6 K 1563/21.WI

VERWALTUNGSGERICHT WIESBADEN

BESCHLUSS

In dem Verwaltungsstreitverfahren

[redacted]

Kläger

bevollmächtigt:

Rechtsanwälte Meisterernst und Kollegen
Oststraße 2, 48145 Münster
Aktenzeichen: 3605/21

gegen

die Landeshauptstadt Wiesbaden,
vertreten durch den Oberbürgermeister
- Rechtsamt -
Wilhelmstraße 32, 65183 Wiesbaden,

Beklagte

wegen Pass- und Ausweisrecht

hat das Verwaltungsgericht Wiesbaden - 6. Kammer - durch

Vorsitzenden Richter am VG Schild
Richter am VG Dr. Buus
Richterin von Borries-Hanstein

am 13.01.2022 beschlossen:

I. Das Verfahren wird ausgesetzt.

II. Das Verfahren wird gemäß Art. 267 AEUV zur Vorabentscheidung dem Gerichtshof der Europäischen Union hinsichtlich der folgenden Fragen vorgelegt:

Verstößt die Verpflichtung zur Aufnahme und Speicherung von Fingerabdrücken in Personalausweisen gemäß Artikel 3 Abs. 5 der Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben (ABl. L 188 vom 12.07.2019, S. 67) gegen höherrangiges Unionsrecht, insbesondere

a) gegen Art. 77 Abs. 3 AEUV

b) gegen Art. 7 und 8 GrCh

c) gegen Art. 35 Abs. 10 DS-GVO

und ist deshalb aus einem der Gründe ungültig?

Gründe:

I.

1 Der Kläger begehrt die Ausstellung eines Personalausweises ohne die Aufnahme von Fingerabdrücken. Dies wird von der Beklagten abgelehnt, da § 5 Abs. 9 PAuswG, welcher auf der Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben (ABl. L 188 vom 12.07.2019, S. 67) beruht, zwingend die Aufnahme zweier Finderabdrücke vorsieht.

2 Die Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates vom 20.06.2019 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben, gilt ab dem 02.08.2021. Die Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat. In Art. 3 Abs. 5 VO (EU) 2019/1157 ist geregelt, dass Personalausweise, die von den Mitgliedsstaaten ausgestellt werden, mit einem Speichermedium versehen werden, das ein Gesichtsbild des Personalausweisinhabers und zwei Fingerabdrücke in interoperablen digitalen Formaten enthält. Im nationalen Recht wurden ebenfalls Regelungen zur der Aufnahme von Fingerabdrücken in Personalausweisen getroffen (§ 5 Abs. 9 PAuswG), wobei der nationale Gesetzgeber ausweislich der Gesetzesbegründung (BT-Drs. 19/21986, S. 22) davon ausgegangen ist, dass Fingerabdrücke gemäß Art. 3 Abs. 5 VO (EU) 2019/1157 aufzunehmen seien.

3 Der Kläger beantragte am 30.11.2021 die Ausstellung eines neuen Personalausweises ohne Fingerabdrücke, da der Chip seines alten

Personalausweises defekt sei. Die Neuausstellung wurde abgelehnt, da seit dem 02.08.2021 die Aufnahme von Fingerabdrücken verpflichtend sei. Zudem habe der Kläger keinen Anspruch auf Ausstellung eines neuen Ausweises, da er bereits im Besitze eines gültigen Ausweisdokuments sei. Ein Personalausweis sei auch mit defektem Chip weiterhin gültig.

4 Die Behörde, die nach nationalem Recht für die Ausstellung der Personalausweise zuständig ist, wird nach dem Recht des Mitgliedstaates als Gefahrenabwehrbehörde tätig. Dennoch unterliegt die Ausstellung von Personalausweisen und die damit verbundene Datenverarbeitung gerade nicht der RL (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates („Gefahrenabwehrrichtlinie“), sondern der DS-GVO (vgl. Erwägungsgrund 40 VO (EU) 2019/1157). Im vorliegenden Fall wird daher der Oberbürgermeister nicht auf dem Gebiet des autonom auszulegenden europarechtlichen Gefahrenabwehrrechts tätig. Gemäß Art. 1 Abs. 1 und Art. 2 Abs. 1 RL (EU) 2016/680 ist diese Richtlinie nur dann anzuwenden, wenn Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit tätig werden. Das Pass- und Ausweiswesen zählt nicht hierunter.

II.

1. Charta der Grundrechte der Europäischen Union (GrCh)

5 **Artikel 7 GrCh**

Achtung des Privat- und Familienlebens

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

6 Artikel 8 GrCh

Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

7 Artikel 52 GrCh

Tragweite und Auslegung der Rechte und Grundsätze

(1) Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

(2) Die Ausübung der durch diese Charta anerkannten Rechte, die in den Verträgen geregelt sind, erfolgt im Rahmen der in den Verträgen festgelegten Bedingungen und Grenzen.

(3) Soweit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt.

(4) Soweit in dieser Charta Grundrechte anerkannt werden, wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, werden sie im Einklang mit diesen Überlieferungen ausgelegt.

(5) Die Bestimmungen dieser Charta, in denen Grundsätze festgelegt sind, können durch Akte der Gesetzgebung und der Ausführung der Organe, Einrichtungen und sonstigen Stellen der Union sowie durch Akte der Mitgliedstaaten zur Durchführung des Rechts der Union in Ausübung ihrer jeweiligen Zuständigkeiten umgesetzt werden. Sie können vor Gericht nur bei der Auslegung dieser Akte und bei Entscheidungen über deren Rechtmäßigkeit herangezogen werden.

(6) Den einzelstaatlichen Rechtsvorschriften und Gepflogenheiten ist, wie es in dieser Charta bestimmt ist, in vollem Umfang Rechnung zu tragen.

(7) Die Erläuterungen, die als Anleitung für die Auslegung dieser Charta verfasst wurden, sind von den Gerichten der Union und der Mitgliedstaaten gebührend zu berücksichtigen.

2. Vertrag über die Arbeitsweise der Europäischen Union in der Fassung der Bekanntmachung vom 9. Mai 2008 (ABl. C 115 S. 47; ABl. 2010 C 83 S. 47; ABl. 2012 C 326 S. 47; ABl. 2016 C 202 S. 47, ber. ABl. C 400 S. 1)
Celex-Nr. 1 1957 E

8 Artikel 21 AEUV

[Freizügigkeit]

(1) Jeder Unionsbürger hat das Recht, sich im Hoheitsgebiet der Mitgliedstaaten vorbehaltlich der in den Verträgen und in den Durchführungsvorschriften vorgesehenen Beschränkungen und Bedingungen frei zu bewegen und aufzuhalten.

(2) Erscheint zur Erreichung dieses Ziels ein Tätigwerden der Union erforderlich und sehen die Verträge hierfür keine Befugnisse vor, so können das Europäische Parlament und der Rat gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften erlassen, mit denen die Ausübung der Rechte nach Absatz 1 erleichtert wird.

