überprüfung gemachter Angaben zur Fluchtroute oder -geschichte.

§ 15 Abs. 4 AsylG ermöglicht eine Durchsuchung Asylsuchender und ihrer Sachen, wenn sie der Aufforderung zur Herausgabe nicht nachkommen.

§ 15a Satz 1 AsylG erklärt die Auswertung der herausgegebenen Datenträger für zulässig, soweit dies für die Feststellung der Identität und Staatsangehörigkeit des Ausländers nach § 15 Absatz 2 Nummer 6 erforderlich ist und der Zweck der Maßnahme nicht durch mildere Mittel erreicht werden kann.

Im Übrigen verweist § 15a AsylG auf die bereits durch Gesetz vom 27. Juli 2015 eingeführten §§ 48 Abs. 3a und 48a AufenthG. Nach § 48 Abs. 3a Satz 3 AufenthG hat „der Ausländer“ die notwendigen Zugangsdaten für eine zuverlässige Auswertung zur Verfügung zu stellen; kommt er dem nicht nach, können die Zugangsdaten nach § 48a AufenthG von den Telekommunikationsdienstleistern erhoben werden. Im Übrigen begrenzt § 48 Abs. 3a AufenthG die Auswertungsbefugnis. Eine Auswertung ist ausgeschlossen, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden (Satz 2); Erkenntnisse aus dem Kernbereich dürfen nicht verwertet werden und sind unverzüglich zu löschen (Satz 5 und 6). Die Auswertung darf nur von Bediensteten mit Befähigung zum Richteramt erfolgen (Satz 4). Die

Auswertung wird in die Akte der antragstellenden Person überführt, auf die anschließend jede*r zuständige Sachbearbeiter*in beim BAMF Zugriff hat.

I. Praktische Durchführung der Datenträgerauswertung

Die Rechtsgrundlage erlaubt ein Auslesen und Auswertung im Asylverfahren, um gemachte Angaben zu Identität und Staatsangehörigkeit zu plausibiliseren,

> siehe zum Ganzen Biselli/Beckmann (2019): Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa, inbs. S. 12ff, online unter https://freiheitsrechte.org/studie-handydatenauswertung/.

Die Rechtsgrundlage erlaubt dies ohne den Zeitpunkt zu präzisieren. Ausweislich der Dienstanweisungen „Identitätsfeststellung“ sowie „AVS Auslesen von mobilen Datenträgern“ des BAMF sollen Datenträger regelmäßig bereits bei der Registrierung der Asylsuchenden ausgelesen werden. Zum Teil geschieht dies aber auch zu anderen Zeitpunkten im Asylverfahren, etwa im Rahmen eines Widerrufs- oder Rücknahmeverfahrens nach den §§ 73 ff. AsylG.

Auch wenn das BAMF laut Gesetz Datenträger aller Art auswerten dürfte, analysiert die Behörde derzeit nur Smartphones und sogenannte Featurephones, also einfachere Handys mit geringerem Funktionsumfang. Der Prozess der Datenträgerauswertung lässt sich in fünf Phasen unterteilen:

Die Asylsuchenden werden mündlich und schriftlich auf seine Pflicht zur Überlassung von Datenträgern hingewiesen und aufgefordert, diese herauszugeben und zu entsperren.

Alle auf dem Gerät befindlichen Daten werden ausgelesen, dieser Gesamtdatensatzes wird automatisch nach bestimmten Kategorien analysiert und ein digitaler Prüfbericht erstellt.

Anschließend wird dieser Prüfbericht in einem Datentresor des BAMF gespeichert.

Auf Antrag der*des Entscheiders*in prüft eine*n BAMF-interne*n Volljurist*in die Freigabe des Prüfberichts.

Der freigegebene Prüfbericht wird in die Asylakte überführt.

Ausgelesen werden Datenträger, wenn die geflüchtete Person keine gültigen Ausweispapiere vorlegen kann,

> vgl. Bundesamt für Migration und Flüchtlinge, Dienstanweisung Asylverfahren, Identitätsfeststellung als **Anlage 1**, Ziff. 3.1.1. und Bundesamt für Migration und

Flüchtlinge, Dienstanweisung für das AVS, Auslesen von mobilen Datenträgern als **Anlage 2**, Ziff. 1.

Wann ein Pass oder Passersatz ungültig ist, ist in § 11 PassG festgelegt. Danach ist ein Dokument insbesondere ungültig, wenn es eine einwandfreie Feststellung der Identität nicht zulässt, verändert worden ist oder die Gültigkeitsdauer abgelaufen ist (§ 11 Abs. 1 Nr. Nr. 1-3 PassG).

Die Validität der Pässe mancher Länder lässt sich aus technischen Gründen nicht unmittelbar vor Ort feststellen; auch in diesen Fällen liest das BAMF die Datenträger der betroffenen Personen aus. Insgesamt existieren drei Prüfebenen der physikalisch-technischen Untersuchung (PTU) von Personaldokumenten. Nur die erste Prüfebene findet vor Ort beim BAMF statt. Wenn die Gültigkeit oder Echtheit der Dokumente nicht vor Ort in der ersten Prüfebene abschließend festgestellt werden kann, findet die Auslesung der Datenträger statt; die zweite und die dritte Prüfebene werden nicht abgewartet,

Anlage 2, S. 2.

Zu den vor Ort untersuchbaren Dokumenten zählen laut der Dienstanweisung „Asylverfahren – Urkundenprüfung“ maschinenlesbare Dokumente aller Herkunftsländer, zusätzlich alle anderen Dokumente aus Syrien, dem Irak, Iran, Eritrea, der Ukraine, Afghanistan und der Russischen Föderation,

Dienstanweisung Asylverfahren, Urkundenprüfung, Stand 06/18 als **Anlage 3**, S. 356.

Legen Asylsuchende keinen Pass oder Passersatz vor, der vom BAMF nach einer Überprüfung vor Ort als gültig anerkannt wird, werden Datenträger ausgelesen. Die Anhörung der asylsuchenden Person ist nach Ansicht des BAMF nicht als vorab einzubeziehendes, milderes Mittel zu anzusehen. Sonstige Dokumente wie ID-Karten, Führerscheine, Flüchtlingsausweise und Militärausweise werden laut „Dienstanweisung Identitätsfeststellung“ zwar vor der *Auswertung* der Datenträger als mildere Mittel in Betracht gezogen, gelten aber jeweils nicht als Passersatzvorlage, die die Anwendbarkeit der Vorschrift über das Auslesen sperrt,

Bundesamt für Migration und Flüchtlinge, Dienstanweisung Asylverfahren, Identitätsfeststellung als **Anlage 1**, Ziff. 3.1.1. und 3.1.

Die Asylsuchenden, deren Datenträger ausgelesen werden sollen, werden bei der Registrierung unter Hinweis auf ihre gesetzlichen Mitwirkungspflichten aufgefordert, ihre

Datenträger herauszugeben und zu entsperren. Für das weitere Vorgehen bestimmt die Dienstanweisung:

> „*Mit dem Dokument D1705 (Datenträger-Erklärung), das dem MARiS-Aktenbestand zugefügt wird, wird festgehalten, ob der Antragsteller einen Datenträger aushändigt, die Aushändigung verweigert oder nicht besitzt. Wird die Herausgabe des Datenträgers verweigert, wird der Antragsteller erneut auf seine Mitwirkungspflicht hingewiesen. Außerdem wird er darauf hingewiesen, dass bei Nichtmitwirkung das Verfahren gem. der vom Antragsteller unterschriebenen Erstbelehrung nach § 33 Abs. 1 AsylG als zurückgenommen angesehen werden kann und das Verfahren eingestellt wird.*“
>
> **Anlage 1**, Ziff. 3.1.1.

Die ausgehändigten Datenträger werden über ein USB-Kabel an ein speziell dafür erworbenes Gerät des schwedischen Herstellers MSAB, den „MSAB Kiosk“, angeschlossen und dort ausgelesen. In der Folge wird zunächst ein kompletter Rohdatensatz ausgelesen und daraus automatisch ein elektronischer Ergebnisreport generiert. Dieser wird in einem Datentresor gespeichert. Nach Abschluss des Vorgangs wird der Datenträger der asylsuchenden Person zurückgegeben, die Kopie des kompletten Rohdatensatzes wird automatisch gelöscht,

> **Anlage 1**, Ziff. 3.1.1.; **Anlage 2**, Ziff. 1 und Bundesamt für Migration und Flüchtlinge, Integriertes Identitätsmanagement – Plausibilisierung, Datenqualität und Sicherheitsaspekte, Einführung in die neuen IT-Tools, Schulung AVS-Mitarbeiter, Entscheider und Volljuristen, 30.08.2017, als **Anlage 4**, S. 55ff.

Der mithilfe der Software XRY des Herstellers MSAB erstellte Ergebnisreport enthält in Form von Tortendiagrammen Informationen zu den Ländervorwahlen der im Adressbuch gespeicherten Kontakte, der ein- und ausgehenden Anrufe und der Textnachrichten verschiedener Messenger. In Form von Tabellen werden die Gesamt-Anrufdauer und die Zahl der Textnachrichten zu und von Nummern mit den jeweiligen Ländervorwahlen dargestellt. In einer weiteren Tabelle werden die Anzahl und Häufigkeit der Top-Level-Domains aufgerufener Internetadressen aufbereitet. Darüber hinaus werden Geolokationsdaten auf einer Karte angezeigt, wofür Fotos sowie möglicherweise Apps ausgewertet werden. Ob darüber hinaus App-Informationen, gespeicherte WLAN-Netzwerke oder aufgezeichnete GPS-Daten betrachtet werden, ist nicht bekannt. Das BAMF gibt hierzu keine Informationen preis.

Zusätzlich wird mithilfe einer erworbenen Software des Herstellers T3K die in Textnachrichten, E-Mails und Browserverläufen verwendete Sprache analysiert und in Tabellen das Ergebnis nach Zahl und Häufigkeit der verwendeten Sprachen dargestellt. Im Fall des Arabischen wird auch der verwendete Dialekt angegeben.

