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

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

53117 Bonn

per beA

25.06.2025

Unser Zeichen:
…

…

Sehr geehrte Damen und Herren,

nehme ich in Bezug auf das Anhörungsschreiben vom …2025 wie folgt Stellung:

Es wird nochmals angeregt, dem Bundesamt für Migration und Flüchtlinge (BAMF) gem. Art. 58 Abs. 2 lit. f DSGVO die weitere Durchführung der Datenträgerauswertung nach § 15a Abs. 1, 2 AslyG zu verbieten, da § 15a AsylG in seiner derzeitigen Form gegen die DSGVO verstößt.

Die Norm ist unionsrechts- und verfassungswidrig, da es ihr an der Geeignetheit, Erforderlichkeit, Angemessenheit sowie hinreichender Bestimmtheit mangelt und sie die Grundrechte der Betroffenen auf Schutz personenbezogener Daten gemäß Art. 8 Abs. 2 GRCh sowie auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verletzt.

Bei der rechtlichen Bewertung ist insbesondere die Absenkung der Eingriffsschwelle für die Datenauslesung durch die am 27.02.2024 geänderten Fassung des § 15a AsylG zu berücksichtigen, die weitergehende Grundrechtseingriffe erlaubt und dadurch die rechtlichen Bedenken gegen die Norm verschärft.

Aufgrund der weiten Formulierung der Rechtsgrundlage und der durch sie erfolgenden schwerwiegenden Grundrechtseingriffe ist eine verfassungs- bzw. datenschutzkonforme

Auslegung der Norm nicht möglich. Selbst eine weite Auslegung der Norm scheitert an zwingenden verfassungsmäßigen Vorgaben. Eine Auslegung darüber hinaus würde dem klaren Gesetzeswortlaut und dem gesetzgeberischen Willen zuwiderlaufen.

Im Einzelnen:

Gliederung

A. Zur Verwarnung nach Art. 58 Abs. 2 lit. b DSGVO

Das Aussprechen einer Verwarnung nach Art. 58 Abs. 2 lit. b DSGVO gegenüber dem Bundesamt für Migration und Flüchtlinge (BAMF) wird befürwortet. Der im Anhörungsschreiben vom …2025 dargelegten Rechtsauffassung wird insofern zugestimmt, als die konkrete Anordnung der Zurverfügungstellung der Zugangsdaten, das Auslesen der Daten sowie die Speicherung derselben als rechtswidrig zu bewerten sind, da mildere Mittel zur Feststellung der Identität oder Staatsangehörigkeit zur Verfügung standen. Damit lag zumindest ein fahrlässiger Verstoß gegen Art. 6 Abs. 1 DSGVO vor.

B. Zum Verbot nach Art. 58 Abs. 2 lit. f DSGVO

Entgegen der im Anhörungsschreiben vom ...2025 dargelegten Rechtsauffassung verletzte bzw. verletzt § 15a AsylG sowohl in seiner alten als auch in seiner am 27.02.2024 geänderten Fassung die Anforderungen der DSGVO in mehrfacher Hinsicht. Die Norm ist nicht hinreichend bestimmt (dazu unter I.), verstößt gegen den Grundsatz der Verhältnismäßigkeit nach Art. 6 Abs. 3 S. 4 DSVGO und verletzt damit die Betroffenen in ihrem Grundrecht auf Schutz personenbezogener Daten aus Art. 8 Abs. 2 GrCH (dazu unter II.). Darüber hinaus liegt ein Verstoß gegen die Grundsätze der Datenminimierung und Datenrichtigkeit nach Art. 5 Abs. 1 lit. c und d DSGVO (dazu unter III.) sowie gegen das Erhebungsverbot besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO vor (siehe dazu unter IV.). Schließlich wird das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verletzt. Insbesondere fehlt es an gesetzlichen Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung (dazu unter V.). Eine verfassungs- und datenschutzkonforme Auslegung kommt nicht in Betracht (dazu unter VI.).

I. Fehlende Bestimmtheit der Rechtsgrundlage, Art. 52 Abs. 1 S. 1 GRCh

Wie in der Beschwerde vom 04.02.2021 ausgeführt (D.III.), fehlt es bereits an einer hinreichend bestimmten Rechtsgrundlage. Nach dem Bestimmtheitsgebot aus Art. 52 Abs. 1 S. 1 GRCh muss die gesetzliche Grundlage zumindest adäquate Begrenzungen vorsehen, welche Daten erhoben werden dürfen und wann ein hinreichender Anlass zur Auswertung besteht.

Der EuGH führt zu den Anforderungen des Art. 52 Abs. 1 GRCh aus, dass Grundrechtseinschränkungen

> *„sich auf das absolut Notwendige beschränken [müssen], und die Regelung, die die fraglichen Einschränkungen enthält, […] klare und präzise Regeln für ihre Tragweite und ihre Anwendung vorsehen [muss]“,*
> EuGH, Urteil vom 04.10.2024 – C 548/21, Rn. 84 f. m.w.N, 98 m.w.N.

Zeitpunkt, Anlass, Reichweite der Befugnisse sowie der Umgang mit Kommunikationsinhalten und besonders sensiblen persönlichen Daten erfahren in § 15a AsylG und den flankierenden Normen in keiner Weise eine Einschränkung. Die Norm ist insofern gerade nicht klar und präzise, sondern lückenhaft und diffus. § 15a AsylG schließt weder aus, dass neben Metadaten auch gespeicherte Kommunikationsinhalte ausgewertet werden dürfen, noch enthält sie Regelungen zur Verarbeitung von automatisiert erhobenen personenbezogenen Daten besonderer Kategorien. Auch wird die Auswertung nicht auf Daten, die für die zu treffenden Feststellungen voraussichtlich geeignet sind, beschränkt. Damit ermöglicht die Norm dem Wortlaut nach Grundrechtseingriffe, die noch wesentlich weiter reichen als die derzeitige behördliche Praxis.

Mit Blick auf die Gesetzesbegründung soll mit der neuen Fassung des § 15a AsylG auch gerade sichergestellt werden, dass die Behörde ihre weitreichenden Befugnisse behält und diese nicht durch Vorgaben der Rechtsprechung eingeschränkt werden. So heißt es in der Gesetzesbegründung u.a.:

> *„Das **frühzeitige Auslesen** von Mobiltelefonen zur Identitätsklärung einer Person ist **auch weiterhin möglich**; es wurden in § 15 Absatz 1 Nummer 6 und § 15a AsylG gesetzliche Anpassungen vorgenommen, die **aufgrund der Entscheidung des Bundesverwaltungsgerichts vom 16.02.2023** (Az: BVerwG 1C 19.21) zu den Voraussetzungen der Auswertung digitaler Datenträger im Asylverfahren **erforderlich** waren. Es wird nunmehr ausdrücklich zwischen den Schritten des Auslesens und des Auswertens unterschieden.“*
> BT-Drs. 563/23, S. 20 [Hervorhebungen durch den Unterzeichner].

