



**MEISTERERNST
DÜSING
MANSTETTEN**

Partnerschaft von
Rechtsanwältinnen und
Rechtsanwälten mbB

Oststraße 2
48145 Münster

Tel. 0251/5 20 91-0
Fax 0251/5 20 91-52

E-Mail: info@meisterernst.de
www.meisterernst.de

Bernd Meisterernst
(bis 2018)

Mechtild Düsing
Fachanwältin für Agrar-,
Erb- und Verwaltungsrecht

Dietrich Manstetten
(bis 2021)

Dr. Frank Schulze
Fachanwalt für Verwaltungs-
recht, Dipl.-Verwaltungswirt

Klaus Kettner
Fachanwalt für Arbeits- und
Sozialrecht

Wilhelm Achelpöhler
Fachanwalt für Verwaltungs- und
für Urheber- und Medienrecht

Dr. Dirk Schuhmacher
Fachanwalt für Agrarrecht

Veronica Bundschuh
Fachanwältin für Arbeitsrecht

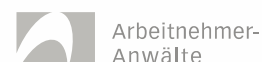
Dr. Rita Coenen
Fachanwältin für Familienrecht
Zertifizierte Mediatorin
Lehrbeauftragte Universität
Münster

Marius Schaefer, MLE
Fachanwalt für Arbeitsrecht

Anna-Kristina Pusch
Fachanwältin für Familien-
und Sozialrecht

**Henning
Schulte im Busch**
Fachanwalt für Agrar- und
Verwaltungsrecht

Dr. Andrea Bockey
Notarin · Fachanwältin für Erb-,
Verwaltungs- und Sozialrecht



Mitglied der
bundesweiten Kooperation
ArbeitnehmerAnwälte
www.arbeitnehmer-anwaelte.de



Meisterernst Düsing Manstetten Postfach 10 05 61 48054 Münster

Gerichtshof
der
Europäischen Union
Kanzlei



01.06.2022

In dem Vorabentscheidungsverfahren C-61/22 Landeshauptstadt
Wiesbaden,
Vorlegendes Gericht: Verwaltungsgericht Wiesbaden – Deutschland

nehmen wir namens und in Vollmacht des Klägers wie folgt Stellung:

Gliederung:

I Einleitung 1

II Der Rechtsstreit 3

III Rechtsausführungen 4

1. Verstoß gegen Art. 77 Abs. 3 AEUV 6
2. Verstoß gegen Art. 7 und 8 GrCh 14
 - (1) Gesetzlich vorgesehener Eingriff 16
 - (2) Von der Union anerkannte dem Gemeinwohl dienende Ziel-
setzungen 18
 - (3) Verhältnismäßigkeit 23
 - a) Geeignetheit 24
 - b) Erforderlichkeit 27

3. Verstoß gegen Art. 35 Abs. 10 DS-GVO 38

IV Beantwortung der Rechtsfragen 39

Partnerschaftsregister Amtsgericht Essen PR 3646 · Stnr.: 337/5716/0084
Sparkasse Münsterland Ost · IBAN: DE05 4005 0150 0000 2996 02 · BIC: WELADED1MST
Deutsche Bank · IBAN: DE06 4007 0024 0011 4009 00 · BIC: DEUTDE33HAN

1. I Einleitung

„Die Verwendung von biometrischen Daten in Informationssystemen ist keineswegs ... [unbedeutend], besonders dann nicht, wenn das betreffende System eine ... hohe Zahl von Personen betrifft. Biometrische Daten ... ändern ... unwiderruflich die Beziehung zwischen Körper und Identität, insofern sie die Merkmale des menschlichen Körpers ‚maschinenlesbar‘ machen und damit ihre weitere Verwendung ermöglichen. Auch wenn die biometrischen Daten nicht vom menschlichen Auge gelesen werden können, so können sie doch mit entsprechenden Hilfsmitteln gelesen und verwendet werden, und das für unbegrenzte Zeit, wo immer die betreffende Person sich auch aufhält.“

2. Diese Warnung des Europäischen Datenschutzbeauftragten¹ hat der Generalanwalt Paolo Mengozzi in der Rechtssache C-291/12 seinen Schlussanträgen vorangestellt. Gegenstand des Verfahrens in der Rechtssache C-291/12 war die mit der Verordnung Nr. 2252/2004 den Mitgliedstaaten auferlegte Verpflichtung, ihren Staatsangehörigen nur dann Pässe auszustellen, wenn sie sich der obligatorischen Erfassung von zwei Fingerabdrücken unterzogen haben, deren Bilder im Übrigen auf dem Pass selbst gespeichert werden. Gegenstand der Verordnung 2019/1157 ist die den Mitgliedsstaaten auferlegte Verpflichtung Personalausweise mit einem Speichermedium zu versehen, welches zwei Fingerabdrücke zu enthalten hat. Angesichts des Umstands, dass in der überwiegenden Zahl der Mitgliedstaaten, Belgien, Bulgarien, Deutschland, Estland, Griechenland, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Polen, Portugal Rumänien Slowakei, Slowenien Spanien Tschechien Ungarn und Zypern eine Verpflichtung besteht, einen Personalausweis mit sich zu führen hat diese Warnung des Europäischen Datenschutzbeauftragten besonderes Gewicht.