(3) Zu den gleichen wie den in Absatz 1 genannten Zwecken kann der Rat, sofern die Verträge hierfür keine Befugnisse vorsehen, gemäß einem besonderen Gesetzgebungsverfahren Maßnahmen erlassen, die die soziale Sicherheit oder den sozialen Schutz betreffen. Der Rat beschließt einstimmig nach Anhörung des Europäischen Parlaments.

9 Artikel 77 AEUV

[Grenzschutzpolitik]

(1) Die Union entwickelt eine Politik, mit der

a) sichergestellt werden soll, dass Personen unabhängig von ihrer Staatsangehörigkeit beim Überschreiten der Binnengrenzen nicht kontrolliert werden;

b) die Personenkontrolle und die wirksame Überwachung des Grenzübertritts an den Außengrenzen sichergestellt werden soll;

c) schrittweise ein integriertes Grenzschutzsystem an den Außengrenzen eingeführt werden soll.

(2) Für die Zwecke des Absatzes 1 erlassen das Europäische Parlament und der Rat gemäß dem ordentlichen Gesetzgebungsverfahren Maßnahmen, die folgende Bereiche betreffen:

a) die gemeinsame Politik in Bezug auf Visa und andere kurzfristige Aufenthaltstitel;

b) die Kontrollen, denen Personen beim Überschreiten der Außengrenzen unterzogen werden;

c) die Voraussetzungen, unter denen sich Drittstaatsangehörige innerhalb der Union während eines kurzen Zeitraums frei bewegen können;

d) alle Maßnahmen, die für die schrittweise Einführung eines integrierten Grenzschutzsystems an den Außengrenzen erforderlich sind;

e) die Abschaffung der Kontrolle von Personen gleich welcher Staatsangehörigkeit beim Überschreiten der Binnengrenzen.

(3) Erscheint zur Erleichterung der Ausübung des in Artikel AEUV Artikel 20 Absatz AEUV Artikel 20 Absatz 2 Buchstabe a genannten Rechts ein Tätigwerden der Union erforderlich, so kann der Rat gemäß einem besonderen Gesetzgebungsverfahren Bestimmungen betreffend Pässe, Personalausweise, Aufenthaltstitel oder diesen gleichgestellte Dokumente erlassen, sofern die Verträge hierfür anderweitig keine Befugnisse vorsehen. Der Rat beschließt einstimmig nach Anhörung des Europäischen Parlaments.

(4) Dieser Artikel berührt nicht die Zuständigkeit der Mitgliedstaaten für die geografische Festlegung ihrer Grenzen nach dem Völkerrecht.

10 Artikel 289 AEUV

[Ordentliches und besonderes Gesetzgebungsverfahren; Initiativrecht in besonderen Fällen]

(1) Das ordentliche Gesetzgebungsverfahren besteht in der gemeinsamen Annahme einer Verordnung, einer Richtlinie oder eines Beschlusses durch das Europäische Parlament und den Rat auf Vorschlag der Kommission. Dieses Verfahren ist in Artikel AEUV Artikel 294 festgelegt.

(2) In bestimmten, in den Verträgen vorgesehenen Fällen erfolgt als besonderes Gesetzgebungsverfahren die Annahme einer Verordnung, einer Richtlinie oder eines Beschlusses durch das Europäische Parlament mit Beteiligung des Rates oder durch den Rat mit Beteiligung des Europäischen Parlaments.

(3) Rechtsakte, die gemäß einem Gesetzgebungsverfahren angenommen werden, sind Gesetzgebungsakte.

(4) In bestimmten, in den Verträgen vorgesehenen Fällen können Gesetzgebungsakte auf Initiative einer Gruppe von Mitgliedstaaten oder des Europäischen Parlaments, auf Empfehlung der Europäischen Zentralbank oder auf Antrag des Gerichtshofs oder der Europäischen Investitionsbank erlassen werden.

3. Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben (ABl. L 188 vom 12.07.2019, S. 67)

11 Erwägungsgrund 2

Die Unionsbürgerschaft verleiht jedem Bürger der Union das Recht auf Freizügigkeit vorbehaltlich bestimmter Beschränkungen und Bedingungen. Mit der Richtlinie 2004/38/EG des Europäischen Parlaments und des Rates wird dieses Recht konkret ausgestaltet. In Artikel 45 der Charta der Grundrechte der Europäischen Union (im Folgenden "Charta") sind die Freizügigkeit und die Aufenthaltsfreiheit ebenfalls verankert. Die Freizügigkeit schließt das Recht ein, mit einem gültigen Personalausweis oder Reisepass Mitgliedstaaten zu verlassen und in Mitgliedstaaten einzureisen.

12 Erwägungsgrund 17

Sicherheitsmerkmale sind erforderlich, um ein Dokument auf seine Echtheit zu überprüfen und die Identität einer Person festzustellen. Die Festlegung von Mindestsicherheitsstandards und die Aufnahme biometrischer Daten in Personalausweise und Aufenthaltskarten für Familienangehörige, die nicht die Staatsangehörigkeit eines Mitgliedstaats besitzen, ist ein wichtiger Schritt, um die Verwendung dieser Dokumente in der Union sicherer zu machen. Die Aufnahme solcher biometrischen Identifikatoren sollte gewährleisten, dass die Unionsbürger in vollem Umfang von ihren Freizügigkeitsrechten Gebrauch machen können.

13 Erwägungsgrund 18

Die Speicherung eines Gesichtsbilds und zweier Fingerabdrücke (im Folgenden "biometrische Daten") auf Personalausweisen und Aufenthaltskarten, die in Bezug auf biometrische Pässe und Aufenthaltstitel für Drittstaatsangehörige bereits vorgesehen ist, stellt eine geeignete Kombination einer zuverlässigen Identifizierung und Echtheitsprüfung im Hinblick auf eine Verringerung des Betrugsrisikos dar, um die Sicherheit von Personalausweisen und Aufenthaltskarten zu verbessern.

14 Erwägungsgrund 19

Als allgemeine Praxis sollten die Mitgliedstaaten zur Überprüfung der Echtheit des Dokuments und der Identität des Inhabers in der Regel vorrangig das Gesichtsbild überprüfen und nur darüber hinaus, falls zur zweifelsfreien Bestätigung der Echtheit des Dokuments und der Identität des Inhabers notwendig, auch die Fingerabdrücke.

15 Erwägungsgrund 21

Diese Verordnung stellt keine Rechtsgrundlage für die Einrichtung oder Aufrechterhaltung von Datenbanken auf nationaler Ebene zur Speicherung biometrischer Daten in den Mitgliedstaaten dar, zumal es sich dabei um eine Frage des nationalen Rechts handelt, welches dem Unionsrecht im Bereich Datenschutz entsprechen muss. Diese Verordnung stellt ferner keine Rechtsgrundlage für die Einrichtung oder Aufrechterhaltung einer zentralen Datenbank auf der Ebene der Union dar.