Als Hinweis auf die Identität werden aus verschiedenen, im Einzelnen benannten Apps ermittelte Namen, Account-Namen, IDs, Geburtstage und E-Mail-Adressen im Klartext dargestellt. Einzelheiten lassen sich Schulungsunterlagen des BAMF entnehmen,

Anlage 4, S. 104 ff.

Nach der „Dienstanweisung Asylverfahren Identitätsfeststellung“ wird der Ergebnisreport nur dann verwendet, wenn der*die Entscheider*in ihn anfordert und ein*e beim BAMF angestellte Volljurist*in ihn für das Asylverfahren freigibt. Eine Anforderung soll erfolgen, wenn basierend auf einer Gesamtschau der verfügbaren Informationen die Identität und Staatsangehörigkeit nicht eindeutig geklärt erscheint und auch nicht mit milderen Mitteln geklärt werden kann. Als mildere Mittel kommen laut Dienstanweisung Asylverfahren Identitätsfeststellung nur Dokumente in Betracht, „die durch ein Lichtbild die Identität belegen können und vom Bundesamt auf ihre Echtheit überprüft werden können“. Dies seien etwa ID-Karten, Führerscheine, Flüchtlingsausweise und Militärausweise,

Anlage 1, Ziff. 3.1 und 3.1.2.

Hält der*die Entscheider*in den Ergebnisreport nicht für verfahrensrelevant, hat er*sie die Löschung zu veranlassen,

Anlage 1, Ziff. 3.1.2.; **Anlage 2**, Ziff. 2.

Der*die zuständige Volljurist*in überprüft, ob der Ergebnisreport für das Verfahren freizugeben ist. Falls ja wird er vom Datentresor in das elektronische Aktensystem MARiS (Migrations-Asyl-Reintegrationssystem) importiert, im Datentresor gelöscht und der Asylakte hinzugefügt. Der Report kann dann zur Vorbereitung der Asylanhörung genutzt werden. Andernfalls wird die Löschung veranlasst,

Anlage 1, Ziff. 3.1.3.

Die elektronische Akte, deren Teil der Ergebnisreport nach der Freigabe wird, darf gem. § 7 Abs. 3 AsylG für zehn Jahre nach unanfechtbarem Abschluss des Asylverfahrens gespeichert bleiben. § 8 Abs. 3 AsylG ermöglicht die Weitergabe der im Asylverfahren erhobenen Daten an zahlreiche andere Behörden, etwa zur Abwehr erheblicher Gefahren für Leib und Leben von Asylsuchenden und Dritten, zur Verfolgung von Straftaten und

Ordnungswidrigkeiten sowie zur Aufdeckung und Verfolgung von zu Unrecht erbrachten Sozialleistungen.

II. Aussagekraft und Zuverlässigkeit der Datenträgerauswertung

Die Bundesregierung hat auf mehrere Kleine Anfragen von Mitgliedern des Deutschen Bundestages Zahlen zur Häufigkeit des Auslesens und Auswertens der Datenträger von Asylsuchenden sowie zu den daraus ermittelten Ergebnissen vorgelegt,

> BT-Drs. 19/8701, 25.03.2019, als **Anlage 5**, S. 28 f.; BT-Drs. Drucksache 19/18498 vom 02.04.2020 als **Anlage 6**, S. 33 f.

Aus diesen Zahlen ist ersichtlich, dass nur etwas über ein Drittel der Erstantragsteller*innen über 14 Jahren ohne Pass bzw. Passersatz angibt, im Besitz eines Datenträgers zu sein. Bei etwa einem Viertel der herausgegebenen Datenträger gelingt die Auslesung bereits technisch nicht – und stellt sich damit als ungeeignet dar. Nur bei weniger als der Hälfte der ausgelesenen Datenträger beantragt die über den Asylantrag entscheidende Person die Auswertung, bei einem erheblichen Teil dieser Fälle verweigert der*die zuständige Volljurist*in die Freigabe mangels Geeignetheit oder Erforderlichkeit. Die durchgeführten Datenträgerauswertungen liefern überwiegend keine aussagekräftigen und für den Zweck der Norm geeigneten Daten, sie widerlegen die Angaben der Asylsuchenden nur in ganz wenigen Fällen. Entgegen des Grundsatzes der Datenminimierung werden damit große Mengen von personenbezogenen Daten verarbeitet, ohne das es auf diese im Ergebnis ankommt. Einzelheiten sind der folgenden Tabelle zu entnehmen:

	2018	**2019**
Erstantragsteller*innen > 14 J. ohne Pass / Passersatz im Besitz von Datenträgern	35 %	40 %
Anteil technisch auslesbarer Datenträger	74 %	77 %
Erstellte Rohdatensätze	11.389	10.116
Datenträger-Erstauswertungsanträge	5.431	4.582
Zur Auswertung freigegebene Datenträger	3.308	3.436
davon keine aussagekräftigen Daten	64 %	58 %
Bestätigung der Angaben	34 %	40 %
Widerlegung der Angaben	2 %	2 %

Die Gründe dafür, dass aus der Datenträgerauswertung vielfach keine aussagekräftigen, und damit für den Zweck der Norm geeigneten Daten gewonnen werden, sind struktureller Art. Zum einen analysiert die Software nicht die Staatsangehörigkeit selbst, sondern Datenkategorien wie die Ländervorwahlen bei den Telekommunikationsverbindungsdaten. Diese Daten können für die Staatsangehörigkeit allenfalls Indizwirkung haben. Da heute viele Menschen Kontakte in zahlreiche Länder haben, lässt sich die Staatsangehörigkeit

eines bestimmten Staates so nicht ermitteln. Die Ermittlung der Identität aus E-Mail-Adressen und Login-Daten ist ebenfalls mit Unsicherheiten behaftet, geben doch viele Menschen bei Online-Applikationen nicht ihren bürgerlichen Namen an. Hinzu kommt, dass erhebliche Risiken einer Erfassung unrichtiger Daten bestehen. So können die auf dem Mobiltelefon einer asylsuchenden Person gespeicherten Daten auch von Vorbesitzer*innen herrühren. Geolokationsdaten sind zudem für Staatsangehörigkeit und Identität wenig aussagekräftig. Ausweislich der Rechtsgrundlage dürfen die ermittelnden Daten aber nicht zur Überprüfung der Angaben zur Fluchtroute oder -geschichte eingesetzt werden. Bei der Ermittlung von Geolokationsdaten aus Fotos ist zudem zu beachten, dass diese extrem fehleranfällig sind. Die softwaregestützte Spracherkennung in Textnachrichten ist mit dem erheblichen Risiko einer fehlerhaften Zuordnung verbunden. Das gilt in besonderer Weise für die Zuordnung arabischer Dialekte, für die zunächst arabische Schriftzeichen in lateinische transkribiert werden müssen und bei denen sich deshalb eine große Vielfalt von unterschiedlichen, phonetisierenden Schreibweisen entwickelt hat.

III. Asylverfahren des Beschwerdeführers

Der Beschwerdeführer ist syrischer Staatsangehöriger […]. Mit Bescheid vom […] wurde ihm die Flüchtlingseigenschaft zuerkannt. Im Jahr […] wurde ein Widerrufsverfahren gegenüber der Flüchtlingsanerkennung eingeleitet […]. In diesem Rahmen wurde der Beschwerdeführer vom Bundesamt für Migration und Flüchtlinge aufgefordert, sein Mobiltelefon zur Auslesung zu überlassen – […].

Die Aufforderung wurde damit begründet, dass der Beschwerdeführer keine gültigen Identitätspapiere vorlegen kann. Dem Beschwerdeführer wurde in der Befragung nicht mitgeteilt, welche Daten aus seinem Mobiltelefon ausgelesen, analysiert oder in der Folge abgespeichert und kenntlich sein würden. Noch am gleichen Tag wurde der Ergebnisreport angefordert und lag dem Mitarbeitenden bei der Befragung des Beschwerdeführers in der Anhörung vor.

Dem Beschwerdeführer wurde mit der Aufforderung zur Herausgabe seines Mobiltelefons ein zu unterzeichnendes Dokument vorlegt, in welchem er auf seine gesetzliche Pflicht zur Herausgabe der Datenträger hingewiesen wurde. Ebenfalls wurde er darauf hingewiesen, dass eine verweigerte Mitwirkung bei der Feststellung von Identität und Staatsangehörigkeit dazu führen kann, dass sein Asylantrag als zurückgezogen angesehen wird. Darüber, welche Daten ausgelesen würden und in welchem Umfang für Mitarbeitende des BAMF einsehbar sein würden, wurde er nicht hingewiesen. Auch durfte er den Ergebnisreport der Auslesung seines Handys nicht einsehen.

[…]

C. Anwendbarkeit der DSGVO und Zuständigkeit des BfDI

Die DSGVO ist auf die Datenerhebung des BAMF anwendbar. Sie gilt grundsätzlich umfassend für die Datenverarbeitung auch von öffentlichen Stellen. Ausnahmetatbestände von Anwendungsbereich der DSGVO hinsichtlich Gefahrenabwehr in Art. 2 Abs. 2 DSGVO greifen hier nicht:

Art. 2 Abs. 2 lit. d DSGVO nimmt vom sachlichen Anwendungsbereich der DSGVO lediglich eine Datenverarbeitung aus, die durch die zuständigen Behörden mit den folgenden Zwecken erfolgt: Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, Strafvollstreckung, Schutz vor und Abwehr von Gefahren für die öffentliche Sicherheit. Der Datenschutz in diesem Bereich ist in einem eigenen Unionsrechtsakt geregelt, nämlich der sog. JI-Richtlinie (EU/2016/680). Art. 1 Abs. 1 der JI- Richtlinie eröffnet spiegelbildlich zu Art. 2 Abs. 2 lit. d DSGVO die Anwendbarkeit der Richtlinie (bzw. von deren nationalen Umsetzungsgesetzen).