3. II Der Rechtsstreit

Der Kläger, ein deutscher Staatsangehöriger beantragte bei der Landeshauptstadt Wiesbaden erfolglos die Ausstellung eines Personalausweises ohne Fin-

¹ Stellungnahme des Europäischen Datenschutzbeauftragten vom 23. März 2005 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für den kurzfristigen Aufenthalt (ABl. C 181, S. 13).

gerabdrücke. Die Ausstellung des Personalausweises lehnte die Landeshauptstadt Wiesbaden unter Hinweis auf die Verordnung 2019/1157 des europäischen Parlaments und des Rates vom 20 Juni 2019 ab, ab, da seit dem 1.8.2021 die Aufnahme von Fingerabdrücken durch § 5 Abs. 9 des Personalausweisgesetzes verpflichtend sei. Am 21.12.2021 erhob der Kläger Klage vor dem Verwaltungsgericht Wiesbaden, mit dem Ziel die Landeshauptstadt Wiesbaden zu verpflichten, ihm einen Personalausweis ohne Fingerabdrücke auszustellen.

4. III Rechtsausführungen

5. Der Kläger ist wie das vorliegende Gericht der Ansicht, dass Art. 3 Abs. 5 VO (EU) 2019/1175 mit Art. 77 AEUV, Art. 7 und 8 GrCh sowie Art. 35 Abs. 10 DSGVO unvereinbar ist.

6. 1. Verstoß gegen Art. 77 Abs. 3 AEUV

Der Verordnungsgeber hat sich hinsichtlich der Kompetenz auf Artikel 21 Abs. 2 AEUV gestützt. Dieser sieht vor, dass Vorschriften im ordentlichen Gesetzgebungsverfahren erlassen werden können, wenn zur Erreichung dieses Ziels ein Tätigwerden der Union erforderlich erscheint und die Verträge hierfür keine Befugnisse vorsehen. Mit diesem Ziel ist das in Artikel 21 Abs. 1 AEUV genannte Recht, sich „frei zu bewegen und aufzuhalten“, gemeint. Dieses Recht wird wortgleich in Artikel 20 Abs. 2 lit. a AEUV aufgeführt.

7. Art. 77 Abs. 3 Satz 1 AEUV ist aber ein eigenständiger Kompetenztitel für „Bestimmungen betreffend Pässe, Personalausweise, Aufenthaltstitel oder diesen gleichgestellte Dokumente“ und sieht für diese Regelungen ein besonderes Gesetzgebungsverfahren vor. Hintergrund ist, dass Art. 18 Abs. 3 EGV früher gerade Vorschriften betreffend Pässe, Personalausweise, Aufenthaltstitel oder diesen gleichgestellte Dokumente aus dem Anwendungsbereich von Art. 18 Abs. 2 EGV (nunmehr Art. 21 Abs. 2 AEUV) herausgenommen hat. Es wird nicht ersichtlich, warum der Verordnungsgeber sich nicht auf Art. 77 Abs. 3 Satz 1 AEUV als Kompetenztitel gestützt hat, der *lex specialis* ist.