16 Erwägungsgrund 22

Die biometrischen Identifikatoren sollten auf dem Speichermedium von Personalausweisen und Aufenthaltsdokumenten für die Zwecke der Überprüfung der Echtheit des Dokuments und der Identität des Inhabers erfasst und gespeichert werden. Diese Überprüfung sollte ausschließlich durch ordnungsgemäß befugte Mitarbeiter erfolgen dürfen und ferner nur, wenn die Vorlage des Dokuments gesetzlich vorgeschrieben ist. Ferner sollten biometrische Daten, die für den Zweck der Personalisierung von Personalausweisen oder Aufenthaltsdokumenten gespeichert werden, auf eine hochsichere Weise gespeichert werden sowie ausschließlich bis zu dem Datum der Abholung des Dokuments und keinesfalls länger als 90 Tage ab dem Datum der Ausstellung des Dokuments. Nach diesem Zeitpunkt sollten die biometrischen Identifikatoren umgehend gelöscht oder vernichtet werden. Jede weitere Verarbeitung dieser Daten in Übereinstimmung mit den Datenschutzvorschriften nach Unionsrecht und nationalem Recht sollte hiervon unberührt bleiben.

17 Erwägungsgrund 40

In Bezug auf die im Rahmen der Anwendung dieser Verordnung zu verarbeitenden personenbezogenen Daten gilt die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates. Es muss weiter präzisiert werden, welche Garantien für die verarbeiteten personenbezogenen Daten sowie insbesondere für sensible Daten wie beispielsweise biometrische Identifikatoren gelten. Die betroffenen Personen sollten darauf hingewiesen werden, dass ihre Dokumente mit einem den kontaktlosen Datenzugriff ermöglichenden Speichermedium, das die sie betreffenden biometrischen Daten enthält, versehen sind; außerdem sollten sie von allen Fällen in Kenntnis gesetzt werden, in denen die in ihren Personalausweisen und Aufenthaltsdokumenten erfassten Daten verwendet werden. In jedem Fall sollten die betroffenen Personen Zugang zu den personenbezogenen Daten haben, die in ihren Personalausweisen und Aufenthaltsdokumenten verarbeitet werden, und sie berichtigen lassen können, indem ein neues Dokument ausgestellt wird, wenn Daten falsch oder unvollständig sind. Das Speichermedium sollte hochsicher sein, und die auf ihm gespeicherten personenbezogenen Daten sollten wirksam vor unbefugtem Zugriff geschützt sein.

18 Erwägungsgrund 41

Die Mitgliedstaaten sollten gemäß der Verordnung (EU) 2016/679 für die ordnungsgemäße Verarbeitung biometrischer Daten verantwortlich sein, die von der Erfassung der Daten bis zu ihrer Aufnahme in das hochsichere Speichermedium reicht.

19 Artikel 3 VO (EU) 2019/1157

Sicherheitsstandards/Gestaltung/Spezifikationen

(1) Die von den Mitgliedstaaten ausgestellten Personalausweise werden im ID-1-Format hergestellt und sind mit einem maschinenlesbaren Bereich ausgestattet. Diese Personalausweise orientieren sich an den Spezifikationen und Mindestsicherheitsstandards des ICAO-Dokuments 9303 und entsprechen den Anforderungen der Buchstaben c, d, f und g des Anhangs der Verordnung (EG) Nr. 1030/2002, geändert durch die Verordnung (EU) 2017/1954.

(2) Die Datenelemente von Personalausweisen entsprechen den Spezifikationen des Teils 5 des ICAO-Dokuments 9303. Abweichend von Unterabsatz 1 kann die Dokumentennummer in Zone I erfasst werden, und die Angabe des Geschlechts ist optional.

(3) Auf dem Dokument erscheint der Titel „Personalausweis“ oder eine andere bereits etablierte nationale Bezeichnung in der Amtssprache oder den Amtssprachen des ausstellenden Mitgliedstaats sowie das Wort „Personalausweis“ in mindestens einer weiteren Amtssprache der Organe der Union.

(4) Auf der Vorderseite des Personalausweises erscheint der zwei Buchstaben umfassende Ländercode des ausstellenden Mitgliedstaats im Negativdruck in einem blauen Rechteck, umgeben von zwölf gelben Sternen.

(5) Die Personalausweise werden mit einem hochsicheren Speichermedium versehen, das ein Gesichtsbild des Personalausweisinhabers und zwei Fingerabdrücke in interoperablen digitalen Formaten enthält. Bei der Erfassung der biometrischen Identifikatoren wenden die Mitgliedstaaten die technischen Spezifikationen gemäß dem Durchführungsbeschluss der Kommission C(2018)7767 an.

20 Artikel 11 VO (EU) 2019/1157

Schutz personenbezogener Daten und Haftung

(1) Unbeschadet der Verordnung (EU) 2016/679 gewährleisten die Mitgliedstaaten die Sicherheit, Integrität, Echtheit und vertrauliche Behandlung der für die Zwecke dieser Verordnung erfassten und gespeicherten Daten.

(2) Für die Zwecke dieser Verordnung gelten die für die Ausstellung von Personalausweisen und Aufenthaltsdokumenten zuständigen Behörden als der Verantwortliche gemäß Artikel 4 Absatz 7 der Verordnung (EU) 2016/679, und sind für die Verarbeitung personenbezogener Daten verantwortlich.

(3) Die Mitgliedstaaten sorgen dafür, dass die Aufsichtsbehörden ihren Aufgaben gemäß der Verordnung (EU) 2016/679 umfassend nachkommen können, was den Zugang zu allen personenbezogenen Daten und allen erforderlichen Informationen sowie zu den Geschäftsräumen und Datenverarbeitungsgeräten der zuständigen Behörden einschließt.

(4) Durch die Zusammenarbeit mit externen Dienstleistungsanbietern wird ein Mitgliedstaat nicht von der Haftung nach dem Unionsrecht oder dem nationalen Recht für Verstöße gegen Pflichten im Zusammenhang mit personenbezogenen Daten befreit.

(5) Maschinenlesbare Informationen dürfen nur gemäß dieser Verordnung oder dem nationalen Recht des ausstellenden Mitgliedstaats in einen Personalausweis und ein Aufenthaltsdokument aufgenommen werden.

(6) Auf dem Speichermedium von Personalausweisen und Aufenthaltsdokumenten gespeicherte biometrische Daten dürfen nur gemäß dem Unionsrecht und dem nationalen Recht von ordnungsgemäß befugten Mitarbeitern der zuständigen nationalen Behörden und Agenturen der Union verwendet werden, um

a) den Personalausweis oder das Aufenthaltsdokument auf seine Echtheit zu überprüfen,

b) die Identität des Inhabers anhand direkt verfügbarer abgleichbarer Merkmale zu überprüfen, wenn die Vorlage des Personalausweises oder Aufenthaltsdokuments gesetzlich vorgeschrieben ist.