II. Verstoß gegen den Grundsatz der Verhältnismäßigkeit, Art. 6 Abs. 3 Satz 4 DSGVO, Art. 52 GRCh

Wie bereits in der Beschwerde vom 04.02.2021 ausgeführt (D.VII.) verstößt § 15a AsylG gegen den Grundsatz der Verhältnismäßigkeit aus Art. 6 Abs. 3 S. 4 DSGVO. Nach dieser Vorschrift muss die Rechtsgrundlage für eine Datenverarbeitung ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen. Diese Voraussetzung ergibt sich bereits aus dem Unionsverfassungsrecht, da gemäß Art. 52 Abs. 1 S. 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.

Zwar verfolgt § 15a AsylG den an sich legitimen Zweck, Asylmissbrauch zu verhindern. Durch die Datenauswertung sollen die Identität und Staatsangehörigkeit von Asylbewerbenden

festgestellt und dadurch Asylanträge nicht berechtigter Antragstellender abgelehnt und die Ausreisepflicht durchgesetzt werden können. Die Norm ist hierzu jedoch schon nicht geeignet (dazu unter 1.), erforderlich (dazu unter 2.) und in ihrer konkreten Gestaltung auch nicht angemessen (dazu unter 3.) und verletzt damit das Grundrecht auf Datenschutz der Betroffenen aus Art. 8 GRCh.

1. Ungeeignetheit

Hinsichtlich der fehlenden Geeignetheit gelten die in meiner Beschwerde bereits vorgetragenen Bedenken fort (siehe dazu ausführlich Beschwerde vom 04.02.2021, D.V.2.b.).

Eine Maßnahme der Datenerhebung und -verarbeitung ist nur dann geeignet, wenn die Daten erheblich sind und ausgeschlossen werden kann, dass unrichtige Daten verarbeitet werden (siehe Art. 5 Abs. 1 lit. c), d) DSGVO). Daran fehlt es bei der auf § 15a AsylG gestützten Datenauslesung und -auswertung.

Durch die nach § 15a Abs. 2 S. 1 AsylG durchgeführte Datenauswertung konnte in der Vergangenheit nur in ca. 2-3 % der Fälle ein Widerspruch zu den von der betroffenen Person gemachten Angaben festgestellt werden; in einem Großteil der Fälle kam es zu keinen verwertbaren Ergebnissen (z.B. in 73,2 % der Auswertungsfällen für das 1. Halbjahr 2023),

> vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Clara Bünger, Nicole Gohlke, Anke Domscheit-Berg, weiterer Abgeordneter und der Fraktion DIE LINKE. vom 05.09.2023, BT-Drs. 20/8222, S. 28, abrufbar unter: https://dserver.bundestag.de/btd/20/082/2008222.pdf; Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Clara Bünger, Nicole Gohlke, Anke Domscheit-Berg, weiterer Abgeordneter und der Fraktion DIE LINKE. vom 17.02.2023 zur ergänzenden Asylstatistik für das Jahr 2022 vom 17.02.2023, BT-Drs. 20/5709, S. 29f.; *Biselli/Beckmann* (2019): Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa, abrufbar unter: https://freiheitsrechte.org/themen/freiheit-im-digitalen/studie-handydatenauswertung (Letzter Abruf der Online-Quellen: 23.06.2025).

Hinzu kommt, dass die erhobenen Daten wegen ihrer Mehrdeutigkeit als Beweis ungeeignet sind und die Auswertung mithin stark fehleranfällig ist. Verbindungsdaten, Geolokationsdaten, die in Textnachrichten verwendete Sprache oder Benutzernamen können aus den unterschiedlichsten Gründen, gerade im Kontext einer Fluchtgeschichte, keine oder irreführende Hinweise auf die Nationalität geben. Oft sind etwa Datensätze zu klein, alte Geräte werden nicht unterstützt oder die Auswertung wird dadurch verzerrt, dass Daten nur teilweise ausgelesen werden können. Für Gerichte schließlich gibt es keine Möglichkeit, die sachliche Richtigkeit und den Beweiswert der durch den Algorithmus getroffenen Schlüsse

nachzuvollziehen. Darüber hinaus trägt die leichte Manipulationsgefahr hinsichtlich der auszuwertenden Daten zur Ungeeignetheit der Maßnahme bei. Für Personen, die ihre Herkunft tatsächlich verschleiern wollen, ist es ein leichtes, die Auswertung ihrer Daten zu manipulieren – sei es über ein zu diesem Zwecke neu erworbenes Gerät oder über die gezielte Löschung von Daten. Für weitergehende Ausführungen verweise ich auf die Beschwerde vom 04.02.2021 (D.V.2.b).

2. Fehlende Erforderlichkeit

§ 15a AsylG verstößt gegen den Erforderlichkeitsgrundsatz, insbesondere senkt die am 27.02.2024 geänderte Fassung des § 15a AsylG die Eingriffsschwelle für die Datenauslesung ab und erlaubt diese auch bei Vorliegen milderer gleich geeigneter Mittel.

Die Neugestaltung des § 15a AsylG widerspricht den vom Bundesverwaltungsgericht aufgestellten Anforderungen an die Datenauslesung. Dem Gericht zufolge muss – nach der alten Fassung des § 15a AsylG – auch das Auslesen eines Datenträgers den Zulässigkeitsvoraussetzungen für die Auswertung entsprechen; das Auslesen ist Teil der Auswertung und als eigenständiger schwerwiegender Grundrechtseingriff (in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme) einzustufen,

vgl. BVerwG, Urteil vom 16.02.2023 – 1 C 19.21, Rn. 25 ff.

Nach der neuen Ausgestaltung der Norm werden Datenauslesung und Datenauswertung in zwei Maßnahmen unterteilt. Nur die Auswertung nach § 15a Abs. 2 S. 1 AsylG wird unter den Vorbehalt gestellt, dass „der Zweck der Maßnahme nicht durch mildere Mittel erreicht werden kann“. Für die Auslesung gilt dies nicht. Nach § 15a Abs. 1 S. 1 AsylG kann die Auslesung schon dann erfolgen, wenn es „zur Feststellung der Identität oder Staatsangehörigkeit erforderlich ist, da der Ausländer keinen gültigen Pass, Passersatz oder sonstigen geeigneten Identitätsnachweis besitzt“. Die Satzkonstellation in Abs. 1 S. 1 „erforderlich ist, da“ stellt klar, dass es sich hierbei gerade nicht um eine strenge Erforderlichkeitsprüfung handelt, die die Auswahl milderer Mittel einbezieht. Stattdessen ist die Maßnahme immer, wenn ein Identitätsnachweis fehlt, erforderlich – unabhängig von etwaigen milderen Mitteln, zum Beispiel einer Befragung oder einer Sprachprobe.