Aus Erwägungsgrund 13 der JI-Richtlinie folgt, dass eine Straftat im Sinne der Richtlinie als eigenständiger Begriff des Unionsrechts anzusehen ist, d. h. nicht der Ausgestaltung oder Definition durch deutsches Recht zugänglich ist. Nach h. M. ist dieser unionsrechtliche Begriff der „Straftat“ weiter zu verstehen als im deutschen Recht und erfasst auch Ordnungswidrigkeiten,

Bäcker, in: Wolff/Brink, Beck-OK-Datenschutzrecht, Art. 2 DSGVO, Rn. 25a m.w.N.

Der Begriff der öffentlichen Sicherheit ist hingegen enger zu verstehen als im deutschen Recht, da ansonsten annähernd die gesamte Ordnungsverwaltung von den Vorgaben der DSGVO ausgenommen würde. Das widerspräche aber dem Ziel der DSGVO, die unter anderem darauf abzielt, Datenverarbeitungen durch öffentliche Stellen zu reglementieren (vgl. 5. Erwägungsgrund DSGVO).

Die Ausnahmen in Art. 2 Abs. 2 DSGVO greifen damit nur, wenn sowohl bei der allgemeinen Kompetenz der Behörde als auch bei der konkreten Maßnahme ein enger Zusammenhang mit der Verhütung und Verfolgung von Straftaten und Ordnungswidrigkeiten vorliegt. Das kann nur bei der Tätigkeit von solchen Behörden angenommen werden kann, deren Kernkompetenz die Verhütung und Bekämpfung von Straftaten oder Ordnungswidrigkeiten ist, insbesondere also Polizeibehörden. Nicht umfasst von der Ausnahmevorschrift des Art. 2

Abs. 2 lit. d DSGVO ist hingegen die Tätigkeit von anderen Ordnungsbehörden einschließlich der im Migrationsrecht tätigen Behörden, die zwar nach deutschem Rechtsverständnis der öffentlichen Sicherheit dienen, jedoch keinen unmittelbaren Bezug zur Verhütung und Bekämpfung von Straftaten haben,

> BeckOK Datenschutzrecht/Bäcker, 34. Ed. 1. August 2020, DS-GVO Art. 2 a.1; Kühling/Buchner/Kühling/Raab, DSGVO Art. 2 Rn. 29.

Die hier einschlägige Kompetenz des BAMF ist die Prüfung von Asylanträgen. Dazu gehört naturgemäß – wie bei allen Verwaltungsverfahren – die Prüfung der Glaubhaftigkeit von Angaben zur Feststellung von Identität und Staatsangehörigkeit. Diese Prüfung und die damit einhergehenden Eingriffsbefugnisse dienen der Sicherung von effektivem und rechtsstaatlichem Verwaltungshandeln. Sie haben jedoch keinen konkreten Bezug zur Verhütung oder Verfolgung von Straftaten.

Daran ändert auch die Tatsache nichts, dass die Handydatenauswertungen ausweislich der Beratung im Bundestag (Erste Beratung, BT-PIPr, S. 22524-22535) auch der Verhinderung von „Asylbetrug“ und der Verschleppung von Abschiebungen dienen soll. Denn diese Formulierungen sind allein zugespitzte Formulierungen des Zwecks der Sicherung eines effektiven Verfahrens.

Zu berücksichtigen ist schließlich, dass Angaben zu Identität und Staatsangehörigkeit gegenüber dem BAMF, die sich durch die Datenauswertung als falsch herausstellen, nicht zu einer Strafverfolgung führen können, da Falschangaben im Asylverfahren nicht strafbewehrt sind. Die Vorschrift des § 95 Abs. 2 Nr. 2 AufenthG gilt allein für das aufenthaltsrechtliche Verfahren gegenüber der Ausländerbehörde, nicht hingegen für das Asylverfahren beim BAMF (BayObLG München, Urteil vom 19. Februar 2020 – 207 StRR 2415/19).

Die weitere Voraussetzung des Art. 2 Abs. 2 lit. a DSGVO, dass die Datenverarbeitung im Rahmen einer Tätigkeit erfolgt, die in den Anwendungsbereich des Unionsrechts fällt, ist ebenfalls gegeben. Anders als in Art. 51 Abs. 1 GRCh ist in Art. 2 Abs. 2 lit. a DSGVO aber nicht gefordert, dass die Tätigkeit der Durchführung des Unionsrechts dient. Für Art. 2 Abs. 2 lit. a DSGVO genügt es, dass die Tätigkeit bei abstrakter Betrachtung einen Bezug zum Unionsrecht hat,

> Bäcker, BeckOK-Datenschutzrecht, Art. 2 DSGVO Rn. 7.

Das deutsche Asylrecht ist in erheblichem Umfang durch die aufgrund von Art. 78 AEUV erlassenen europäischen Asylrichtlinien geprägt. Insbesondere macht die Richtlinie

2013/32/EU weitreichende Vorgaben für das Asylverfahren und regelt dabei in Art. 13 auch die Verpflichtung der Antragsteller, mit den zuständigen Behörden zur Feststellung ihrer Identität zusammenzuarbeiten. Gem. Art. 13 Abs. 1 S. 2 der Richtlinie 2013/32/EU können die Mitgliedstaaten weitere Verpflichtungen zur Zusammenarbeit auferlegen, sofern diese Verpflichtungen für die Bearbeitung des Antrags erforderlich sind. Die Verpflichtung nach § 15a AsylG stützt sich insofern auf diesen durch das Unionsrecht vorgegebenen Rahmen.
Die Beschwerde gem. Art. 77 Abs. 1 DSGVO ist an die zuständige Aufsichtsbehörde zu richten. Der BfDI ist für die Kontrolle der Datenverarbeitung durch öffentliche Stellen des Bundes und damit auch des Bundesamtes für Migration und Flüchtlinge zuständig, § 9 Abs. 1 BDSG.

D. Verstoß der Datenträgerauswertung gegen die DSGVO

Das Auslesen und Auswerten von Datenträgern Asylsuchender durch das BAMF steht mit den Vorgaben der DSGVO nicht im Einklang. Die Praxis überschreitet bereits teilweise die Rechtsgrundlage und widerspricht damit bereits dem Grundsatz der Rechtmäßigkeit (dazu unter D.II.), zudem ist die Rechtsgrundlage zu unbestimmt (dazu unter D.III.). Soweit personenbezogene Daten besonderer Kategorien erhoben werden, ist diese Verarbeitung nach Art. 9 Abs. 1 DSGVO unzulässig (dazu unter D.IV). Außerdem verstößt die Praxis gegen diverse Datenverarbeitungsgrundsätze der DSGVO, nämlich gegen den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO (dazu unter D.V.), sowie gegen den Grundsatz der Datenrichtigkeit Art. 5 Abs. 1 lit. d DSGVO (dazu unter D.VI.). Die Rechtsgrundlage des § 15a AsylG verstößt schließlich gegen Art. 6 Abs. 3 Satz 4 DSGVO, weil sie Rechtseingriffe zulässt, die unverhältnismäßig zum Zweck der Datenverarbeitung sind (D.VII.).

I. Datenverarbeitungsvorgänge

Ein Datenverarbeitungsvorgang im Sinne der DSGVO liegt nicht nur vor, wenn Daten vom Verantwortlichen für bestimmte Zwecke verwendet werden. Nach Art. 4 Nr. 2 DSGVO ist ausdrücklich auch das Auslesen, Ordnen und Speichern personenbezogener Daten mithilfe automatisierter Verfahren erfasst. Es gilt ein weiter Verarbeitungsbegriff. Daher gelten für die Auslesung von Datenträger Asylsuchender durch das BAMF und die softwaregestützte Generierung des Ergebnisreports die Anforderungen der DSGVO auch in solchen Fällen, in denen der abgespeicherte Ergebnisreport für das Asylverfahren von der beim BAMF entscheidenden Person anschließend nicht angefordert wird.

II. BAMF-Datenverarbeitung überschreitet die Rechtsgrundlage, Art. 5 Abs. 1 lit. a Alt. 1, Art. 6 Abs. 1 DSGVO

Gemäß Art. 1 Abs. 1 lit. 1 Alt. 1 und Art. 6 Abs. 1 DSGVO müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Eine Datenverarbeitung ist nur nach Einwilligung oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage rechtmäßig.

Die Rechtsgrundlage des § 15 Abs. 2. Nr. 6 AsylG überschreitet das BAMF jedoch ausweislich der eigenen Schulungsunterlagen. Nach § 15 Abs. 2. Nr. 6 AsylG muss der Ausländer im Falle des Nichtbesitzes eines gültigen Passes oder Passersatzes auf Verlangen Datenträger herausgeben. Voraussetzung der Datenträgerauswertung ist damit einerseits, dass festgestellt ist, das keine Dokumente vorgelegt werden oder vorgelegte Dokumente ungültig sind. Zudem muss „Nichtbesitz“ nach Wortlaut und Systematik der Norm so verstanden werden, dass ein bloß vorübergehendes, von der betroffenen Person nicht zu vertretendes Nichtbesitzen von Dokumenten nicht darunterfällt.

Das BAMF liest ausweislich seiner Schulungsmaterialien auch Handydaten sowohl bei Geflüchteten aus, bei denen die Gültigkeit der vorgelegten Pass- oder Passersatzdokumente nicht bereits vor Ort abschließend überprüft werden konnte, als auch bei Geflüchteten, die gültige Dokumente im Termin deshalb nicht vorlegen können, weil diese von einer anderen Behörde einbehalten werden. Die Handydatenauswertungen in diesen Fällen sind bereits deshalb rechtswidrig, weil sie die Rechtsgrundlage des § 15a AsylG überschreiten.

III. Fehlende Bestimmtheit der Rechtsgrundlage, Art. 52 Abs. 1 Satz 1 GrCH

Eine Einschränkung des Grundrechts auf Datenschutz nach Art. 8 GRCh und Art. 16 AEUV ist nur nach den Vorgaben des Art. 52 Abs. 1 GrCH zulässig. Erforderlich ist eine gesetzliche Grundlage, die hinreichend bestimmt ist (Art. 52 Abs. 1 Satz 1 GrCH). Dafür muss das einschränkende Gesetz „hinreichend klar und genau“ sein,

> EuGH, C-419/14 – WebMindLicenses, 17.12.2015 Rn. 81; GA Cruz Villalón, C-70/10 – Scarlet, Slg.2011, I-11959 Nr. 100; Jarass GrCh, 4. Aufl. 2021 Rn. 27, EU-GRCh Art. 52 Rn. 27.