(7) Die Mitgliedstaaten halten eine Liste der zuständigen Behörden vor, die Zugang zu den biometrischen Daten haben, die auf dem in Artikel 3 Absatz 5 dieser Verordnung genannten Speichermedium gespeichert sind, und übermitteln diese Liste jährlich der Kommission. Die Kommission veröffentlicht im Internet eine Zusammenstellung dieser nationalen Listen.

4. Verordnung (EU) 2016/679 des Europäische Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DS-GVO; ABl. EU vom 4.5.2016, L 119, S. 1)

21 Artikel 9 VO (EU) 2016/679

Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,

b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,

c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,

d) die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,

e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,

f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,

g) die Verarbeitung ist 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,

h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,

i) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

j) die Verarbeitung ist 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, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.

(3) Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

(4) Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

22 Artikel 35 VO (EU) 2016/679

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

[…]

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

5. Personalausweisgesetz (PAuswG) vom 18. Juni 2009 (BGBl. I S. 1346), das zuletzt durch Artikel 2 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2281) geändert worden ist, (BGBl I 2009, 1346)

23 § 5 PAuswG

Ausweismuster; gespeicherte Daten

[…]

(9) Die auf Grund der Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben (ABl. L 188 vom 12.7.2019, S. 67), auf dem elektronischen Speichermedium zu speichernden zwei Fingerabdrücke der antragstellenden Person werden in Form des flachen Abdrucks des linken und rechten Zeigefingers im elektronischen Speicher- und Verarbeitungsmedium des Personalausweises gespeichert. Bei Fehlen eines Zeigefingers, ungenügender Qualität des Fingerabdrucks oder Verletzungen der Fingerkuppe wird ersatzweise der flache Abdruck entweder des Daumens, des Mittelfingers oder des Ringfingers gespeichert. Fingerabdrücke sind nicht zu speichern, wenn die Abnahme der Fingerabdrücke aus medizinischen Gründen, die nicht nur vorübergehender Art sind, unmöglich ist.

24 § 9 PAuswG

Ausstellung des Ausweises

(1) Personalausweise und vorläufige Personalausweise werden auf Antrag für Deutsche im Sinne des Artikels 116 Abs. 1 des Grundgesetzes ausgestellt. § 3a Abs. 1 des Verwaltungsverfahrensgesetzes ist nicht anzuwenden. Im Antragsverfahren nachzureichende Erklärungen können mittels Datenübertragung abgegeben werden. Die antragstellende Person und ihr gesetzlicher Vertreter können sich bei der Stellung des Antrags nicht durch einen Bevollmächtigten vertreten lassen. Dies gilt nicht für eine handlungs- oder einwilligungsunfähige antragstellende Person, wenn eine für diesen Fall erteilte, öffentlich beglaubigte oder beurkundete Vollmacht vorliegt. Die antragstellende Person und ihr gesetzlicher oder bevollmächtigter Vertreter sollen persönlich erscheinen.

(2) Für Minderjährige, die noch nicht 16 Jahre alt sind, und für Personen, die geschäftsunfähig sind und sich nicht nach Absatz 1 Satz 5 durch einen Bevollmächtigten vertreten lassen, kann nur diejenige Person den Antrag stellen, die sorgeberechtigt ist oder als Betreuer ihren Aufenthalt bestimmen darf. Sie ist

verpflichtet, für Jugendliche, die 16, aber noch nicht 18 Jahre alt sind, innerhalb von sechs Wochen, nachdem der Jugendliche 16 Jahre alt geworden ist, den Antrag auf Ausstellung eines Ausweises zu stellen, falls dies der Jugendliche unterlässt. Jugendliche, die mindestens 16 Jahre alt sind, dürfen Verfahrenshandlungen nach diesem Gesetz vornehmen.

(3) In dem Antrag sind alle Tatsachen anzugeben, die zur Feststellung der Person des Antragstellers und seiner Eigenschaft als Deutscher notwendig sind. Die Angaben zum Doktorgrad und zu den Ordens- und Künstlernamen sind freiwillig. Die antragstellende Person hat die erforderlichen Nachweise zu erbringen. Fingerabdrücke von Kindern sind nicht abzunehmen, solange die Kinder noch nicht sechs Jahre alt sind.

(4) Bestehen Zweifel über die Person des Antragstellers, sind die zur Feststellung seiner Identität erforderlichen Maßnahmen zu treffen. Die Personalausweisbehörde kann die Durchführung erkennungsdienstlicher Maßnahmen veranlassen, wenn die Identität der antragstellenden Person auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann. Ist die Identität festgestellt, so sind die im Zusammenhang mit der Feststellung angefallenen Unterlagen zu vernichten. Die Vernichtung ist zu protokollieren.

(5) Die Unterschrift durch ein Kind ist zu leisten, wenn es zum Zeitpunkt der Beantragung des Ausweises zehn Jahre oder älter ist.

(6) Für Deutsche im Sinne des Artikels 116 Absatz 1 des Grundgesetzes werden nach Maßgabe des § 6a Ersatz-Personalausweise von Amts wegen ausgestellt. Absatz 1 Satz 2 bis 6, Absatz 2 Satz 3, Absatz 3 Satz 1 bis 3 sowie die Absätze 4 und 5 gelten entsprechend.

III.

25 Das vorlegende Gericht ist zur Vorlage der Frage gemäß Art. 267 Abs. 1 lit. b, Abs. 2 AEUV berechtigt. Denn in Frage steht die Gültigkeit von Art. 3 Abs. 5 VO (EU) 2019/1157, der sekundäres Unionsrecht darstellt.

26 Die Entscheidung über die Frage ist für den Erlass des Urteiles erforderlich. Falls Art 3 Abs. 5 VO (EU) 2019/1157 gegen höherrangiges Recht der Europäischen Union verstößt, hat der Kläger einen Anspruch auf Ausstellung eines Personalausweises ohne die Aufnahme von Fingerabdrücken, § 9 Abs. 1 S. 1 PAuswG. Die nationale

Regelung in § 5 Abs. 9 PAuswG würde ihre Grundlage verlieren, da sie gegen Unionsrecht verstoßen würde.

27 Selbst wenn der alte Personalausweis des Klägers trotz defektem Chip gemäß § 28 Abs. 3 PAuswG weiterhin gültig ist, so muss sich der Kläger spätestens nach Ablauf der auf 10 Jahre ausgelegten Gültigkeitsdauer einen neuen Personalausweis ausstellen lassen. Zudem kann der Kläger nach § 6 Abs. 2 PAuswG vor Ablauf der Gültigkeit eines Personalausweises einen neuen Personalausweis beantragen, wenn ein berechtigtes Interesse an der Neuausstellung dargelegt wird. Im Falle eines defekten Chips ist die Nutzung der Online-Ausweisfunktion nicht mehr möglich. Auch ist die automatisierte Grenzkontrolle nicht mehr nutzbar (https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Digitale-Verwaltung/Online-Ausweisfunktion/FAQ-Online-Ausweisfunktion/faq-online-ausweisfunktion_node.html). In dieser eingeschränkten Nutzungsmöglichkeit ist ein berechtigtes Interesse an einer Neuausstellung zu sehen.