Diese Stufung hat zur Konsequenz, dass das Auslesen der Daten gerade nicht als ultima ratio, sondern als Regelmaßnahme – weit im Vorfeld einer potentiellen Auswertung – erfolgt. Der Behörde wird explizit ermöglicht, die Daten zunächst auszulesen, auch wenn mildere Mittel zur Feststellung der Identität und Staatsangehörigkeit verbleiben. Die Daten können anschließend über einen langen Zeitraum gespeichert werden, bis die Behörde andere, mildere Maßnahmen erfolglos durchgeführt hat und darauffolgend beabsichtigt, die

ausgelesenen Daten auszuwerten. Eine solche massenhafte Speicherung persönlicher Daten auf Vorrat ist jedoch nur dann ausnahmsweise zulässig, wenn die rechtliche Regelung dem besonderen Gewicht des darin liegenden Eingriffs hinreichend Rechnung trägt,

vgl. BverfGE 125, 260 (205 f.).

Dies ist angesichts der Streubreite der Maßnahme, der fehlenden zeitlichen und inhaltlichen Einschränkungen und der Bedeutung und Sensibilität der potentiell betroffenen Daten ersichtlich nicht der Fall (ausführlich hierzu unter B.II.3.).

Wenn mit der neuen Fassung des § 15a AsylG die gesetzlichen Voraussetzungen für das Auslesen bewusst abgesenkt werden, so kann dies nur als Versuch gewertet werden, die Anforderungen der Rechtsprechung zu umgehen. Dabei wird verkannt, dass es sich bei dem Auslesen um einen eigenen, intensiven Grundrechtseingriff handelt. Die neue Fassung des § 15a AsylG verschärft damit noch einmal die Gefahren für Datenschutz und Grundrechte und senkt die Eingriffsschwelle in verfassungswidriger Weise ab.

3. Unangemessenheit

Die Schwere der in § 15a AsylG normierten Befugnisse steht auch außer Verhältnis zu dem Gewicht der rechtfertigenden Gründe. Das standardmäßige, anlasslose und umfassende Auslesen und Auswerten der persönlichen Daten von Geflüchteten zur Identitätsfeststellung stellt jeweils eine besonders intensive Art der Datenverarbeitung dar und greift schwerwiegend in Art. 8 GRCh der Betroffenen ein (dazu unter a.). Dieser Eingriff steht außer Verhältnis zum öffentlichen Interesse an der Feststellung der Identität und Staatsangehörigkeit (dazu unter b.).

a. Intensität der Datenverarbeitung

§ 15a AsylG erlaubt das Auslesen und Auswerten eines potentiell immensen Datenbestandes. Gerade Smartphones werden oft als „digitaler Hausstand“ geführt, der eine Vielzahl an persönlichkeitsrelevanten Daten vereint: Nachrichten an Familienmitglieder und Partner*innen, Kontaktdaten inklusive Informationen über Anwält*innenkontakte, Konto- und Zahlungsdaten, Zugang zu E-Mail-Accounts, die Suchmaschinen-Historie, Aufenthaltsdaten, intime und persönliche Fotos. Die Verarbeitung gewinnt dadurch an Intensität, dass sie Geflüchtete betrifft, für die ihre Mobilgeräte oft die einzige kommunikative Verbindung zu engen Angehörigen in ihrer alten Heimat sind und wichtige Erinnerungen enthalten. Fotos, Videos, Textnachrichten und sonstige gespeicherte Aufzeichnungen geben dem Smartphone im Zusammenspiel regelmäßig die Funktion eines Tagebuchs. Aus Smartphone-Daten lassen sich Bewegungsprofile und soziale Netzwerke ableiten, sie ermöglichen das Erstellen von detaillierten Persönlichkeitsprofilen ihrer Nutzer*innen,

vgl. *T. W. Boonstra, M. E. Larsen, H. Christensen* (2015): Mapping dynamic social networks in real life using participants' own smartphones, abrufbar unter: https://www.cell.com/action/showPdf?pii=S2405-8440%2815%2930056-6; *C. Stachl, S. Hilbert, J.-Q. Au, D. Buschek, A. De Luca, B. Bischl, H. Hussmann, M. Bühner* (2017): Personality Traits Predict Smartphone Usage. Eur. J. Pers., 31: 701 – 722, abrufbar unter: https://www.researchgate.net/publication/318879569_Personality_Traits_Predict_Smartphone_Usage (Letzter Abruf der Online-Quellen: 23.06.2023).

Hinzu tritt der nicht zu unterschätzende und grundrechtlich relevante Einschüchterungseffekt, der entsteht, wenn die für den Asylantrag zuständige Behörde Zugriff auf all jene, teils intimen Daten erhält. Geflüchtete Personen befinden sich in einer höchst vulnerablen und ungewissen Position, in der sie – selbst ohne konkrete Hinweise auf missbräuchliches Verhalten durch Behördenmitarbeitende – die umfassende Durchleuchtung ihrer Daten zwangsläufig als bedrohlich empfinden.

Darüber hinaus umfasst die Norm auch eine Vielzahl von weiteren Datenträgern, inklusive Featurephones, USB-Sticks, Festplatten, Tablets, Laptops und Smart Watches. Sie betrifft potentiell jede Person, die ohne Identitätspapiere Asyl beantragt, mithin eine Vielzahl an Personen. Die Norm grenzt in keiner Hinsicht den Zeitpunkt oder Anlass des Auslesens oder Auswertens ein; sie schränkt auch nicht die Art der Daten ein, die ausgelesen und ausgewertet werden dürfen. Die Eingriffe betreffen damit auch Kommunikationsinhalte und besonders sensible persönliche Daten. Regelmäßig mitumfasst sind außerdem Daten Dritter.

So hat auch der EuGH in seiner jüngsten Entscheidung zum Datenzugriff auf Mobiletelefone durch staatliche Behörden ausdrücklich festgestellt, dass ein solcher Zugriff aufgrund der Vielfalt und Sensibilität der gespeicherten Daten, die sehr genaue Schlüsse auf das Privatleben der betroffenen Person zulassen, einen schwerwiegenden oder im Einzelfall sogar besonders schwerwiegenden Eingriff in die in den Art. 7 und 8 GRCh verbürgten Grundrechte darstelle,

EuGH (Große Kammer), Urteil vom 04.10.2024 – C-548/21, Rn. 92 ff.