8. Bei der bestehenden Regelung für die Reisepässe hat sich der Verordnungsgeber auf Art. 62 Nr. 2 Buchst. a EG (a.F.) gestützt. Nach dieser Bestimmung hatte der Rat der Europäischen Union nach dem Verfahren des Art. 67 EG innerhalb eines Zeitraums von fünf Jahren nach Inkrafttreten des Vertrags von Amsterdam „Maßnahmen bezüglich des Überschreitens der Außengrenzen der Mitgliedstaaten, mit denen ... Normen und Verfahren [festgelegt werden], die von den Mitgliedstaaten bei der Durchführung der Personenkontrollen an diesen Grenzen einzuhalten sind“, zu beschließen. Die entsprechende Kompetenznorm wäre nunmehr Art. 77 Abs. 2 lit. b. Es ging mithin um eine Regelung im Bereich des Grenzschutzes².
9. Für die Kompetenzgrundlage aus Art. 21 Abs. 2 AEUV (Bestimmungen zur Erleichterung der Wahrnehmung des Rechts der Unionsbürger, sich im Hoheitsgebiet der Mitgliedsstaaten frei zu bewegen und aufzuhalten) und aus Art. 77 Abs. 2 lit. b AEUV (Kontrollen an den Außengrenzen) ist das ordentliche Gesetzgebungsverfahren vorgesehen, für Art. 77 Abs. 3 AEUV (Pass- und Ausweiswesen) hingegen das besondere Gesetzgebungsverfahren.
10. Art. 289 Abs. 1 und 2 AEUV unterscheidet zwischen dem ordentlichen Gesetzgebungsverfahren (näher dargelegt in Art. 294 AEUV) und dem in den Verträgen festgelegten besonderen Gesetzgebungsverfahren. Das besondere Gesetzgebungsverfahren ist je nach Regelungsgegenstand differenziert ausgestaltet, so dass ein einheitliches „besonderes Gesetzgebungsverfahren“ nicht existiert.
11. Art. 48 Abs. 7 UAbs. 2 EUV kann der Europäische Rat in Fällen, in denen nach Maßgabe des Vertrags über die Arbeitsweise der Europäischen Union Gesetzgebungsakte vom Rat gemäß einem besonderen Gesetzgebungsverfahren erlassen werden müssen, einen Beschluss erlassen, wonach die Gesetzgebungsakte gemäß dem ordentlichen Gesetzgebungsverfahren erlassen werden können.
12. Schon der Wortlaut „gemäß einem besonderen Gesetzgebungsverfahren erlassen werden müssen“ deutet darauf hin, dass hier – abseits von Art. 48 Abs. 7

² vgl. auch EuGH, Urteil vom 17. Oktober 2013 – C-291/12 –, Rn. 15-20

UAbs. 2 EUV – den Institutionen gerade kein Ermessen bei der Abkehr eines besonderen Gesetzgebungsverfahrens obliegt.

13. Dies dürfte also einen erheblichen Verfahrensverstoß darstellen, da als Kompetenztitel hier allein die speziellere Norm des Art. 77 Abs. 3 AEUV in Betracht kam. Die Kompetenz nach Art. 77 Abs. 3 AEUV stellt höhere Anforderungen an das Gesetzgebungsverfahren, etwa indem der Rat einstimmig nach Anhörung des Europäischen Parlaments entscheidet. Deshalb hätte die VO 2019/1157 im besonderen Gesetzgebungsverfahren erlassen werden müssen.

14. 2. Verstoß gegen Art. 7 und 8 GrCh

15. Die Erfassung und die Speicherung von Fingerabdrücken in Personalausweisen stellen einen Eingriff in die Rechte auf Achtung des Privatlebens (Art. 7 GrCh) und auf Schutz personenbezogener Daten (Art. 8 GrCh) dar.³ Nach Art. 52 Abs. 1 der Charta sind Einschränkungen der Ausübung dieser Rechte zulässig, sofern sie gesetzlich vorgesehen sind und den Wesensgehalt dieser Rechte achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit müssen sie erforderlich sein und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

16. (1) Gesetzlich vorgesehen.

17. Die Erfassung und Speicherung der Fingerabdrücke ist in Art. 5 Abs. 3 gesetzlich vorgesehen.

18. (2) Von der Union anerkannte dem Gemeinwohl dienende Zielsetzungen.

19. Die Verordnung also solche soll der Erleichterung der Freizügigkeit dienen. Dazu dient die Erfassung nach Logik des Gesetzgebers, indem die die Überprüfung der Echtheit und die Überprüfung der Identität ermöglicht wird.

20. Nach Artikel 11 Abs. 6 der EU-Verordnung dürfen auf dem Speichermedium von Personalausweisen und Aufenthaltsdokumenten gespeicherte biometrische Da-

³ vgl. zur Bejahung des Eingriffs für die Erfassung und Speicherung von Fingerabdrücken in Reisepässen: EuGH, Urteil vom 17. Oktober 2013 – C-291/12 –, Rn. 24-30.

ten 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. Jedoch wird nicht begründet, inwiefern dies die Freizügigkeit erleichtert.