28 Das vorlegende Gericht hat Zweifel daran, ob Art. 3 Abs. 5 VO (EU) 2019/1175 unionsrechtskonform ist. Diese Zweifel beruhen auf dem Zustandekommen der Verordnung (EU) 2019/1157 im ordentlichen Gesetzgebungsverfahren, auf der Vereinbarkeit des Art. 3 Abs. 5 VO (EU) 2019/1157 mit Art. 7 und 8 GrCh und auf der fehlenden Abwägungsentscheidung nach Art. 35 Abs. 10 DS-GVO.

29 **1.** Zur Überzeugung des Gerichts hätte für den Erlass der VO (EU) 2019/1157 das besondere Gesetzgebungsverfahren des Art. 77 AEUV durchgeführt werden müssen.

30 Der AEUV unterscheidet in dessen Art. 289 zwischen dem ordentlichen Gesetzgebungsverfahren und den besonderen Gesetzgebungsverfahren. Die VO (EU) 2019/1157 wurde auf Art. 21 Abs. 2 AEUV gestützt und auf Vorschlag der Europäischen Kommission nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente, nach Stellungnahme des Europäischen Wirtschafts- und

Sozialausschusses und nach Anhörung des Ausschusses der Regionen gemäß dem ordentlichen Gesetzgebungsverfahren erlassen.

31 Laut Art. 21 Abs. 2 AEUV können das Europäische Parlament und der Rat gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften erlassen, mit denen die Ausübung des Freizügigkeitsrechts erleichtert wird, wenn zur Erreichung dieses Ziels ein Tätigwerden der Union erforderlich erscheint und die Verträge hierfür keine Befugnisse vorsehen.

32 Art. 77 Abs. 3 S. 1 AEUV enthält eine weitere Kompetenznorm, die sich unter anderem auf Regelungen zu Personalausweisen bezieht. Gemäß dieser Norm kann der Rat gemäß einem besonderen Gesetzgebungsverfahren Bestimmungen betreffend Pässe, Personalausweise, Aufenthaltstitel oder diesen gleichgestellte Dokumente erlassen, sofern die Verträge hierfür anderweitig keine Befugnisse vorsehen, falls zur Erleichterung der Freizügigkeit ein Tätigwerden der Union erforderlich ist. Der Rat beschließt einstimmig nach Anhörung des Europäischen Parlaments. Durch dieses Erfordernis der Einstimmigkeit wird den Mitgliedstaaten auf diesem Gebiet ein Höchstmaß an Souveränität belassen (von der Groeben/Schwarze/Sarah Progin-Theuerkauf, 7. Aufl. 2015, AEUV Art. 77, Rn 22).

33 Art. 77 AEUV entspricht dem damaligen Art. 62 EGV (EG-Vertrag). Die VO (EG) 2252/2004, in deren Art. 1 Abs. 2 bestimmt ist, dass Fingerabdrücke in Reisepässen gespeichert werden, wurde damals vom Verordnungsgeber auf Art. 62 EGV gestützt. Mit Urteil vom 17.10.2013 entschied der Europäische Gerichthof, dass Art. 62 Nr. 2 Buchst. a EGV eine geeignete Rechtsgrundlage für den Erlass der VO (EG) 2252/2004, insbesondere deren Art. 1 Abs. 2, darstellte (EuGH, Urteil vom 17.10.2013 – C-291/12 –, Rn. 20; CELEX 62012CJ0291).

34 Die Kompetenz nach Art. 77 Abs. 3 AEUV geht Art. 21 Abs. 2 AEUV vor, da Art. 77 Abs. 3 AEUV als dem Inhalt nach speziellere Vorschrift höhere Anforderungen an das Gesetzgebungsverfahren stellt (Schwarze/Becker/Hatje/Schoo, EU-Kommentar, AEUV Art. 77 Rn. 20, beck-online) und Art. 21 Abs. 2 AEUV nur dann einschlägig ist, wenn die Verträge für das Erreichen des Ziels der Förderung der Freizügigkeit keine

anderen Befugnisse vorsehen. Die VO (EU) 2019/1157 bezieht sich zwar nicht auf die Weiterentwicklung des Schengen-Besitzstandes, intendiert aber wie die VO (EG) 2252/2004 die Angleichung der Sicherheitsmerkmale und die Aufnahme biometrischer Identifikatoren als wichtigen Schritt zur Verwendung neuer Elemente im Hinblick auf künftige Entwicklungen auf europäischer Ebene. Hierdurch soll wie bei der VO (EG) 2252/2004 die Sicherheit von Dokumenten (hier: Personalausweisen statt Reisepässen) erhöht werden.

35 Nach alledem ist das Gericht der Auffassung, dass es für den wirksamen Erlass der VO (EU) 2019/1157 – und damit auch des Art. 3 Abs. 5 dieser Verordnung – des besonderen Gesetzgebungsverfahrens nach Art. 77 Abs. 3 AEUV bedurft hätte.

36 2. Zudem bestehen inhaltliche Zweifel an der Vereinbarkeit der Erfassung und Speicherung von Fingerabdrücken bei Personalausweisen mit Art. 7 und 8 GrCh.

37 Nach Art. 7 GrCh hat jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation. Aus Art. 8 GrCh folgt das Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten.

38 Bereits im Urteil vom 17.10.2013 hat der Europäische Gerichtshof festgestellt, dass die Erfassung und die Speicherung von Fingerabdrücken durch die nationalen Behörden in Reisepässen, die in Art. 1 Abs. 2 der Verordnung Nr. 2252/2004 geregelt sind, einen Eingriff in die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellen (EuGH, Urteil vom 17.10.2013 – C-291/12 –, Rn. 30, CELEX 62012CJ0291). Fingerabdrücke sind personenbezogene Daten, da sie objektiv unverwechselbare Informationen über natürliche Personen enthalten und deren genaue Identifizierung ermöglichen (EuGH, Urteil vom 17.10.2013 – C-291/12 –, Rn. 27, CELEX 62012CJ0291, unter Verweis auf EGMR, Urteil vom 04.12.2008, S. und Marper/Vereinigtes Königreich, Reports of judgments and decisions 2008-V, S. 213, §§ 68 und 84). Dieselben Grundrechte sind auch bei der Erfassung und Speicherung von Fingerabdrücken bei Personalausweisen betroffen.

39 Das Gericht hat Zweifel daran, ob die Erfassung der Fingerabdrücke und damit ein Eingriff in Art. 7 und 8 GrCh auch bei Personalausweisen gerechtfertigt ist.