Dem EuGH zufolge liegt ein besonders schwerwiegender Eingriff vor, wenn besonders sensible personenbezogene Daten vom Zugriff bzw. Zugriffsversuch betroffen sind, wie etwa solche, von denen auf „rassische oder ethnische Herkunft, politische Meinungen und religiöse oder weltanschauliche Überzeugungen“ geschlossen werden könne,

EuGH, Urteil vom 04.10.2024 – C 548/21, Rn. 94; EuGH, Urteil vom 22.06.2021 – C-439/19, Rn. 74.

Beim Zugriff auf Mobiltelefone sind derartige Daten regelmäßig betroffen – aufgrund des typischen Nutzungsverhaltens sowie der Vielfalt, des Umfangs und der Sensibilität der dort gespeicherten Informationen.

b. Eingriff außer Verhältnis zum Zweck

Die durch die Datenverarbeitung verursachte Belastung steht auch nicht in einem angemessenen Verhältnis zu den verfolgten Zielen. Wie bereits ausgeführt, ist schon zweifelhaft, ob die Maßnahmen überhaupt geeignet sind, die Identität und Staatsangehörigkeit festzustellen. Das nur mittelbare Ziel, das Asylverfahren vor Missbrauch zu schützen, rechtfertigt hingegen keine derart intensiven datenschutzrelevanten Eingriffe. Es konnte bislang nicht nachgewiesen werden, dass aus den Anträgen nicht asylberechtigter Personen heraus eine Gefahr für die Handlungsfähigkeit der Verwaltung entsteht. Auch stehen weder die Verhütung noch die Ahndung von Straftaten als verstärkende Ziele im Raum.

Dass die Befugnisse des § 15a AsylG nicht angemessen sind, zeigt sich auch angesichts der Kosten, die das Auslesen und Auswerten der Datenträger verursacht,

> siehe erneut *Biselli/Beckmann* (2019): Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa, online unter https://freiheitsrechte.org/themen/freiheit-im-digitalen/studie-handydatenauswertung (Letzter Abruf: 23.06.2025).

Schließlich fehlt es an einem unionsrechtlich als zwingend vorgegebenen Gerichtsvorbehalt für den Datenzugriff. Hinsichtlich des Zugriffs auf Mobiltelefone durch staatliche Stellen hat der EuGH in seiner jüngsten Entscheidung ausgeführt, dass,

> *„[u]m namentlich sicherzustellen, dass der Grundsatz der Verhältnismäßigkeit in jedem Einzelfall durch eine Gewichtung aller relevanten Gesichtspunkte gewahrt wird, es von* ***wesentlicher Bedeutung*** *[ist], dass der Zugang der zuständigen nationalen Behörden zu personenbezogenen Daten, wenn er die Gefahr eines schwerwiegenden oder sogar besonders schwerwiegenden Eingriffs in die Grundrechte der betroffenen Person mit sich bringt, von einer* ***vorherigen Kontrolle durch ein Gericht*** *oder eine* ***unabhängige Verwaltungsstelle*** *abhängig gemacht wird.“* EuGH, Urteil vom 04.10.2024 – C 548/21, Rn. 102 ff. [Hervorhebungen durch den Unterzeichner].

§ 15a AsylG sieht keine vorherige Kontrolle des Datenzugriffs durch eine unabhängige Stelle vor, um die Wahrung der Verhältnismäßigkeit sicherzustellen.

III. Verstoß gegen die Grundsätze des Art. 5 Abs. 1 lit. c, d DSGVO

1. Datenminimierung

Wie bereits in der Beschwerde vom 04.02.2021 ausgeführt (D.V.), widerspricht die Datenauslesung und -auswertung nach § 15a Abs. 1 und 2 AsylG auch dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO. Danach müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dies ist nur dann der Fall, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann, vgl. Erwägungsgrund Nr. 50 DSGVO.

Während zur Angemessenheit und Erheblichkeit das bereits Ausgeführte gilt (s.o. B.II.1., 3.), kommt erschwerend hinzu, dass die Daten nicht auf das notwendige Maß beschränkt sind. Stattdessen ermächtigt § 15a AsylG dazu, den gesamten Rohdatensatz aus dem jeweiligen Datenträger auszulesen und auszuwerten. Dabei werden in großem Umfang – und oft überwiegend – Daten verarbeitet, die keinerlei Bezug zur Identität oder Staatsangehörigkeit haben. Eine Beschränkung auf bestimmte Daten ist in der Rechtsgrundlage, entgegen der Anforderungen der DSGVO, nicht vorgesehen.

Der Verstoß wird durch die Neufassung des § 15a Abs. 1 AsylG, nach der die Speicherung einer Vielzahl an Daten auf Vorrat ermöglicht wird, weiter vertieft. Eine gesetzliche Beschränkung auf das „notwendige Maß“ ist nicht vorhanden.

2. Datenrichtigkeit

§ 15a AsylG missachtet auch den Grundsatz der Datenrichtigkeit nach Art. 5 Abs. 1 lit. d) DSGVO. Danach müssen die Daten sachlich richtig sein, d.h. den für den Zweck der Datenverarbeitung relevanten Ausschnitt der Realität korrekt darstellen.

Ob dies für die Daten der Auswertung zutrifft, kann weder behördenintern noch gerichtlich einwandfrei überprüft werden. Fest steht aber, dass durch die Art der Daten eine hohe Fehleranfälligkeit bei der Auswertung besteht – etwa, weil Geolokationsdaten auch Fotos betreffen, die an die betroffene Person verschickt wurden; weil Geo-Tags insgesamt sehr fehleranfällig sind; weil Sprachzuordnung, gerade bei arabischen Dialekten und der Übersetzung in lateinische Buchstaben, nur unzuverlässig funktioniert; weil Ergebnisse durch eine technisch bedingt nur punktuelle Auswertung verzerrt werden; etc. Ich verweise hierzu auf die Ausführungen in der Beschwerde vom 04.02.2021 (D.VI.).

IV. Verstoß gegen Art. 9 Abs. 1 DSGVO

Die Befugnis zum Auslesen und Auswerten nach § 15a AsylG betrifft unstreitig die Verarbeitung besonderer personenbezogener Daten nach Art. 9 Abs. 1 DSGVO. Eine solche Verarbeitung ist grundsätzlich untersagt.

Die Verarbeitung könnte nur ausnahmsweise erlaubt werden, wenn sie nach Art. 9 Abs. 2 lit. g) DSGVO „auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich“ wäre.