Es ist unzulässig, schwerwiegende Eingriffe zu ermöglichen, ohne die „konkreten objektiven Umstände“ der Befugnis zu regeln,

> Jarass GrCh, 4. Aufl. 2021 Rn. 27, EU-Grundrechte-Charta Art. 52 Rn. 27.

Dem wird § 15a AsylG nicht gerecht. Die Rechtsgrundlage hätte zumindest adäquate Begrenzungen vorsehen müssen, welche Daten erhoben werden dürfen und wann ein

hinreichender Anlass zur Auswertung besteht. Eine solche Eingrenzung war aber politisch gerade nicht gewollt. In der Begründung des Regierungsentwurfs des § 15a AsylG wurde ausdrücklich vorgesehen, dass die Datenträgerauswertung routinemäßig bei allen Asylsuchenden ohne anerkannte Ausweispapiere bereits zum Zeitpunkt der Registrierung stattfinden soll,

> BT-Drs. 18/11546 vom 16. März 2017, als **Anlage 7**, S. 15.

Insofern wird bereits an dieser Stelle nicht geprüft, ob andere Mittel den Zweck, nämlich die Feststellung von Identität und Staatsangehörigkeit, erreichen können: Andere und mildere Mittel, die der Erforderlichkeit der Auswertung entgegenstehen, sind die Asylanhörung als solche sowie die Prüfung der Validität anderer vorgelegter Dokumente, die deutlich bessere Indizien darstellen können als die Datenträgerauswertung.

§ 15a AsylG schließt zudem weder aus, dass neben Metadaten auch gespeicherte Kommunikationsinhalte ausgewertet werden dürfen, noch enthält er Regelungen zur Verarbeitung von automatisiert erhobenen personenbezogenen Daten besonderer Kategorien. Damit ermöglicht die Regelung dem Wortlaut nach Grundrechtseingriffe, die noch wesentlich weiter reichen als die derzeitige Praxis. Ausdrücklich unzulässig ist es lediglich nach § 15a AsylG i.V.m. § 48 Abs. 3a Satz 5 AufenthG, Erkenntnisse aus dem Kernbereich privater Lebensgestaltung zu verwerten. Dies verhindert aber nicht, dass Daten aus dem Kernbereich erhoben werden, diese als Teil des aus einem Endgerät ausgelesenen Datensatzes gespeichert bleiben und die für die Auswertung zuständige Person davon Kenntnis erlangt. Denn das Erhebungsverbot des § 15a AsylG i.V.m. § 48 Abs. 3a Satz 1 AufenthG ist praktisch bedeutungslos, da von der Auswertung der Datenträger von Asylsuchenden nie „allein“ Erkenntnisse aus dem Kernbereich zu erwarten sind,

> vgl. **Anlage 8**: Tabbara: Ineffektiv aber nicht ohne Wirkung. Der staatliche Zugriff auf Mobiltelefone von Geflüchteten, November 2019 in: Vorgänge, Ausgabe 227, S. 123, 127; Funke-Kaiser, in: GK-AsylG, EL 115 März 2018, § 15a Rn. 12.

Und schließlich gilt der Kernbereichsschutz nur für einen kleinen Kreis intimer Äußerungen, während Kommunikationsinhalte mit sozialem Bezug erfasst werden dürfen.

Soweit § 15a AsylG also keinerlei Einschränkungen vorsieht, in welchem Umfang und auf welche Art die Daten von Datenträgern zum Zweck der Feststellung von Identität und Staatsangehörigkeit verarbeitet werden darf, verstößt er gegen die europarechtliche Voraussetzung der Bestimmtheit der Rechtsgrundlage.

Effektiver Grundrechtsschutz würde außerdem voraussetzen, dass § 15a AsylG das BAMF zu einer umfassenden Dokumentation verpflichtet, die der Bundesdatenschutzbeauftragte zum Gegenstand seiner Überprüfung machen kann,

vgl. BVerfG NJW 2019, 827 Rn. 156 ff.

Das Fehlen einer solchen Regelung in § 15a AsylG hat bereits vor Inkrafttreten die damalige Bundesdatenschutzbeauftragte als verfassungsrechtliches Defizit bemängelt,

BT-Drs. 18 (4) 831, **Anlage 9**, S. 8.

IV. Verstoß gegen Erhebungsverbot besonderer Kategorien personenbezogener Daten, Art. 9 DSGVO

Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung bestimmter Kategorien von personenbezogenen Daten grundsätzlich unzulässig. Solche Daten werden jedoch vom BAMF im Rahmen der Handydatenauswertungen erhoben (dazu unter D.IV.1). Dies ist auch nicht ausnahmsweise nach Art. 9 Abs. 2 lit. g DSGVO zulässig (dazu unter D.IV.2.).

1. Erhebung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DSGVO

Die ausgelesenen Rohdatensätze von Mobiltelefonen werden in Fotos, Nachrichten und E-Mail-Nachrichten in aller Regel besonderer Kategorien personenbezogener Daten enthalten, etwa über die rassische und ethnische Herkunft, politische Meinung, Gewerkschafts- und Religionszugehörigkeit, das Sexualleben oder die sexuelle Orientierung.

Aber auch der Ergebnisreport kann Daten im Sinne des Art. 9 Abs. 1 DSGVO enthalten. Dort erscheinen nicht nur Tabellen über Verbindungsdaten, sondern auch die verwendeten Apps oder die verwendeten Account-Namen, die unter Umständen Rückschlüsse auf die sexuelle Orientierung zulassen können. Das BAMF sieht beispielsweise, welche Dating-Apps eine Person verwendet, was Rückschlüsse auf sexuelle Orientierung zulassen kann. Weiter sieht das BAMF, mit welchem Namen Dating-Apps genutzt werden. Ebenfalls angezeigt werden gewählte Login-Namen oder für den Login verwendete E-Mail-Adressen, deren Domain die politische Meinung oder die Religions- oder Gewerkschaftszugehörigkeit ersichtlich werden lassen kann.

§ 15a AsylG i.V.m. § 48 Abs. 3a Satz 5 AufenthG verbietet es, Daten aus dem Kernbereich privater Lebensgestaltung zu verwerten. Die vom BVerfG für das deutsche Verfassungsrecht entwickelte Kategorie des Kernbereichs privater Lebensgestaltung ist deutlich enger als Art. 9 Abs. 1 DSGVO und betrifft in erster Linie Äußerungen über innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse

höchstpersönlicher Art im Gespräch mit engen Familienangehörigen, Freunden und Berufsgeheimnisträgern,

BVerfGE 109, 279 (313); 141, 220 (Rn. 121).

Auch soweit Daten zum Kernbereich privater Lebensgestaltung in diesem Sinne zählen, kann § 48 Abs. 3a Satz 5 AufenthG jedoch nicht verhindern, dass diese verarbeitet werden. § 48 Abs. 3a Satz 1 AufenthG verbietet nur, Datenträger überhaupt auszuwerten, wenn *allein* Erkenntnisse aus dem Kernbereich zu erwarten sind; dies wird indes kaum je der Fall sein.

2. Keine Ausnahme nach Art. 9 Abs. 2 lit. g DSGVO
Art. 9 Abs. 2 lit. g DSGVO lässt die Verarbeitung von Daten im Sinne des Art. 9 Abs. 1 DSGVO ausnahmsweise zu, wenn dies eine Rechtsgrundlage im Recht der Mitgliedsstaaten zur Wahrung eines „erheblichen öffentlichen Interesses“ vorsieht.

§ 7 Abs. 1 Satz 2 AsylG ermächtigt zwar zur Erhebung von Daten im Sinne des Art. 9 Abs. 1 DSGVO, soweit dies im Einzelfall zur Aufgabenerfüllung erforderlich ist. Hier verlangt eine unionsrechtskonforme, entsprechend strenge Auslegung des Begriffs „Aufgabenerfüllung“ jedoch, dass dies nur dann zulässig ist, wenn der Verarbeitungsgrund jedoch wiederum Art. 9 Abs. 2 DSGVO entspricht.

Art. 9 Abs. 2 lit g. DSGVO gestattet die Verarbeitung besonderer Kategorien personenbezogener Daten nicht zu jedem beliebigen von den Mitgliedsstaaten verfolgten öffentlichen Interesse, sondern nur zur Wahrung eines „erheblichen“ öffentlichen Interesses. Nicht ausreichend sind dafür also Interessen, die zwar der Allgemeinheit dienen, die für diese jedoch nicht so erheblich sind, dass die Allgemeinheit ohne die in Rede stehende Maßnahme ernsthaft beeinträchtigt wäre,

Schiff in Ehmann/Selmayr/Schiff, 2. Aufl. 2018, DS-GVO Art. 9 Rn. 52.

§ 22 Abs. 1 Nr. 2 BDSG spezifiziert insoweit, dass die Verarbeitung besonderer Kategorien personenbezogener Daten durch öffentliche Stellen u.a. zulässig ist, wenn dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit, zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist. Für die Gefahrenabwehr wird insoweit verlangt, dass die zu schützenden Rechtsgüter hinreichend qualifiziert sein müssen,

Petri in Simitis/Hornung/Spieker gen. Döhmann, Datenschutzrecht, Art. 9 DSGVO, Rn. 69; Schiff in Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 9 Rn. 54.

Alledem wird die Verarbeitung besonderer Kategorien personenbezogener Daten durch das BAMF jedoch nicht gerecht. Diese dient laut § 15a AsylG zur Feststellung von Identität – also Namen, Geburtsort und -datum – sowie der Staatsangehörigkeit. Die Feststellung ist über die verarbeiteten Daten nicht möglich (dazu unten genauer, unter V.0), und dafür dürfte im Regelfall nicht erforderlich sein, Daten besonderer Kategorien zu verarbeiten. An der hier offenkundig intendierten bloßen Plausibilisierung von Angaben und der Ermittlung von Indizien bei der Feststellung von Identität und Staatsangehörigkeit dürfte zudem keinesfalls ein erhebliches öffentliches Interesse bestehen.