40 Nach Art. 52 GrCh muss jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

41 Zudem ist in Art. 8 Abs. 2 GrCh bestimmt, dass personenbezogene Daten nur mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden dürfen.

42 Im vorliegenden Fall liegt zur Überzeugung des Gerichts – ebenso wie der Europäische Gerichtshof zu Reisepässen entschieden hat – keine Einwilligung der einen Personalausweis beantragenden Personen in die Erfassung ihrer Fingerabdrücke vor. Jedoch bestimmt dies Art. 3 Abs. 5 VO (EU) 2019/1157 als gesetzliche Regelung für alle Personalausweise.

43 Gemäß § 1 Abs. 1 S. 1 PAuswG sind alle Deutschen verpflichtet, einen gültigen Ausweis zu besitzen, sobald sie 16 Jahre alt sind und der allgemeinen Meldepflicht unterliegen oder, ohne ihr zu unterliegen, sich überwiegend in Deutschland aufhalten. Zur Ausstellung dieses Dokuments ist die Abnahme von Fingerabdrücken damit zwingend vorgeschrieben. Da eine Personalausweispflicht besteht, kann nicht davon ausgegangen werden, dass diejenigen, die einen Personalausweis beantragen, in eine solche Datenverarbeitung eingewilligt haben (so auch EuGH, Urteil vom 17.10.2013 – C-291/12 – Rn. 31, CELEX 62012CJ0291).

44 Mithin bedarf es nach Art. 52 Abs. 1 GrCh einer ***legitimen*** gesetzlichen Grundlage.

45 Zwar ist die Aufnahme von Fingerabdrücken in Personalausweisen in Art. 3 Abs. 5 VO (EU) 2019/1157 gesetzlich vorgesehen. Auch entspricht dies zumindest in Teilen den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen.

46 Ausweislich der Erwägungsgründe (1), (4) und (46) dient die VO (EU) 2019/1157 dazu, die Freizügigkeit zu stärken und der Fälschung von Dokumenten und der Vorspiegelung falscher Tatsachen in Bezug auf die an das Aufenthaltsrecht geknüpften Bedingungen vorzubeugen. Die Freizügigkeit schließt das Recht ein, mit einem gültigen Personalausweis oder Reisepass Mitgliedstaaten zu verlassen und in Mitgliedstaaten einzureisen, Erwägungsgrund (2). Nach Erwägungsgrund (18) dient die Aufnahme von Fingerabdrücken dazu, dass in Kombination mit dem Gesichtsbild eine zuverlässige Identifizierung des Inhabers und eine Verringerung des Betrugsrisikos erreicht werden kann.

47 Innerhalb der Europäischen Union kann der Personalausweis im Rahmen der Grenzüberschreitung genutzt werden. Außerdem erlauben auch Staaten, die nicht der EU angehören, die Einreise mit dem Personalausweis, so etwa insbesondere die Schweiz, Island, Norwegen, Albanien und Montenegro. Der Personalausweis wird vor diesem Hintergrund zumindest auch als Reisedokument genutzt, sodass hierdurch die Regelung auch dem Zweck dient, die illegale Einreise aus diesen Ländern zu verhindern. Dies würde eine von der Union anerkannte dem Gemeinwohl dienende Zielsetzung darstellen (EuGH, Urteil vom 17.10.2013 – C-291/12 –, Rn. 38, CELEX 62012CJ0291). Allerdings liegt der Hauptzweck des Personalausweises gerade nicht primär darin, ein Reisedokument im Schengen-Raum wie der Reisepass zu sein. Insoweit verweisen die Erwägungsgründe der VO (EU) 2019/1157 zu Recht, entgegen denen in der VO 2252/2004, gerade nicht auf den Schengen-Raum als Raum der Freiheit.

48 Auch regelt die VO (EU) 2019/1157 die Nutzung der gespeicherten biometrischen Daten nicht in diesem Sinne, wenn in Art. 11 Abs. 6 VO (EU) 2019/1157 festlegt ist, dass die gespeicherten biometrischen Daten nur verwendet werden dürfen, um die Echtheit oder Identität des Inhabers zu überprüfen. Mithin lässt die VO (EU)

2019/1157 offen, wie die Freizügigkeit erleichtert werden soll. Das Ziel der Verhinderung illegaler Einreise kann insoweit nicht mit der Erleichterung der Freizügigkeit gleichgesetzt werden.

49 Selbst wenn die Regelung eine dem Gemeinwohl dienende Zielsetzung verfolgen sollte, bestehen jedoch Zweifel daran, ob Art. 3 Abs. 5 VO (EU) 2019/1157 verhältnismäßig ist. Dies wäre nur dann der Fall, wenn die Einschränkungen dieser Rechte aus der GrCh gemessen an den mit der VO (EU) 2019/1157 verfolgten Zielen und damit gemessen am Zweck, die illegale Einreise von Personen in das Unionsgebiet zu verhindern und eine zuverlässige Identifizierung des Ausweisinhabers zu ermöglichen, verhältnismäßig sind. Hierfür müssen die mit dieser Verordnung eingesetzten Mittel zur Erreichung dieser Ziele geeignet sein und nicht über das dazu Erforderliche hinausgehen (EuGH, Urteil vom 17.10.2013 – C-291/12 –, Rn. 40, Rn. 38, CELEX 62012CJ0291).

50 Hierbei muss der Ansicht des Gerichts nach berücksichtigt werden, dass der Personalausweis in tatsächlicher und rechtlicher Hinsicht nicht mit dem Reisepass gleichgesetzt werden kann, sondern dass hinsichtlich der Verwendung dieser Dokumente deutliche Unterschiede bestehen. Dennoch werden durch Art. 3 Abs. 5 VO (EU) 2019/1157 die beiden Dokumente hinsichtlich der Fingerabdrücke gleich behandelt.

51 Zwar kann der Personalausweis – wie oben bereits dargestellt – auch als Reisedokument verwendet werden. Dennoch unterscheiden sich Personalausweise und Reisepässe sowohl in rechtlicher, als auch praktischer Hinsicht. Selbst wenn Personalausweise auch als Reisedokumente im Freizügigkeitskontext genutzt werden, erfolgt keine routinemäßige Kontrolle zumindest bei Reisen zwischen EU-Mitgliedsstaaten. Zudem dürfte für die meisten Unionsbürger die primäre Funktion der nationalen Identitätskarte nicht mit der Freizügigkeit verknüpft sein. Personalausweise weisen nämlich über diese hinausgehende Nutzungsarten auf. So werden Personalausweise im Alltag unter anderem für Interaktionen mit den nationalen Verwaltungsbehörden oder mit privaten Dritten, wie etwa Banken oder

Fluggesellschaften genutzt. Unionsbürger, die ihre Freizügigkeit ausüben wollen würden, können dies bereits mit ihrem Reisepass tun (in diesem Sinne auch: Stellungnahme des Europäischen Datenschutzbeauftragten zur geplanten Einführung der Speicherung von Fingerabdrücken in Personalausweisen vom 10.08.2018, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en.pdf S. 10).