Dies ist aber nicht der Fall. Zur fehlenden Angemessenheit verweise ich auf die Ausführungen oben (unter B.II.3.). Ein erhebliches öffentliches Interesse hingegen lässt sich nicht begründen. Zwar handelt es sich bei der Feststellung der Identität und der Staatsangehörigkeit um ein legitimes Interesse. Es ist jedoch – selbst wenn außer Acht gelassen wird, dass die Maßnahme zum Nachweis schon gar nicht geeignet ist, s.o. – keinesfalls in dem Sinne erheblich, dass die Allgemeinheit ohne die Maßnahme ernsthaft beeinträchtigt wäre,

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

V. Verstoß gegen nationale Grundrechte

Ein Verbot nach Art. 58 Abs. 2 lit. f DSGVO muss dann ausgesprochen werden, wenn eine Norm gegen die DSGVO verstößt. Wegen der Öffnungsklausel in Art. 6 Abs. 1 lit. e i.V.m.. Abs. 3 S. 1 lit. b DSGVO umfasst dies auch die Prüfung nationaler Grundrechte.

§ 15a AsylG ist in seiner jetzigen Form nicht mit den Grundrechten vereinbar. Die Norm greift in nicht gerechtfertigter Weise in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein.

1. Schutzbereich

Der Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ist eröffnet. Es ist als Maßstab anzuwenden, wenn

> *„die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem **Umfang** und in einer **Vielfalt** enthalten können, dass ein Zugriff auf das System es ermöglicht, einen **Einblick in wesentliche Teile der Lebensgestaltung** einer Person zu gewinnen oder gar ein **aussagekräftiges Bild der Persönlichkeit** zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden. Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen. Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können“,*
> BVerfGE 120, 274 (314).

§ 15a Abs. 1 und 2 AsylG ermächtigen zur Auslesung und Auswertung von Datenträgern und ermöglichen dem BAMF dadurch, Einblicke in wesentliche Teile der Lebensgestaltung der Betroffenen zu gewinnen. Auch wenn in der derzeitigen Praxis nur Mobiltelefone mit großem Funktionsumfang (Smartphones) und Mobiltelefone mit geringerem Funktionsumfang (Featurephones) ausgelesen und ausgewertet werden, sind von der Ermächtigungsgrundlage auch andere informationstechnische Systeme umfasst. In der Begründung des Regierungsentwurfs zur Einführung § 15a AsylG a.F. werden neben Mobiltelefonen auch Tablets und Laptops genannt,

> Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur besseren Durchsetzung der AusreisepflichtBT-Drs. 18/11546, S. 23, abrufbar unter: https://dip21.bundestag.de/dip21/btd/18/115/1811546.pdf (Letzter Abruf: 23.06.2025).

Die Vorschrift erfasst damit Systeme, die eine Vielzahl von personenbezogenen Daten enthalten, insbesondere die vom Bundesverfassungsgericht angesprochenen Personalcomputer und Mobiltelefone mit großem Funktionsumfang.

2. Eingriff

Den ersten Grundrechtseingriff stellt der technische Vorgang der Auslesung sämtlicher Daten des Datenträgers dar, bei dem also der Rohdatensatz kopiert wird. Einen weiteren Eingriff begründet die anschließende Auswertung und die Generierung des elektronischen Ergebnisreports mithilfe des „MSAB Kiosk“, bei dem noch kein Mensch Kenntnis von persönlichen Daten der Asylsuchenden erlangt,

vgl. BVerwG, Urteil vom 16.02.2023 – 1 C 19.21, Rn. 25.

An einem Eingriff fehlt es im Rahmen von elektronischen Datenverarbeitungsprozessen lediglich dann, wenn Daten nur zufällig am Rande miterfasst und unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden gelöscht werden,

BVerfGE 150, 244 (48).

Demgegenüber werden die Datenträger der Asylsuchenden ohne anerkannte Ausweispapiere vom BAMF vollständig kopiert und kurzfristig gespeichert, um für das Verfahren möglicherweise bedeutsame Daten zu erheben.

Ein weiterer technischer Grundrechtseingriff ist die längerfristige Speicherung des von der Software bei der Auswertung des Rohdatensatzes erstellten Ergebnisreports in einem Datentresor,

vgl. BVerwG, Urteil vom 16.02.2023 – 1 C 19.21, Rn. 25.

Eigenständige Eingriffsqualität kommt sodann der Prüfung des Ergebnisreports durch eine*n Volljurist*in auf einen Auswertungsantrag des*der Entscheider*in zu. Hier erhält erstmals ein Mensch Kenntnis von den auf dem Datenträger gespeicherten Daten, selbst wenn der Datenträger für das weitere Verfahren nicht freigegeben wird.

Wird der Ergebnisreport freigegeben, erfolgt schließlich ein weiterer, vertiefter Grundrechtseingriff dadurch, dass der*die Entscheider*in den Report der Entscheidung über den Asylantrag zugrunde legt und unter Umständen in der Anhörung Fragen zu im Report dargestellten Daten stellt. Er*sie kann diese Daten dann als Grundlage seiner*ihrer Befragung in der Anhörung im Asylverfahren sowie zur Entscheidung über den Asylantrag heranziehen. Er*sie kann zudem die in der Tabelle über die Identität vermerkten Daten, etwa den Namen eines Facebook-Profils zum Anlass für weitere eigenständige Recherchen nehmen. Zudem können etliche weitere Behörden unter besonderen Voraussetzungen auf die Asylakte zugreifen und das Ergebnis der Handydatenauswertung damit ebenfalls zur Kenntnis nehmen.

3. Rechtfertigung

Auch hinsichtlich eines Eingriffes in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme fehlt es an einer hinreichend bestimmten und verhältnismäßigen Gesetzesgrundlage (s.o. B.I. und II. sowie Beschwerde vom 04.02.2021, D.III.). Zudem ist der § 15a AsylG nicht ausreichend durch verfahrensrechtliche Sicherungsmaßnahmen flankiert. Dies gilt umso mehr für die neue Fassung des § 15a AsylG, der das Auslesen der Daten ohne die vorherige Prüfung milderer Mittel erlaubt (s.o. B.II.2.).

a. Unverhältnismäßigkeit

Der schwerwiegende Eingriff in die Persönlichkeitsrechte einer Vielzahl an Menschen steht außer Verhältnis zum Zweck, die Rückführung von nicht asylberechtigten Menschen zu ermöglichen. Im Rahmen der Verhältnismäßigkeitsprüfung ist insbesondere die verfassungsrechtliche Rechtsprechung zu beachten, dass angesichts der hohen Eingriffsintensität solche Eingriffe nur erfolgen dürfen, wenn tatsächliche Anhaltspunkte für eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut vorliegen,

vgl. BVerfGE 141, 220 (212).