V. Verstoß gegen den Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c DSGVO, Art. 6 Abs. 3 Satz 4

Nach dem Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Die drei Merkmale „angemessen“, „erheblich“ und „auf das notwendige Maß beschränkt“ ergeben zusammen genommen die Vorgabe, dass die Datenverarbeitung zur Erreichung des festgelegten Verarbeitungszwecks erforderlich sein muss. Sie sind zwar schwer trennscharf zu definieren, in ihnen klingen jedoch unterschiedliche Aspekt an,

Herbst, in: Kühling/Buchner, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 57.

Die BAMF-Datenverarbeitung dient dazu, Namen, Geburtsdatum und -ort sowie Staatsangehörigkeit der papierlosen Geflüchteten festzustellen (dazu unter 1). Zu diesem Zweck sind die verarbeiteten Daten jedoch weder angemessen und erheblich (dazu unter 2) noch auf das dazu notwendige Maß beschränkt (dazu unter 3).

1. Zweck der Datenverarbeitung

Die Erheblichkeit und Angemessenheit der Datenverarbeitung sind am Zweck der Datenverarbeitung zu messen. Nach Art. 5 Abs. 1 lit. b DSGVO 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. Dieser zentrale Grundsatz der Zweckbindung der Datenverarbeitung ist bereits in der EU-Grundrechtecharta verbürgt, derzufolge personenbezogene Daten nur für festgelegte Zwecke verarbeitet werden dürfen (Art. 8 Abs. 2 Satz 1 GRCh). Der für die Datenverarbeitung Verantwortliche muss also Zwecke der Datenverarbeitung konkret und präzise festlegen. Der Grundsatz der Zweckbindung soll gewährleisten, dass betroffene Personen darauf vertrauen können, dass ihre Daten nur zu den von ihr oder einem Gesetz erlaubten Zwecken verarbeitet werden und ihnen dies möglichst genau bekannt ist,

Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 5 Rn. 65f.

Der Zweck der Datenverarbeitung ist in § 15a Asylgesetz festgelegt, nämlich die Feststellung von Identität und Staatsangehörigkeit. Festgestellt werden sollen damit insbesondere Namen, Geburtsort und -datum sowie Nationalität.

Eindeutig ist ein Zweck, wenn er von anderen möglichen Zwecken klar zu unterscheiden ist, also ausdrücklich benannt und konkret bestimmt ist und legitim ist er, wenn er rechtmäßig und von der Rechtsordnung gebilligt ist,

Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 5 Rn. 71, 76 und Rn. 90f.

Identität und Staatsangehörigkeit, soweit möglich, festzustellen, ist ein im Rahmen des Asylverfahrens rechtmäßiger und legitimer Zweck. Der Zweck ist zudem eindeutig, also abgrenzbar und konkret festgelegt.

2. Mangelnde Angemessenheit und Erheblichkeit der Daten für die Klärung von Staatsangehörigkeit und Identität
Die Erhebung der Daten ist aber nicht angemessen oder erheblich.

Dem Zweck angemessen sind personenbezogene Daten, wenn sie entweder überhaupt einen Bezug zum Verarbeitungszweck haben bzw. der Bezug nicht beanstandet werden kann,

so Herbst in Kühling/Buchner/Herbst, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 57; Frenzel in Paal/Pauly/Frenzel, 2. Aufl. 2018, DS-GVO Art. 5 Rn. 35.

Teilweise wird darüber hinaus gefordert, dass die Datenverarbeitung nur dann angemessen ist, wenn sie bezogen auf den Zweck hinsichtlich Funktion, Inhalt und Umfang sachgerecht sind,

so Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 5 Rn. 119.

Die Erhebung personenbezogener Daten ist im Sinne des Art. 5 Abs. 1 lit. c erheblich, wenn sie jedenfalls für irgendeinen Aspekt des Zwecks entscheidend sind. Nicht ganz einheitlich wird beurteilt, ob der Zweck der Datenverarbeitung lediglich im Sinne einer „Geeignetheit“ gefördert werden muss oder ob nur ein Beitrag der Datenverarbeitung erheblich ist, der zur Zweckerreichung *entscheidend* ist.

Für einen derart entscheidenden Beitrag spricht sich *Roßnagel* aus (in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DSGVO Rn. 120). Für eine bloße Geeignetheit hingegen *Herbst* (in Kühling/Buchner/Herbst, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 57).

Datenverarbeitungen des BAMF sind nicht auf derart angemessene und erhebliche Datenverarbeitungen begrenzt (dazu 1.), die verarbeiteten Daten sind insgesamt nicht hinreichend aussagekräftig, um erheblich zu sein (dazu 2.). Diese Erkenntnis wird durch die Ergebnisse der Auswertungen gestützt (dazu 3.).

a. Keinerlei Begrenzung auf erhebliche und angemessene Daten beim Auslesen der Daten
Die Datenverarbeitung des BAMF ist nicht auf solche Daten beschränkt, die erheblich sein können. Es liest nämlich einen vollständigen Rohdatensatz aus den Mobiltelefonen Geflüchteter aus und verarbeitet dabei große Mengen von Daten, die keinerlei Aufschluss über Identität und Staatsangehörigkeit geben können und auch vom BAMF nicht dafür verwendet werden sollen.

b. Keine hinreichende Aussagekraft der zum Ergebnisreport verarbeiteten Daten
Auch die dann im Ergebnisreport weiter verarbeiteten Daten sind nicht erheblich. Im Ergebnisreport der Handydatenauswertungen des BAMF werden Metadaten zusammengestellt, die Aussagen treffen über die Ländervorwahlen ein- und ausgehender Anrufe und Nachrichten sowie von Kontakten, über in E-Mails, im Browserverlauf und in Nachrichten verwendete Sprache sowie über die im Browserverlauf verwendeten Länderendungen und die GPS-Daten aus Fotos und Apps.

Zusätzlich werden Login-Daten von Apps, also zum Beispiel Namen oder Mailadressen, im Klartext angegeben.

Diese vom BAMF bei der softwaregestützten Auswertung erhobenen Daten sind nicht hinreichend aussagekräftig, um entscheidend oder überhaupt irgendwie zur beabsichtigten Klärung von Staatsangehörigkeit und Identität beizutragen.

In einem verwaltungsgerichtlichen Verfahren könnte das BAMF mit dem Ergebnisreport die Behauptung, die Person habe eine andere als die bei der Anhörung angegebene Staatsangehörigkeit, nicht nachweisen. Maßgeblich sind gem. § 98 VwGO die Vorschriften der ZPO über das Beweisverfahren. Bei dem Ergebnisreport handelt es sich um ein elektronisches Dokument einer öffentlichen Stelle, dass nach § 371a Abs. 3 i.V.m. § 418 ZPO vollen Beweis der darin bezeugten Tatsachen begründet. Bezeugt werden im

Ergebnisreport aber allenfalls die dort erfassten Merkmale, nicht die Staatsangehörigkeit selbst. Hierfür stellen sie lediglich ein Indiz dar, das die asylsuchende Person durch den Vortrag alternativer Erklärungsansätze widerlegen kann.

So kann die Auswertung der Verbindungsdaten zwar zeigen, dass die betroffene Person häufig mit bestimmten Ländervorwahlen kommuniziert. Daraus können jedoch keine Rückschlüsse auf die Staatsangehörigkeit der Anschlussinhaber*innen abgeleitet werden. Noch weniger können daraus Schlüsse über die Staatsangehörigkeit der geflüchteten Person gezogen werden. Regelmäßige Kontakte in ein Land können insbesondere daraus resultieren, dass jemand dort eine Zeit lang gelebt hat oder sich gegenwärtig Angehörige oder Bekannte dort aufhalten. Gerade bei Menschen auf der Flucht ist es wahrscheinlich, dass ihr Familien- und Bekanntenkreis aus dem Heimatland sich ebenfalls nicht mehr dort, sondern in unterschiedlichen Ländern befindet, oder aber, dass sie mit Menschen im Kontakt stehen, die sie auf der Flucht oder im neuen Gastland kennengelernt haben. Die Auswertung von Ländervorwahlen ist damit weder angemessen noch erheblich, da bereits kein Bezug zum Verarbeitungszweck besteht, dieser jedoch keinesfalls irgendwie nennenswert gefördert wird.

Die auf einer Karte dargestellten Geolokationsdaten geben ebenfalls keine Hinweise auf die Staatsangehörigkeit. Sie können aus Fotos und Apps abgeleitet auf Aufenthalte in einem Land hinweisen, wobei solche GPS-Daten jedoch als besonders fehleranfällig gelten. Einzelne Geotags können deshalb nichts beweisen, weil die zugrundeliegenden Bilder von einem anderen Gerät stammen oder die Ortung gestört sein kann. Allenfalls eine größere Anzahl von Fotos mit Ortsinformationen kann ein Indiz dafür sein, dass sich Gerät und Besitzer an diesem Ort befunden haben. Eine Verarbeitung von GPS-Daten ist aufgrund des schwierig zubeurteilenden, eher fernen Bezugs zum Zweck bereits nicht angemessen, keinesfalls aber erheblich.