52 Zudem besteht in Deutschland eine Pflicht, einen Personalausweis zu besitzen, § 1 Abs. 1 S. 1 PAuswG. Der Bürger kann im Gegensatz zum Reisepass nicht selbst entscheiden, ob er einen Personalausweis beantragt oder nicht. Auch der Europäische Datenschutzbeauftragte ist der Ansicht, dass die Aufnahme und Speicherung von Fingerabdrücken weitreichende Auswirkungen auf bis zu 370 Mio. EU-Bürger hätte, da er bei 85 % der EU-Bevölkerung die obligatorische Abnahme von Fingerabdrücken verlangen würde. Dieser breit angelegte Anwendungsbereich sowie die höchst sensiblen Daten, die verarbeitet werden (Gesichtsbilder in Kombination mit Fingerabdrücken), verlangen eine gründliche Prüfung auf der Grundlage einer strengen Prüfung der Notwendigkeit (Stellungnahme des Europäischen Datenschutzbeauftragten zur geplanten Einführung der Speicherung von Fingerabdrücken in Personalausweisen vom 10.08.2018, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en.pdf S. 9, 10 m.w.N). Das Gericht folgt der Überlegung des Europäische Datenschutzbeauftragte, dass in Anbetracht der Unterschiede zwischen Personalausweisen und Reisepässen die Einführung von Sicherheitsmerkmalen, die für Reisepässe möglicherweise als angemessen gelten, für Personalausweise nicht automatisch gelten darf, sondern dies der Überlegung und einer gründlichen Analyse bedarf (ABl. C 338 vom 21.09.2018, S. 22). Diese fehlt vorliegend.

53 Das Gericht ist der Ansicht, dass sich in Kombination mit den oben geschilderten weit gefassten Verwendungsmöglichkeiten und der Vielzahl der betroffenen

Unionsbürger nach eine viel höhere Eingriffsintensität im Vergleich zu Reisepässen ergibt, die im Gegenzug auch eine stärkere Rechtfertigung erfordert.

54 Im Rahmen der Auslegung der Art. 7 und 8 GrCh sind auch die Wertungen der DS-GVO zu berücksichtigen. Ausweislich der Erwägungsgründe (1) und (2) der DS-GVO ist der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ein Grundrecht. Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Die DS-GVO soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.

55 Daktyloskopische Daten sind besondere Arten personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO, nämlich biometrische Daten. Diese werden in Art. 4 Nr. 14 DS-GVO definiert als mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten. Gemäß Art. 9 Abs. 1 DS-GVO ist die Verarbeitung solcher biometrischen Daten im Grundsatz untersagt und nur in eng gefassten Ausnahmefällen zulässig.

56 Soweit die Fingerabdrücke in Personalausweisen aufgenommen werden sollen, um die Fälschungssicherheit zu fördern, ist festzuhalten, dass in den Jahren 2013-2017 lediglich 38.870 gefälschte Identitätskarten festgestellt worden sein sollen und seit Jahren die Nutzung gefälschter Identitätskarten abnimmt (Stellungnahme des Europäischen Datenschutzbeauftragten zur geplanten Einführung der Speicherung von Fingerabdrücken in Personalausweisen vom 10.08.2018, abrufbar unter

https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en.pdf,S.11).

57 Es ist bereits nicht hinreichend deutlich, ob die Aufnahme von Fingerabdrücken die Sicherheit vor Fälschungen tatsächlich zu fördern vermag. Eine Übereinstimmung der biometrischen Daten, die auf dem Chip des Personalausweises gespeichert sind mit den Fingerabdrücken des Besitzers des Ausweises bestätigt lediglich, dass das Dokument zum Besitzer gehört. Aus der Übereinstimmung an sich folgt noch kein Nachweis der Identität, solange nicht der Personalausweis selbst als echt festgestellt wurde. Zwar ist anerkannt, dass die Nutzung biometrischer Daten die Wahrscheinlichkeit der erfolgreichen Fälschung eines Dokumentes reduziert, so dass die Aufnahme von Fingerabdrücken zumindest teilweise den Zweck fördern kann (Stellungnahme des Europäischen Datenschutzbeauftragten zur geplanten Einführung der Speicherung von Fingerabdrücken in Personalausweisen vom 10.08.2018, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en.pdf S. 13).

58 Ob jedoch diese Möglichkeit den weitreichenden Eingriff zu rechtfertigen vermag, erscheint höchst fraglich, zumal auch ein Personalausweis mit defektem Chip entgegen der VO (EU) 2019/1157 nach nationalem Recht weiterhin gültig ist. Hierzu führt das Bundesamt für Sicherheit in der Informationstechnik aus, dass „ein Ausweis mit funktionsunfähigem Chip seine Gültigkeit [behält], auch wenn der integrierte Chip erkennbar defekt ist. Die Sicherheit als Ausweisdokument ist durch die physischen Sicherheitsmerkmale gegeben“ (https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Digitale-Verwaltung/Online-Ausweisfunktion/FAQ-Online-Ausweisfunktion/faq-online-ausweisfunktion_node.html). Wenn jedoch die Sicherheit allein durch die physischen Sicherheitsmerkmale (insbesondere Mikroschriften, UV-Aufdrucke etc.) gegeben ist, stellt sich die Frage nach der Erforderlichkeit der Aufnahme von Fingerabdrücken umso deutlicher.

59 Auch der Europäische Datenschutzbeauftragte betonte, dass Sicherheitsmaßnahmen bezogen auf den Druck des Dokuments, wie etwa die Verwendung von Hologrammen oder Wassermarken, eine deutlich geringere Eingriffsintensität hätten. Diese Methoden würden keine Verarbeitung von personenbezogenen Daten beinhalten, wären jedoch auch dazu in der Lage, die Fälschung von Ausweisdokumenten zu verhindern und die Authentizität eines Dokuments zu verifizieren (Stellungnahme des Europäischen Datenschutzbeauftragten zur geplanten Einführung der Speicherung von Fingerabdrücken in Personalausweisen vom 10.08.2018, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en.pdf S. 16).