Dies ist bei den auf § 15a AsylG gestützten Maßnahmen nicht der Fall. Die standardmäßig durchgeführte Identitätsfeststellung dient weder der Verhinderung noch der Aufklärung von Straftaten, bei denen die Rechtgüter anderer gefährdet wären. Vielmehr zielen die Maßnahmen nur darauf ab, bloßes Verwaltungshandeln zu effektivieren und migrationspolitische Zielsetzungen durchzusetzen. Darüber hinaus steht – wie zuvor beschrieben – schon gar nicht im Raum, dass die Verwaltung durch eine Flut falscher Angaben zur Identität überfordert wird. Vielmehr entsteht durch das Auslesen und Auswerten ein Mehraufwand für die Verwaltung, der in keinem Verhältnis zum Zweck der Maßnahme und ihren Erfolgsaussichten steht.

b. Bestimmtheit und Normenklarheit

Auch mit Blick auf die Wesentlichkeitstheorie und das Gebot der Normenbestimmtheit und Normenklarheit aus Art. 20 Abs. 3 GG fehlt § 15a AsylG die hinreichende Bestimmtheit (s.o. B.I und IV. sowie Beschwerde vom 04.02.2021 (D.III.)).

c. Fehlender Kernbereichsschutz

Für die Datenauslesung und -auswertung nach § 15a Abs. 1 und 2 AsylG fehlen ausreichende gesetzliche Schutzvorkehrungen für den absolut geschützten Kernbereich privater Lebensgestaltung. Solche Vorkehrungen sind bei derart schwerwiegenden Eingriffen in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verfassungsrechtlich geboten.

aa. Verfassungsrechtliche Anforderungen an den Kernbereichsschutz

Der Kernbereich privater Lebensgestaltung erfasst insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden, wie es insbesondere bei Gesprächen im Bereich der Wohnung der Fall ist. Zu diesen Personen gehören insbesondere Ehe- oder

Lebenspartner, Geschwister und Verwandte in gerader Linie, vor allem, wenn sie im selben Haushalt leben, aber auch Strafverteidiger*innen, Ärzt*innen, Geistliche und enge persönliche Freund*innen,

BVerfGE, 141, 220 (121).

Der Schutz des Kernbereichs privater Lebensgestaltung ist strikt und darf nicht durch Abwägung mit den Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden,

vgl. BVerfGE 109, 279 (314); BVerfGE 120, 274 (339); st. Rspr.

Das Bundesverfassungsgericht hat für staatliche Überwachungsmaßnahmen, die mit einer besonders hohen Eingriffsintensität einhergehen, besondere Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung gestellt, die zwingend einzuhalten sind. Die besondere Intensität eines solchen Eingriffs wird gerade durch die höchstpersönliche Natur der erhobenen Daten begründet, die sich insbesondere auch aus deren Verknüpfung ergibt,

vgl. BVerfGE 141, 220 (210).

So hat es in seinen Entscheidungen zu geheimen Überwachungsmaßnahmen entschieden, dass die gesetzliche Grundlage dem Kernbereichsschutz zwingend auf zwei Ebenen Rechnung tragen muss. Erstens sind auf der Ebene der Datenerhebung Vorkehrungen im Sinne einer vorgelagerten Prüfung zu treffen, die eine unbeabsichtigte Miterfassung von Kernbereichsinformationen nach Möglichkeit ausschließen. Zweitens sind auf der Ebene der nachgelagerten Auswertung und Verwertung die Folgen eines dennoch nicht vermiedenen Eindringens in den Kernbereich privater Lebensgestaltung strikt zu minimieren,

vgl. BVerfGE 141, 220 (126); BVerfGE 165, 1 (108).

Sobald eine Überwachungsmaßnahme typischerweise zur Erhebung kernbereichsrelevanter Daten führt, müsse der Gesetzgeber Regelungen schaffen, die einen wirksamen Schutz normenklar gewährleisten. Lediglich außerhalb solcher verletzungsgeneigten Befugnisse sei eine ausdrückliche Regelung nicht erforderlich,

vgl. BVerfGE 141, 220 (123); BVerfGE 165, 1 (108).

Das entscheidende Kriterium ist demnach die Verletzungsgeneigtheit einer staatlichen Maßnahme, d.h. die Qualität und Quantität der von der Maßnahme erfassten Daten; es kommt dabei nicht darauf an, ob sie heimlich oder offen erfolgt,

so auch *Möller*, in: Hofmann, Ausländerrecht, 3. Auflage 2023, § 48 Rn. 60; für „offene“ Datenzugriffe auf beschlagnahmte Mobiltelefone nach § 94 ff. StPO so auch *El-Ghazi*, Beschlagnahme und Auswertung von Handys, Laptops & Co., NJW-Beil 2024, 46 (49 Rn. 16) und *Schneider*, Kernbereich privater Lebensgestaltung, JuS 2021, 29 (33).

Wie bereits oben umfassend ausgeführt, erlaubt § 15a Abs. 1 und 2 AsylG ausdrücklich die Auslesung und Auswertung aller Daten, die auf den eingezogenen Datenträgern vorhanden sind (B.II.3.a.). Insbesondere enthalten Mobiltelefone typischerweise Daten, die dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind (Kommunikationsinhalte, intime Bilder und Videos etc.). Bei § 15a Abs. 1 und 2 AslyG handelt sich damit um besonders verletzungsgeneigte Befugnisse.

bb. Unzureichender vorgelagerter Schutz des Kernbereichs privater Lebensgestaltung

Der vorgelagerte Schutz des Kernbereichs privater Lebensgestaltung nach § 15a Abs. 2 S. 2 - 6 AsylG ist unzureichend.

Lediglich die Auswertung von Datenträgern ist nach § 15a Abs. 2 S. 2 AsylG unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch das Auswerten von Datenträgern allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Diese Regelung ist aber praktisch bedeutungslos, da von der Auswertung der Datenträger von Asylsuchenden nie „allein“ Erkenntnisse aus dem Kernbereich zu erwarten sind. Vielmehr handelt es sich bei den betroffenen Datenträgern regelmäßig um Mischdatenbestände, sodass der angestrebte Kernbereichsschutz vollständig leer läuft und im Ergebnis keinen Schutz bietet,

so auch *Möller*, in: Hofmann, Ausländerrecht, 3. Auflage 2023, § 48 Rn. 60 und *Lehnert*, in: Huber/Mantel, Aufenthaltsgesetz/Asylgesetz, 4. Auflage 2025, § 48 Rn. 21 sowie GK-AslylG/Funke-Kaiser AsylG § 15a Rn. 12; vgl. *Vasel/Heck*, NVwZ 2024, 540 (546); Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zum Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht, 23.03.2017, S. 7; abrufbar unter: https://www.bundestag.de/resource/blob/500024/bf72784c6e0f00bc5d801ccd5aee690b/18-4-831-data.pdf (Letzter Abruf: 23.06.2025).