Die vom BAMF untersuchten Daten können Aussagen treffen über die Sprache, in der eine Person kommuniziert. Der Zusammenhang zwischen verwendeter und untersuchter Sprache zu Nationalität besteht jedoch allenfalls mittelbar. Im neuen Land angekommen ist ohnehin zu erwarten, dass ein Teil der Kommunikation auf Deutsch oder Englisch geschieht. Ob die BAMF-Software alle Sprachen erfasst, in der eine Person kommuniziert, hat viel mit dem Kommunikationskanal zu tun, den eine Person verwendet. Denn nicht alle Messenger werden von der BAMF-Software untersucht. Kommuniziert die Person mit ihrer Familie immer auf einem bestimmten Weg, wird dieser aber nicht erfasst, so taucht die Sprache im Ergebnisreport nicht auf. Ob die Person in der Landessprache ihres Herkunftslandes

kommuniziert, hat wiederum damit zu tun, ob eine Person eine Migrationsgeschichte in der Familie hat, zu einer Minderheit gehört oder auch einfach zu einer bestimmten sozialen Schicht. So können Asylsuchende auch Sprachen bzw. Dialekte sprechen, die in dem Land ihrer Staatsangehörigkeit nicht verbreitet sind. Das ist beispielsweise der Fall, wenn Flüchtlinge einer Minderheit angehören, (z.B. während der Flucht) für längere Zeit im Ausland gelebt haben oder in einer Familie aufgewachsen sind, die (teilweise) nicht aus ihrem Heimatland stammt. Wenn hypothetisch etwa Deutschland wieder zum Ausgangspunkt von Migrationsbewegungen würde, dann fänden sich unter den Menschen mit deutschem Pass auch zahlreiche Individuen, deren bevorzugte Kommunikationssprache beispielsweise Italienisch, Vietnamesisch, Griechisch oder Türkisch ist. Dieses Gedankenexperiment macht deutlich, dass die Praxis der Sprachenanalyse seitens des BAMF schon im Ansatz verfehlt und damit ungeeignet ist.

Daten über die in Textnachrichten verwendete Sprachen geben zudem in vielen Fällen nicht einmal einen Hinweis auf ein bestimmtes Land, werden viele Sprachen – namentlich diejenigen früherer europäischer Kolonialmächte – doch in zahlreichen Ländern gesprochen. Auch die Verbreitung der von der Software erhobenen arabischen Dialekte deckt sich nicht mit den Staatsgrenzen. So wird Tschadisch-Arabisch (Schuwa) im Tschad, Südsudan, Sudan, Kamerun, Niger, Nigeria und der Zentralafrikanischen Republik gesprochen. Golf-Arabisch (Chalidschi) ist in Bahrain, Irak, Kuwait, Katar, den Vereinigten Arabischen Emiraten, Saudi-Arabien, Iran und im Oman verbreitet. Und levantinisches Arabisch wird in Jordanien, den palästinensischen Autonomiegebieten und Israel sowie in Syrien gesprochen. Nach alldem erscheint die Verarbeitung der seitens des BAMF verwendeten Daten jedenfalls nicht erheblich, weil sie keinen sinnvollen Beitrag zur Feststellung der Identität und Staatsangehörigkeit leisten kann.

Weiter können die Daten Aussagen darüber treffen, mit welchen Namen oder Mailadressen bestimmte Apps genutzt werden. Das kann jedoch keinen verlässlichen Rückschluss auf den tatsächlichen Namen einer Person zulassen. Auch die Identität von Asylsuchenden lässt sich mit den von der Software gespeicherten Daten nicht zuverlässig ermitteln. Viele Menschen geben in E-Mail-Adressen und als Login-Daten bei Apps nicht ihren bürgerlichen Namen, sondern einen Spitz- oder Fantasienamen an. Gerade unter Geflüchteten ist die Wahrscheinlichkeit, dass sie ihre Identität im Netz geheim zu halten wünschen, sogar wahrscheinlicher. Diese Klardaten sind damit also weder angemessen noch erheblich.

Zu beachten ist schließlich, dass Asylsuchende ein erst vor kurzem erworbenes Mobiltelefon ohne aussagekräftige Datenbestände besitzen können. Auch kann ein Mobiltelefon einen

widersprüchlichen Datenbestand haben, etwa wenn mehrere Personen das Telefon nutzen oder das Mobiltelefon zuvor einer anderen Person gehörte und die Daten nicht vollständig gelöscht wurden. Es ist angesichts der häufig unbrauchbaren Ergebnisse der Handydatenauswertungen plausibel, dass dies einen nennenswerten Teil der Geflüchteten betrifft.

Dass die Datenverarbeitung daher entscheidend dem Zweck der Feststellung der Identität und Staatsangehörigkeit dient, ist nicht zu erkennen.

c. Ergebnis der Datenauswertungen stützt diese Erkenntnis

Das Ergebnis der Datenauswertungen stützt die Erkenntnis, dass es auf die Handydatenauswertungen nicht entscheidend ankommt. So wurden in weniger als 50 % der Fälle keine Freigabe der ausgelesenen Daten beantragt und in einem substantiellen Teil die Freigabe verweigert. Vor allem aber führt die Datenverarbeitung selbst nach Zahlen des BAMF nur in 2 % der Fälle zu einem Widerspruch zu den Angaben des geflüchteten Menschen – und dabei ist noch unklar, ob diese Zweifel einer etwaigen gerichtlichen Überprüfung standhalten würden. Mit anderen Worten verarbeitet das BAMF die Daten von zumindest 49 von 50 betroffenen Personen völlig unnötig – und dies bei mitunter tiefen Eingriffen in die Privatsphäre.

3. Datenverarbeitung über das notwendige Maß hinaus

Darüber hinaus verstößt die Datenauswertung im Asylverfahren aus weiteren Gründen gegen den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO. Nach dem Grundsatz der Datenminimierung muss die Datenverarbeitung auf das notwendige Maß beschränkt sein. Nach diesem Grundsatz dürfen personenbezogene Daten nur verarbeitet werden, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann, (vgl. dazu: Erwägungsgrund Nr. 50 DSGVO).

Daraus ergibt sich, dass auf personenbezogene Daten nur dann zurückgegriffen werden darf, wenn keine alternative Methode zur Verfügung steht, um den mit der Verarbeitung angestrebten Zweck zu erreichen,

> *Heberlein* in Ehmann/Selmayr, DS_GVO, 2. Auflage 2018, Art. 5 Rn. 22, ähnlich *Roßnagel* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 5 Rn. 121.

Die Datenauswertung ist zu umfassend und nicht hinreichend begrenzt (dazu a.) und sie ist in den meisten Fällen nie und jedenfalls vor einer Anhörung nicht notwendig (dazu b).

a. Keine Begrenzung des Umfangs der Datenauswertung auf notwendige Daten
Erstens werden nach dem praktizierten Verfahren im Sinne eines Gesamtdatenansatzes jegliche Daten aus dem Datenträger ausgelesen. Die Beschränkung auf das notwendige Maß bedeutet, dass es sein kann, dass Daten, die angemessen und erheblich sind, dennoch in Umfang, Genauigkeit, Dichte oder in Aussagekraft weiter gehen, als der Zweck dies unbedingt erfordert,

> Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 5 Rn. 121.

Sollten die ausgelesenen Handydaten entgegen der hier vertretenen Ansicht für erheblich eingestuft werden, so gehen sie doch jedenfalls in ihrem Umfang und Genauigkeit weiter, als der Zweck dies unbedingt erfordert. Eine Beschränkung auf notwendige Daten findet gerade nicht statt.

b. Eine Feststellung von Identität und Staatsangehörigkeit kann ohne Handydatenauswertungen erfolgen
Die Feststellung von Identität und Staatsangehörigkeit kann ohne Handydatenauswertung erfolgen. Selbst in den Fällen, in denen Handydaten ausgewertet und zu Rate gezogen werden, wird diesen Daten nur eine Indizwirkung beigemessen, sie sind also immer nur eine unwesentliche, zusätzliche Information.

Wenn das BAMF Datenträger ausliest, dann tut es das bereits bei der Registrierung von Asylsuchenden als Routinemaßnahme bei all denjenigen, die keinen vom BAMF anerkannten Pass oder Passersatz vorweisen können. Es wird demnach nicht abgewartet und beurteilt, ob durch andere Maßnahmen – etwa im Rahmen der Anhörung – etwaige Zweifel an der Identität oder der Staatsangehörigkeit überhaupt fortbestehen. Stattdessen erfolgen die eigenständigen Datenverarbeitungsvorgänge der Auslesung von Datenträgern und der Speicherung des Ergebnisreports auf Vorrat. Datenverarbeitungen auf Vorrat sind unvereinbar mit dem Grundsatz der Datenminimierung,

> Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 5 Rn. 121, unter Verweis auf BVerfGE 65, 1 (46).

Die Datenträgerauswertung ist insgesamt, jedenfalls aber vor einer Anhörung gerade nicht notwendig zur Zweckerreichung. Eine Auslesung und Auswertung ist gänzlich verzichtbar und könnte zumindest aber auf einen späteren Zeitpunkt verschoben werden, wenn Zweifel aufgekommen sind.

Auch diese Erkenntnis wird durch die Ergebnisse der Datenträgerauswertungen gestützt: Ausweislich der von der Bundesregierung genannten Zahlen (oben B.1) beantragen Sachbearbeiter*innen des BAMF in weniger als 50 % der Fälle tatsächlich den Zugriff auf die Ergebnisprotokolle der Auswertungen. Auch sie erachten damit offensichtlich die Datenauswertung für nicht notwendig, um Zweck, Identität und Staatsangehörigkeit festzustellen.

VI. Verstoß gegen Grundsatz der Datenrichtigkeit, Art. 5 Abs. 1 lit. d DSGVO

Art. 5 Abs. 1 lit. d DSGVO kodifiziert den Grundsatz, dass die verarbeiteten personenbezogenen Daten sachlich richtig sein müssen. Sachlich richtig sind Daten, die bezogen auf den Zweck der Datenverarbeitung den relevanten Ausschnitt aus der Realität korrekt darstellen,

> Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 5 Rn. 139.

Die softwaregestützte Datenträgerauswertung generiert in erheblichem Umfang Daten, die entweder sachlich unzutreffend sind oder deren Richtigkeit für keinen der Beteiligten zu ermitteln ist.

Da der Rohdatensatz, der durch das BAMF untersucht wird, anschließend gelöscht wird, gibt es keinen originalen Datensatz, der herangezogen werden könnte, um die Richtigkeit der ermittelten Ergebnisse überprüfen zu können. Die im Ergebnisprotokoll angegebenen Daten sind größtenteils Metadaten, so dass jeglicher Kontext fehlt, um zu überprüfen, ob ein Ergebnis richtig ist.