60 In diesem Rahmen ist auch eines der wichtigsten Prinzipien des europäischen Datenschutzrechts zu beachten: Das Prinzip der Datenminimierung bzw. Datensparsamkeit. Hiernach muss die Erhebung und Nutzung von persönlichen Daten verhältnismäßig und erforderlich, sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

61 Sollte es nötig sein, Fingerabdrücke zu erfassen, stellt sich auch die Frage, warum es der Ablichtung des gesamten Abdrucks bedarf. Hierdurch wird zwar die Interoperabilität der verschiedenen Arten der Systeme, die Fingerabdrücke erkennen können, gefördert. Diese Systeme können in drei Unterkategorien eingeteilt werden. Zum einen gibt es die Systeme, die komplette Ablichtungen der Fingerabdrücke speichern und vergleichen. Andere Systeme verwenden so genannte Minuzien. Diese Minuzien beschreiben eine Teilmenge von Charakteristiken, die aus den Ablichtungen der Fingerabdrücke gewonnen werden. Die dritte Kategorie sind Systeme, die mit einzelnen Mustern, die aus Ablichtungen der Fingerabdrücke extrahiert werden, arbeiten. Falls lediglich eine Minuzie gespeichert würde, könnte ein Mitgliedstaat, der mit einem System arbeitet, das eine Ablichtung des gesamten Fingerabdrucks verwendet, diese nicht nutzen. Die Speicherung des gesamten Fingerabdrucks fördert die Interoperabilität, jedoch erhöht sie die Anzahl der gespeicherten persönlichen Daten und damit das Risiko des Identitätsdiebstahles,

falls es zu einem Datenleck kommt (Stellungnahme des Europäischen Datenschutzbeauftragten zur geplanten Einführung der Speicherung von Fingerabdrücken in Personalausweisen vom 10.08.2018, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en.pdf S. 14).

62 Die in den Personalausweisen verwendeten RFID-Chips lassen sich unter Umständen auch von nicht autorisierten Scannern auslesen. Dies liegt daran, dass sie über ein Funkfeld aktiviert werden und im Anschluss die Daten in verschlüsselter Form übertragen. Damit hängt die Sicherheit des Verfahrens letztlich an der Qualität der Übertragungs- und Verschlüsselungstechnologie. Gerade die Verwendung des gesamten Fingerabdrucks wirkt sich in diesem Zusammenhang risikoerhöhend aus (in diesem Zusammenhang zu elektronischen Aufenthaltstiteln: NK-AuslR/*Schild*, 2. Aufl. 2016, AufenthG § 78 Rn. 37).

63 Bei alledem ist auch zu beachten, dass es sich bei Fingerabdrücken um biometrische Daten handelt. Der Verordnungsgeber hat unter anderem durch die Einführung von Art. 9 DS-GVO gezeigt, dass diese einem besonderen Schutz unterliegen.

64 Selbst die VO (EU) 2019/1157 verzichtet auf das „Sicherheitsmerkmal“ des Fingerabdrucks bei Kindern unter 12 Jahren und befreit Kinder unter 6 Jahren vollständig von der Pflicht zur Abgabe, Art. 3 Abs. 7 VO (EU) 2019/1157. Viel wichtiger ist aber, dass bei Personen, denen eine Abnahme von Fingerabdrücken physisch nicht möglich ist (z.B. bei Adermatoglyphie), diese von der Pflicht zur Abgabe befreit sind. Wozu dann dieses Sicherheitsmerkmal noch dienen soll, bleibt in der VO (EU) 2019/1157 ungeregelt und schlicht offen.

65 3. Der Europäische Datenschutzbeauftragte unterstreicht in seiner Stellungnahme vom 10.08.2018 ferner, dass Artikel 35 Abs. 10 DS-GVO auf die Erfassung und Verarbeitung der Fingerabdrücke Anwendung findet. Nach Artikel 35 Abs. 1 DS-GVO ist eine Datenschutz-Folgenabschätzung durchzuführen, bevor eine Verarbeitung

erfolgt, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Diese Datenschutz-Folgeabschätzung sollte sich insbesondere mit einer Beurteilung der Risiken für die Rechte und Freiheiten der betroffenen Personen sowie mit den Maßnahmen beschäftigen, mit denen gegen diese Risiken vorgegangen werden soll, wie Garantien und Sicherheitsvorkehrungen (Stellungnahme des Europäischen Datenschutzbeauftragten zur geplanten Einführung der Speicherung von Fingerabdrücken in Personalausweisen vom 10.08.2018, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en.pdf, S. 12).

66 Da die Rechtsgrundlage auf Unionsrecht, dem der Verantwortliche unterliegt, beruht und da diese Rechtsvorschriften den konkreten Verarbeitungsvorgang regeln, hat die allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage zu erfolgen (Art. 35 Abs. 10 DS-GVO). Eine solche Folgenabschätzung wäre daher bei Erlass der VO (EU) 2019/1157 durchzuführen gewesen. Sie ist ausweislich der Erwägungsgründe nicht erfolgt.

67 Das Gericht ist, wie der Europäische Datenschutzbeauftragte in seiner Stellungnahme vom 10.08.2018, der Auffassung, dass die Folgenabschätzung die obligatorische Aufnahme sowohl von Gesichtsbildern als auch von (zwei) Fingerabdrücken in Personalausweise nicht tragen würde. Bereits in Gesetzgebungsverfahren hat der Europäische Datenschutzbeauftragte empfohlen, vor diesem Hintergrund die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung biometrischer Daten (Gesichtsbild in Kombination mit Fingerabdrücken) erneut zu prüfen (ABl. C 338 vom 21.09.2018, S. 22).

68 Der Verordnungsgeber geht in Erwägungsgrund (40) auf diese Problematik in Bezug auf die DS-GVO nur sehr allgemein ein. Es verbleibt bei unbestimmten Aussagen, wie etwa, dass die Unionsbürger über das Speichermedium informiert werden solle und weiter präzisiert werden müsste, welche Garantien für die verarbeiteten personenbezogenen Daten sowie insbesondere für sensible Daten wie

beispielsweise biometrische Identifikatoren gelten. Das Speichermedium sollte hochsicher sein, und die auf ihm gespeicherten personenbezogenen Daten sollten wirksam vor unbefugtem Zugriff geschützt sein. Es bleibt vage, was mit „hochsicher“ gemeint ist und wie die Garantien und Schutzvorkehrungen ausgestaltet sein sollen. Insbesondere ist keine Abwägung mit den Risiken bei einem Datenleck des Chips und dem Eingriff in Art. 7 und 8 GrCh ersichtlich.

69 Es stellt sich daher die Frage, ob das Unterlassen einer verpflichtenden Risikofolgeabschätzung die Wirksamkeit einer Norm unberührt lassen kann oder nicht vielmehr bei zwingender Verpflichtung des Normgebers zur Durchführung einer Risikofolgeabschätzung sein Unterlassen zu einer Ungültigkeit der Norm führen muss. Andernfalls würde der Normgeber für sein Fehlverhalten belohnt werden.

70 Nach alledem ist eine Vorlage an den Europäischen Gerichtshof geboten, um eine Klärung zu erreichen, ob Art. 3 Abs. 5 VO (EU) 2019/1157 wirksam ist.

IV.

71 Der Beschluss ist unanfechtbar.

Schild **Dr. Buus** **Neckermann**

Beglaubigt:
Wiesbaden, den 20.01.2022

Acar
Justizbeschäftigte