Auch das Verwertungsverbot von kernbereichsrelevanten Informationen nach § 15a Abs. 2 S. 3 AsylG gewährleistet keinen ausreichenden Schutz, da es nicht verhindert, dass Daten aus dem Kernbereich erhoben werden und die für die Auswertung zuständige Person davon Kenntnis erlangt. Hinsichtlich der Befugnis zum Auslesen von Datenträgern in § 15a Abs. 1

AsylG findet sich keinerlei Begrenzung zum Schutz des Kernbereichs privater Lebensgestaltung.

Zwingend erforderlich und ohne Weiteres möglich wäre eine Regelung entsprechend § 100d Abs. 3 S. 1 StPO, welche einen wirksamen Kernbereichsschutz gewährleistet. Nach § 100d Abs. 3 S. 1 StPO ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.

cc. Unzureichender nachgelagerter Schutz des Kernbereichs privater Lebensgestaltung mangels Richtervorbehalts

Auch der nachgelagerte Kernbereichsschutz ist unzureichend. Auf der Ebene der Auswertung und Verwertung ist dessen Einhaltung durch eine unabhängige Prüfung sicherzustellen. Es fehlt aber an institutionalisierten Mechanismen, die eine solche unabhängige Kontrolle gewährleisten.

Nach der Rechtsprechung des Bundesverfassungsgerichts hat der Gesetzgeber auf der Ebene der Auswertung für den Fall, dass die Erfassung von kernbereichsrelevanten Informationen nicht vermieden werden kann, in der Regel die Sichtung der erfassten Daten durch eine unabhängige Stelle vorzusehen, die die kernbereichsrelevanten Informationen vor der anschließenden Verwendung der Daten herausfiltert. Die Erforderlichkeit einer solchen Sichtung hängt von der Art sowie gegebenenfalls auch der Ausgestaltung der jeweiligen Befugnis ab. Dabei kann auf die Sichtung durch eine unabhängige Stelle umso eher verzichtet werden, je verlässlicher schon auf der ersten Stufe die Erfassung kernbereichsrelevanter Sachverhalte vermieden wird und umgekehrt,

vgl. BVerfGE 141, 220 (129 m.w.N.).

Wie bereits oben ausgeführt, sieht § 15a Abs. 1 S. 2 - 6 AsylG unzureichende Vorkehrungen vor, den Schutz des Kernbereichs schon im Vorfeld zu gewährleisten. Daher ist die Sichtung durch eine unabhängige Stelle unverzichtbar.

Die Regelung des § 15a Abs. 1 S. 6 AsylG, wonach der Datenträger nur durch Bedienstete mit Befähigung zum Richter*innenamt ausgewertet werden darf, genügt diesen Anforderungen nicht. Erforderlich wäre ein Gerichtsvorbehalt, der auf eine Kontrolle der Maßnahme durch eine unabhängige und neutrale Instanz abzielt.

Das Grundgesetz geht davon aus, dass Richter*innen aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer strikten Unterwerfung unter das Gesetz (Art. 97 GG) die Rechte der Betroffenen im Einzelfall am besten und sichersten wahren können,

vgl. BVerfGE 149, 293 (96); *Wildhagen*, Persönlichkeitsschutz durch präventive Kontrolle, 2011, S. 184 f.

Ungeachtet ihrer juristischen Qualifikation fehlt es bei Behördenmitarbeiter*innen, die aufgrund beamtenrechtlicher oder arbeitsvertraglicher Treuepflichten den Weisungen ihres Dienstherrn bzw. ihres Arbeitgebers unterstehen und bei denen aufgrund ihrer Aufgabenstellung und den damit verbundenen Zielsetzungen eine interessensgeleitete Entscheidung nicht auszuschließen ist, an der für einen Gerichtsvorbehalt typischen Unabhängigkeit und Unparteilichkeit,

vgl. *Vasel/Heck*, NVwZ 2024, 540 (547); Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, a.a.O.; *Möller*, in: Hofmann, Ausländerrecht, 3. Auflage 2023, § 48 Rn. 53.

Im Übrigen ist der „Volljurist*innenvorbehalt“ nicht geeignet, die materiellen Bedenken gegen die Eingriffsermächtigung auszuräumen. Gerichtsvorbehalte oder vergleichbare Regelungen sind nur dann grundrechtlich sinnvoll, wenn die Gerichte prüfen können, ob grundrechtsschützende materielle Eingriffsvoraussetzungen vorliegen. Dagegen sind sie nicht dazu geeignet, die Mängel einer zu niedrig angesetzten Eingriffsschwelle auszugleichen,

BVerfGE 120, 274 (331).

d. Verfahrensrechtliche Sicherungen

Auch die weiteren verfahrensrechtlichen Sicherungen gewährleisten nur unzureichend die Transparenz der Datenverwendung und effektiven Rechtsschutz. Den Betroffenen stehen lediglich die allgemeinen Betroffenenrechte der DSGVO zur Verfügung, also ein Anspruch auf Löschung nach Art. 17 Abs. 1 lit. a DSGVO und ein Anspruch auf Auskunft nach Art. 15 DSGVO. Selbst diese Rechte sind den Betroffenen in der Regel nicht geläufig und von Seiten der Behörde erfolgen diesbezüglich keine Hinweise. Behördeninterne Transparenzanforderungen sind ebenso wenig bekannt wie Maßgaben zu Dokumentation und Monitoring.

VI. Keine verfassungs- bzw. datenschutzkonforme Auslegung möglich

Eine verfassungs- bzw. datenschutzkonforme Auslegung des § 15a AsylG kommt nicht in Betracht.

Nach dem in ständiger Rechtsprechung entwickelten Grundsatz der verfassungskonformen Auslegung ist ein Gesetz dann nicht verfassungswidrig, wenn eine Auslegung möglich ist, die im Einklang mit dem Grundgesetz steht, und das Gesetz bei dieser Auslegung sinnvoll bleibt,

BVerfGE 2, 266 (267); st. Rspr.

Aufgrund der weiten Formulierung der Rechtsgrundlage und der durch sie erfolgenden schwerwiegenden Grundrechtseingriffe ist eine verfassungskonforme Auslegung der Norm jedoch nicht möglich. Keine der Auslegungsvarianten ermöglicht eine Behebung der Verstöße gegen die DSGVO und den Verhältnismäßigkeitsgrundsatz.