Bei den von der Software erfassten Geolokationsdaten ist nicht klar, ob sich die betroffene Person selbst an dem auf der Karte im Ergebnisreport verzeichneten Ort aufgehalten hat. Viele Menschen haben auf ihren Smartphones eine Vielzahl von mit Ortsangaben (sogenannte Geotags) versehenen Fotos gespeichert, die ihnen zugesendet worden sind. Geotags sind zudem sehr fehleranfällig. In diesem Sinne wird auch im Ergebnisreport des Beschwerdeführers ausgeführt, dass „aufgrund der hochdynamischen Natur der App-Daten" nicht in jedem Fall garantiert werden kann, dass sich das Gerät auch am erkannten Ort befunden habe (Bl. 42 d.A.).

Bei der Spracherkennungssoftware bestehen Zweifel, ob sie Sprachen und insbesondere arabische Dialekte zutreffend zuordnet. Gerade die Tatsache, dass es bei der Transkription arabischsprachiger Nachrichten in lateinische Zeichen oftmals mehrere Möglichkeiten gibt,

kann leicht zu Zuordnungsfehlern führen. Da Zuordnungsfehler bei arabischen Dialekten sehr viel wahrscheinlicher sind als bei mit lateinischem Alphabet geschriebenen Sprachen, werden zudem arabischsprechende Asylsuchende benachteiligt. Verschiedene Sprachwissenschaftler*innen bezweifeln, ob die Sprachzuordnung zuverlässig sein kann,

> siehe u.a. bei P. Hummel: Software soll Dialekt von Asylbewerbern untersuchen, Die Welt v. 17.03.2017, https://www.welt.de/wissenschaft/article162926845/Software-soll-Dialekt-von-Asylbewerbern-untersuchen.html; A. Biselli: Software, die an der Realität scheitern muss, ZEIT Online v. 17.03.2017, https://www.zeit.de/digital/ internet/2017-03/bamf-asylbewerber-sprach-analyse-software-computerlinguistik.

Die Bundesregierung hat auf eine Kleine Anfrage gegenüber dem Deutschen Bundestag eingeräumt, dass die Fehlerquote bei der Dialekt-/Spracherkennung bei etwa 15 Prozent liege,

> BT-Drs. 19/6647 vom 19. Dezember 2018, als **Anlage 10**, Antwort auf Frage 11.

Eine weitere Fehlerquelle ergibt sich dadurch, dass die Software möglicherweise einige der verwendeten Apps nicht auslesen kann. Dadurch kann das Ergebnis verzerrt werden. Dies ist etwa der Fall, wenn die*der Antragsteller*in vor allem über Apps kommuniziert, die vom System des BAMF nicht unterstützt werden, oder wenn die Ländervorwahlen von eingehenden Nachrichten analysiert werden, ein*e Antragsteller*in aber vor allem über Messenger kommuniziert, die keine Telefonnummer als Identifikationsmerkmal nutzen und demnach auch keine Ländervorwahl enthalten. Dann wird nur ein Teil der tatsächlichen Kommunikation ausgewertet, und es kann leicht eine Verzerrung der Ergebnisse entstehen. Das ist zum Beispiel bei dem populären Messengerdienst Telegram so. Schließlich ist zu beachten, dass Daten von Datenträgern erhoben werden können, die gar nicht von deren Besitzer*in stammen. Neben der Tatsache, dass auf einem Datenträger Daten gespeichert sein können, die der ihn nutzenden Person zugesendet worden sind, ist auch denkbar, dass jemand einen Datenträger von einer anderen Person übernommen hat, ohne dass deren Benutzerprofil zuvor vollständig gelöscht wurde. Zudem kann es vorkommen, dass Datenträger durch mehrere Personen genutzt werden, sich z.B. eine Person dort für eine App angemeldet hat. Schließlich erscheint es nicht völlig ausgeschlossen, dass einzelne Asylsuchende in Kenntnis der Untersuchungen (bestimmte) Daten von ihren Telefonen löschen und dadurch das Ergebnis verfälschen. Der Bundesregierung sind laut eigener Aussage zumindest einzelne Fälle bekannt, in denen Antragsteller*innen „manipulierte“ Mobilgeräte vorgelegt haben.

Ob bei der Erzeugung des Ergebnisreports zutreffende Daten dargestellt werden, ist für die Bediensteten des BAMF nicht erkennbar. Sie kennen die Algorithmen nicht und haben keinen technischen Sachverstand, um die Zuverlässigkeit der automatisierten Erhebung einzuschätzen. Handreichungen des BAMF für seine Bediensteten, wie sie feststellen können, dass Datenträger nur unvollständig ausgewertet worden sind und dass keine von Dritten erzeugten Daten erhoben worden sind, finden sich nicht.

Auch die Verwaltungsgerichte haben in etwaigen Rechtsstreitigkeiten in aller Regel keine Möglichkeit, die sachliche Richtigkeit und den Beweiswert der vom BAMF ermittelten Daten und durch die Software des BAMF gezogenen Schlüsse im Ergebnisreports einzuschätzen. Anders als sonstige Beweismittel in Gerichtsverfahren kann die Qualität und Zuverlässigkeit der Datenträgerauswertung überhaupt nicht überprüft oder in Zweifel gezogen werden. Denn dazu wäre es notwendig, dass das BAMF die zugrunde liegenden Algorithmen offenlegt oder extern überprüfen ließe, um beispielsweise Fehlerquoten klar zu machen. Besonders bei der Spracherkennung wäre zwingend notwendig, dass das BAMF offenlegt, welchen „Trainingsdatensatz“ das BAMF verwendet, also wie viele Sprachproben welcher Sprache der Software als Lerndatensatz zugrunde gelegt wurde. Eine externe Überprüfung dieser Software ist aber weder individuell im Verfahren möglich noch behördlicherseits erfolgt. Angesichts der Schwere der möglichen Folgen einer falschen Entscheidung im Asylverfahren widerspricht dies dem Rechtsstaatsgebot (Art. 20 Abs. 3 GG).

Zugleich wird es durch diesen Mangel an Offenlegung der Algorithmen faktisch unmöglich, die Löschungspflicht nach Art. 5 Abs. 1 lit. d DSGVO durchzusetzen: Wenn die betreffende Person erst gar nicht prüfen kann, ob die Daten sachlich richtig sind, kann sie auch keine Löschung verlangen.

VII. Unverhältnismäßigkeit der Rechtsgrundlage, Art. 6 Abs. 3 Satz 4 DSGVO, Art. 52 GRCh

Die DSGVO ermächtigt die Mitgliedsstaaten in Art. 6 Abs. 3 Satz 1 lit. b i.V.m. Abs. 1 UAbs. 1 lit. e, Rechtsgrundlagen zur Datenverarbeitung im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt zu schaffen. Diese müssen nach Art. 6 Abs. 3 Satz 4 DSGVO jedoch verhältnismäßig zum verfolgten legitimen Zweck sein. Diese Voraussetzung ergibt sich bereits aus dem Unionsverfassungsrecht, da gemäß Art. 52 Abs. 1 Satz 2 GRCh eine gesetzliche Erlaubnis zur Verarbeitung personenbezogener Daten und damit eine Einschränkung des Grundrechts auf Datenschutz nach Art. 8 GRCh und Art. 16 AEUV nur „unter Wahrung des Grundsatzes der Verhältnismäßigkeit“ zulässig ist.

1. Geeignetheit und Erforderlichkeit
Jede Einschränkung von Grundrechten muss in Hinblick auf das verfolgte Ziel geeignet sein. Dabei genügt es grundsätzlich, wenn das Ziel zumindest gefördert wird,

> EuGH, C-92/09 – Schecke, Slg.2010, I-11063 Rn.72; Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta Art. 8 Rn. 17.

Zudem muss die betreffende Datenverarbeitung gem. Art. 52 Abs. 1 Satz 2 zur Erreichung dieses Ziels erforderlich sein. Sie darf nicht über das zur Erreichung des Ziels Erforderliche hinausgehen, es darf kein milderes Mittel zur Verfügung stehen,

> Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta Art. 8 Rn. 17 mwN.

Im Bereich der Datenverarbeitung findet eine verschärfte Geeignetheitsprüfung bereits im Rahmen der Prüfung der Datenminimierung, insbesondere bei der Angemessenheit und Erheblichkeit (Art. 5 Abs. 1 lit. c, siehe oben unter V.0), wie auch unter dem Gebot der Datenrichtigkeit statt (Art. 5 Abs. 1 lit. d DSGVO, siehe oben unter 0).

Auch eine verschärfte Prüfung der Erforderlichkeit findet sich bereits unter dem Gebot der Datenminimierung, und zwar der Begrenzung von Datenverarbeitungen auf das notwendige Maß (Art. 5 Abs. 1 lit. c DSGVO, siehe oben unter V.).

2. Angemessenheit
Eigenständige Bedeutung kommt jedoch der Prüfung der Angemessenheit im Rahmen von Art. Abs. 3 Satz 4 DSGVO zu. Zudem darf die durch die Datenverarbeitung verursachte Belastung für den Grundrechtsträger nicht in einem unangemessenen Verhältnis zu den verfolgten Zielen stehen. Insoweit müssen die Belange „ausgewogen gewichtet“ werden,

> Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta Art. 8 Rn. 17 mwN.

Eine derartige ausgewogene Gewichtung der betroffenen Belange ist jedoch in der Normenstruktur von § 15 Abs. 2 Nr. 6 und § 15a AsylG nicht angelegt.

Werten staatliche Stellen ein informationstechnisches System aus, auf dem sich eine Vielzahl von Daten befinden, die erhebliche Rückschlüsse über das Leben der Betroffenen zulassen, liegt darin ein intensiver Grundrechtseingriff. Zwar erfolgt in der derzeitigen Praxis im Wesentlichen nur eine automatisierte Auswertung von Metadaten, während Bedienstete des BAMF keine auf dem Datenträger gespeicherten Kommunikationsinhalte lesen. Doch greift die automatisierte Auswertung auf einen immensen Datenbestand zu. So verbinden insbesondere Smartphones große Mengen persönlicher Daten und enthalten

gewissermaßen den gesamten digitalen Hausstand: Nachrichten an Familienmitglieder, Kontaktdaten inklusive Informationen über Anwält*innenkontakte, Konto-und Zahlungsdaten, Zugang zu E-Mail-Accounts, die Suchmaschinen-Historie, Aufenthaltsdaten, intime und persönliche Fotos. Aus Smartphone-Daten lassen sich Bewegungsprofile und soziale Netzwerke ableiten, sie ermöglichen das Erstellen von detaillierten Persönlichkeitsprofilen ihrer Nutzer*innen.