Es ist – vor dem Hintergrund der erkennbaren gesetzgeberischen Intention – auch nicht Aufgabe der Gerichte oder Behörden, diese strengeren Vorgaben im Wege einer verfassungs- und datenschutzkonformen Auslegung zu etablieren. Das Bundesverfassungsgericht hat in ständiger Rechtsprechung aus dem grundgesetzlichen Gesetzesvorbehalt und dem Rechtsstaatsprinzip (Art. 20 Abs. 3 GG) sowie dem Demokratieprinzip (Art. 20 Abs. 1 und 2 GG) die Verpflichtung des Gesetzgebers abgeleitet, in allen grundlegenden normativen Bereichen die wesentlichen Entscheidungen selbst zu treffen. Er muss vor allem für die Verwirklichung der Grundrechte Anlass, Zweck und Grenzen des Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festlegen und damit der Regierung und Verwaltung steuernde und begrenzende Handlungsmaßstäbe vorgeben und den Gerichten die Rechtskontrolle ermöglichen,

BVerfGE 120, 274 (209, 315 f.); BVerfGE 100, 313 (359 f.); BVerGE 162, 378.

Die Anforderungen an den Grad der Klarheit und Bestimmtheit der gesetzlichen Ermächtigungsgrundlage wachsen mit der Intensität des Grundrechtseingriffs: Sie sind umso strenger, je intensiver der Grundrechtseingriff ist,

stRspr; vgl. nur BVerfGE 86, 288 (311); 93, 213 (238); 109, 133 (188); 128, 282 (318); 131, 268 (306); vgl. auch BVerfGE 110, 33 (55); 120, 378 (408).

Gerade im Bereich von staatlichen Überwachungsbefugnissen gelten besonders strenge Anforderungen. So hat das Bundesverfassungsgericht bezogen auf Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in seinem Urteil zum BKA-Gesetz zu den Anforderungen an die gesetzliche Bestimmtheit ausgeführt:

„*Bei der näheren Ausgestaltung der Einzelbefugnisse kommt es für deren Angemessenheit wie für die zu fordernde Bestimmtheit maßgeblich auf das Gewicht des jeweils normierten Eingriffs an. Je tiefer Überwachungsmaßnahmen in das Privatleben hineinreichen und berechtigte Vertraulichkeitserwartungen überwinden, desto strenger sind die Anforderungen*“,

BVerfGE 141, 220 (105).

Anlass, Zweck und Grenzen der Datenauslesung und -auswertung nach § 15a AsylG sowie Vorkehrungen zur Wahrung der Verhältnismäßigkeit muss der Gesetzgeber somit mit hinreichender Deutlichkeit selbst festlegen. Eine Delegation dieser Regelungskompetenz an Gerichte oder Behörden im Wege einer einschränkenden Anwendung der Norm durch diese ist mit Blick auf die hohe Eingriffsintensität unzulässig.

Die Möglichkeit einer verfassungskonformen Auslegung endet mithin dort, wo sie mit dem Wortlaut und dem klar erkennbaren Willen des Gesetzgebers in Widerspruch träte,

> BVerfGE 95, 64 (93); BVerfGE 138, 64 (86).

Der Wortlaut ist hierbei in mehrfacher Hinsicht eindeutig:

So verlangt § 15a Abs. 1 S. 1 AsylG offensichtlich keine Erforderlichkeitsprüfung, die aber für eine Grundrechtskonformität notwendig wäre (s.o. B.II.2.). Durch die Formulierung „erforderlich, da“ wird keine Prüfung milderer Mittel vorausgesetzt.

Zudem lässt sich unter keiner Auslegungsvariante eine Beschränkung auf bestimmte, relevante Daten in die Rechtsgrundlage hineinlesen (s.o. B.III.1.). Aus dem Wortlaut ergibt sich gerade keine Beschränkung auf bestimmte Daten, sondern es sollen alle in Frage kommenden „Datenträger“ und „Daten“ ausgelesen und ausgewertet werden. Die Regelung zum Schutz des Kernbereichs privater Lebensgestaltung in § 15a Abs. 2 S. 2 AsylG hingegen läuft faktisch leer und bezieht sich ohnehin nur auf den Eingriff durch das Auswerten, nicht aber auf das Auslesen der Daten (s.o. B.V.3.c.).

Schließlich mangelt es auch an dem für eine Grundrechtskonformität erforderlichen Gerichtsvorbehalt für die Auswertung (s.o. B.V.3.d.). Dieser kann nicht entgegen des eindeutigen Wortlauts – „Befähigung zum Richteramt“ – in die Norm hineingelesen werden.

Hinsichtlich des gesetzgeberischen Willens wurde zuvor bereits dargelegt, dass die neue Fassung des § 15a AsylG die Befugnisse der Behörde ganz bewusst – über die Grenzen der verfassungskonformen Auslegung hinaus – erweitern soll (siehe B.II.2.). An der bisherigen Verwaltungspraxis, die sich unter der alten Fassung des § 15a AsylG etabliert hat, soll sich nach der Gesetzesbegründung gerade nichts ändern:

> „*Es ist davon auszugehen, dass sich durch die Konkretisierungen die betroffenen Verfahrensabläufe im BAMF nicht spürbar verändern werden*“, Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Verbesserung der Rückführung (Rückführungsverbesserungsgesetz), BT-Drs. 563/23, S. 32, abrufbar unter:

https://www.bundesrat.de/SharedDocs/drucksachen/2023/0501-0600/563-23.pdf?__blob=publicationFile&v=1 (Letzter Abruf: 23.06.2025).

C. Konsequenzen

In der derzeitigen Ausgestaltung ist § 15a AsylG als rechtswidrig einzustufen. Mit der Norm wird ein erheblicher Eingriff in die Persönlichkeitsrechte von Menschen legitimiert, die als Teil einer besonders vulnerablen Gruppe hierdurch besonders betroffen sind. Dem gegenüber stehen einerseits ein unangemessen hoher Ressourcenaufwand und andererseits ein verschwindend geringer praktischer Nutzen der Maßnahme. Nur höchst selten kann die Auswertung mündliche Angaben widerlegen und die Möglichkeiten der Umgehung sind vielfältig.

Die bloße Verwarnung nach Art. 58 Abs. 2 lit. b DSGVO genügt nicht der Tatsache, dass es sich bei dem § 15a AsylG um eine rechtswidrige Norm handelt, auf deren Grundlage kontinuierlich weitere rechtswidrige Datenverarbeitungen durchgeführt werden. Um die fortschreitenden, nicht gerechtfertigten Eingriffe in Persönlichkeitsrechte zu verhindern, rege ich nochmals nachdrücklich an, ein Verbot der Verarbeitung zu verhängen.

Namens und in Vollmacht des Beschwerdeführers … wird daher der Antrag vom 04.02.2021 aufrechterhalten.

Mit freundlichen Grüßen

Dr. Lehnert, Rechtsanwalt