Auch die Aussagekraft von Telekommunikationsverbindungsdaten ist weitreichend. Je nach Nutzung von Telekommunikationsdiensten seitens der Betroffenen lassen sich tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten gewinnen.

Der Eingriff hat zudem eine erheblich Streubreite. Nach Angaben des Bundesministeriums des Innern wurden im Jahr 2018 insgesamt 11.389 Datenträger ausgelesen. Die gesetzlichen Voraussetzungen erfüllen indes deutlich mehr Personen. So konnten laut Innenministerium im Jahr 2018 45.322 Antragsteller*innen keine Identitätspapiere vorlegen, das entspricht 54,2 Prozent. 2019 konnten 34.938 Antragsteller*innen keine Papiere vorlegen, was 49,1 Prozent der Antragsteller*innen entsprach,

> Antwort auf Kleine Anfragen von die Linke, BT-Drs. 19/8701, **Anlage 5**, S. 27 und BT-Drs. 19/18498, **Anlage 6**, S. 31.

Dies entspricht den Schätzungen der Bundesregierung im Vorfeld der Gesetzesänderung. In der Begründung des Gesetzentwurfs wurde im Rahmen des Erfüllungsaufwandes angenommen, dass eine Datenträgerauswertung bei 50 bis 60 Prozent der Antragsteller*innen angezeigt sei. Basierend auf der Anzahl von 280.000 registrierten Asylsuchenden im Jahr 2016 ging die Bundesregierung von jährlich 150.000 Personen aus, bei denen eine Datenträgerauslesung in Betracht käme,

> BT-Drs. 18/11546, **Anlage 7**, S.15.

Erfasst werden somit die Daten einer Vielzahl von Personen ohne Anknüpfung an ein zurechenbar vorwerfbares Verhalten oder einen individuell begründeten Verdacht. Gerade daraus ist eine besondere Grundrechtsgefahr abzuleiten,

> vgl. BVerfGE 125, 260 (318).

Die Erhebung von Telekommunikationsverbindungsdaten hat zudem immer auch zur Folge, dass personenbezogene Daten Dritter miterhoben werden.

Der Eingriff wird dadurch vertieft, dass das Gesetz zur Auslesung und Auswertung einer Vielzahl von Geräten ermächtigt. Die gesetzlichen Regelungen beschränken die Maßnahme nicht auf Smartphones, der Begriff „Datenträger“ ermöglicht grundsätzlich ebenso die Auswertung anderer Geräte, etwa als Featurephone bezeichnete einfachere Modelle von Mobiltelefonen, aber auch USB-Sticks, Festplatten, Tablets, Laptops oder sogar Fitnessarmbänder.

Die Datenträgerauswertung ist auch deshalb ein schwerwiegender Grundrechtseingriff, weil die Betroffenen im Vorfeld der Anhörung eingeschüchtert werden. Da ihnen nicht mitgeteilt wird, in welcher Weise ihr Datenträger ausgewertet wird und sie keinen Einblick in den Ergebnisreport erhalten, müssen sie davon ausgehen, dass den Personen, die die Anhörung durchführen und die über den Asylantrag entscheiden, alle darauf gespeicherten Informationen bekannt sind oder dass der Datenträger zumindest zur Nachprüfung ihrer Angaben bei der Anhörung umfassend durchsucht werden könnte. Die Asylsuchenden wissen nicht, was das BAMF über sie weiß, wissen aber, dass es vieles, auch Höchstpersönliches über sie wissen kann. Dadurch kann bei ihnen ein diffuses Bedrohungsgefühl entstehen.

Der Eingriff weist überdies, erstens, aufgrund der existenziellen Bedeutung des grundrechtlich geschützten Asylverfahrens eine nochmals besondere Intensität auf, trifft, zweitens, mit Asylsuchenden eine besonders vulnerable Bevölkerungsgruppe, und hat, drittens, aufgrund der Anwendung in nur bestimmten Fallkonstellationen hinsichtlich einzelner Länder ein diskriminierendes Momentum.

Auf der anderen Seite kann das – überdies nur mittelbare – Ziel der §§ 15 Abs. 2 Nr. 6, 15a AsylG – nämlich das Asylverfahren zu effektivieren und vor Missbrauch zu schützen – diesen Eingriff nicht rechtfertigen. Das bloße Ziel, die Glaubhaftigkeit von Angaben im Asylverfahren zu prüfen und damit allgemein die Effektivität von Verwaltungshandeln sicherzustellen und konkret und im Ergebnis im vorliegenden Kontext das Aufenthaltsrecht von Menschen zu versagen, wenngleich keine Anhaltspunkte bestehen, dass die betreffenden Personen hochrangige Rechtsgüter durch Straftaten beeinträchtigen werden, rechtfertigt eine derart eingriffsintensive Maßnahme nicht. Das gilt umso mehr, als die Daten des Ergebnisreports zur Feststellung der Staatsangehörigkeit lediglich Indizien abgeben und keinen Beweis erbringen.

VIII. Verstoß gegen das Transparenzgebot und Informationspflichten, Art. 5 Abs. 1 lit. a Alt. 3, Art. 13 DSGVO

Nach Art. 4 Abs. 1 lit. a Alt. 3 DSGVO müssen personenbezogene Daten „in einer für die betroffene Person nachvollziehbaren Weise“ verarbeitet werden.

Der Grundsatz der Transparenz beschränkt sich nicht auf ein Auskunftsrecht der betroffenen Person, sondern umfasst alle Informationen und Informationsmaßnahmen, die erforderlich sind, damit die betroffene Person überprüfen kann, ob die Datenverarbeitung rechtmäßig ist, und ihre Rechte wahrnehmen kann. Denn ohne ausreichende Transparenz wird die betroffene Person faktisch rechtlos gestellt,

> Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 5 Rn. 50; BVerfGE 65, 1 (46, 59).

Der Grundsatz begründet für den Verantwortlichen Pflichten, ausreichende Transparenz zu gewährleisten. Erhebt er personenbezogene Daten bei der betroffenen Person – wie vorliegend das BAMF – ist er nach Art. 13 verpflichtet, auch ohne dass eine betroffene Person dies einfordert, sie zum Zeitpunkt der Datenerhebung über die in Art. 13 Abs. 1 und Abs. 2 aufgelisteten Angaben zu informieren,

> Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 5 Rn. 52).

Die verpflichtenden Angaben nach Art. 13 Abs. 1 umfassen u.a. Zweck der Datenverarbeitung und Rechtsgrundlage (lit. c), die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (lit. e). Zusätzlich muss der Verantwortliche die betroffene Person gemäß Art. 13 Abs. 2 DSGVO zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung stellen: Die Speicherdauer bzw. die Kriterien, nach denen sich die Speicherdauer bemisst (lit. a), das Bestehen eines Rechts auf Auskunft (lit. b), das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde (lit. d), ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist und welche möglichen Folgen die Nichtbereitstellung hätte (lit. e).

Zwar wurde dem Beschwerdeführer der Zweck der Datenauswertung und Rechtsgrundlage mitgeteilt (Art. 13 Abs. 1 lit. c) und er wurde darauf hingewiesen, dass er gesetzlich zur Herausgabe des Mobiltelefons und der Duldung der Datenauswertung verpflichtet sei und er wurde auch auf die mögliche rechtliche Konsequenz einer verweigerten Mitwirkungspflicht hingewiesen (Art. 13 Abs. 2 lit. 3), die darin bestehen kann, dass seine Weigerung als Rücknahme des Asylantrags gewertet wird.

Ansonsten sind die verpflichtenden Angaben und Informationen aber sämtlich nicht gewährt worden, insbesondere wurde er nicht darüber aufgeklärt, wer auf seine Daten Zugriff haben würde und in welchem Umfang (Art. 13 Abs. 1 lit. e), die Speicherdauer bzw. Kriterien zur Bemessung der Speicherdauer wurden ihm nicht mitgeteilt (Art. 13 Abs. 2 lit. a). Indem er im Anschluss an die Auswertung den Ergebnisreport nicht und damit die Tiefe des Rechtseingriffs nicht einsehen konnte, handelte es sich faktisch und im Ergebnis um eine heimliche Datenauswertung, die zugleich eine verfahrensrechtliche Kontrolle erschwert und die andererseits durch kein anderes valides Rechtsgut gerechtfertigt werden kann. Überdiese wurde der Beschwerdeführer weder auf ein Auskunftsrecht (Art. 13 Abs. 2 lit. b) noch auf sein Beschwerderecht beim Bundesdatenschutzbeauftragten (Art. 13 Abs. 2 lit. d) hingewiesen.

E. Konsequenzen

Stellt der BfDI einen Verstoß des § 15a AsylG gegen die DSGVO fest, kann er dem BAMF gem. § 58 Abs. 2 lit. f DSGVO verbieten, auf dieser Grundlage weitere Datenträgerauswertungen durchzuführen. Behörden haben zwar in national-rechtlichen Sachverhalten nach herrschender Meinung kein Recht, Gesetze außer Anwendung zu lassen, wenn sie sie für verfassungswidrig halten. Unionsrechtlich sind dagegen alle staatlichen Stellen verpflichtet, unionsrechtswidrige nationale Rechtsakte einschließlich Parlamentsgesetzen außer Anwendung zu lassen,

EuGH, Rs. 66/77, NJW 1978, 1741 – Simmenthal II.

Sollte der BfDI nicht von einem in der Rechtsgrundlage liegenden Verstoß gegen die DSGVO ausgehen, könnte er dem BAMF jedenfalls die konkrete Art und Weise der Datenträgerauswertung untersagen.

Die Anlagen sind dem Original per Post, nicht jedoch dem vorab versendeten Fax beigefügt.

Mit freundlichen Grüßen

Dr. Lehnert, Rechtsanwalt