21. Bei der Erfassung und Speicherung von Reisepässen wurden auch diese zwei konkreten Ziele verfolgt, nämlich erstens den Schutz vor Fälschung von Pässen und zweitens die Verhinderung der betrügerischen Verwendung von Pässen, d. h. deren Verwendung durch andere Personen als ihren rechtmäßigen Inhaber. Mit der Verfolgung dieser Ziele bezweckte diese Bestimmung aber nach der Rechtsprechung des EuGH insbesondere, die illegale Einreise von Personen in das Unionsgebiet zu verhindern⁴. Zwischen der Bekämpfung von Identitäts- und Dokumentenbetrug und dem Ziel der Bekämpfung der illegalen Einreise besteht damit ein Zusammenhang⁵. Das Ziel der Verhinderung illegaler Einreise ist aber nicht mit der Erleichterung der Freizügigkeit gleichzusetzen.

22. Es ist also schon nicht dargelegt, dass mit der Erfassung und Speicherung der Fingerabdrücke von der Union anerkannte dem Gemeinwohl dienende Zielsetzungen verfolgt werden.

23. (3) Verhältnismäßigkeit

Hinsichtlich der Prüfung der Verhältnismäßigkeit ist zu beachten, dass nach ständiger Rechtsprechung des EuGH der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene verlangt, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten auf das „absolut Notwendige“ zu beschränken haben⁶.

24. (a) Geeignetheit. Fingerabdrücke sind zu folgenden Maßnahmen geeignet:

⁴ vgl. Urteil vom 17. Oktober 2013 – C-291/12 –, Rn. 37

⁵ vgl. GA Giovanni Pitruzzella, Schlussantrag vom 2. Mai 2019 – C-70/28 – ECLI:EU:C:2019:361, Rn. 21

⁶ vgl. EuGH, Urteil vom 3. Oktober 2019 – C-70/18 –, Rn. 56 und Urteil vom 21. Dezember 2016 – C-203/15 und C-698/15 –, Rn. 96.

25. Echtheit des Dokuments: Zur Prüfung der Echtheit des Dokuments kann die Erfassung und Speicherung von Fingerabdrücken nur dann dienen, wenn man unterstellt, dass das Vorhandensein der Daten auf dem Chip eine eigenständige Hürde für das Fälschen oder Verfälschen des Dokuments darstellt. Mit anderen Worten: Nicht die Prüfung der Zuordnung des Fingerabdrucks zum (vermeintlichen) Dokumenteninhaber trägt zur Prüfung der Echtheit des Dokuments bei, sondern nur die Prüfung, ob überhaupt ein Fingerabdruck auf dem Chip vorliegt. In diesem Sinne hat der EuGH auch hinsichtlich der Erfassung und Speicherung von Fingerabdrücken in Reisepässen argumentiert: *„Bezüglich der Frage, ob Art. 1 Abs. 2 der Verordnung Nr. 2252/2004 geeignet ist, das Ziel des Schutzes vor Fälschungen von Reisepässen zu erreichen, ist unstreitig, dass die Speicherung von Fingerabdrücken auf einem Speichermedium mit hohem Sicherheitsstandard, wie sie in dieser Bestimmung vorgesehen ist, einen hohen technischen Entwicklungsstand erfordert. Sie ist daher geeignet, die Gefahr der Fälschung von Pässen zu verringern und die Aufgabe der mit der Überprüfung der Authentizität der Pässe an den Grenzen betrauten Stellen zu erleichtern“*⁷. Verifizierung: Ein auf dem Chip gespeicherter Fingerabdruck kann nur der Verifikation, aber nicht der Identifikation dienen. Verifikation meint, dass ermittelt wird, ob eine Person diejenige ist, die Inhaber des Ausweises ist. Es geht also um einen 1:1-Abgleich der überprüften Person. Identifikation meint hingegen, dass ermittelt wird, ob die biometrischen Daten einer realen Person, von der biometrische Daten (in einer Datenbank) gespeichert sind, entsprechen. Dieses Ziel ist jedoch nach der Verordnung gerade nicht erlaubt bzw. wird nicht verfolgt.

26. Auf diesen Unterschied hat der EuGH bei der Beurteilung der Erfassung und Speicherung von Fingerabdrücken in Reisepässen abgestellt, wenn er ausführt: *„Eine solche mangelnde Übereinstimmung [Anm.: der Fingerabdrücke des Inhabers des Reisepasses mit den in dieses Dokument aufgenommenen Daten] wird lediglich dazu führen, dass die Aufmerksamkeit der zuständigen Behörden auf den Betreffenden gelenkt und in der Folge in Bezug auf ihn eine eingehende Überprüfung vorgenommen wird, um seine Identität endgültig zu klären“*⁸.

⁷ EuGH, Urteil vom 17. Oktober 2013 – C-291/12 –, Rn. 41

⁸ EuGH, Urteil vom 17. Oktober 2013 – C-291/12 –, Rn. 44

27. (b) Erforderlichkeit

Der Gesetzgeber hat zu prüfen, ob Maßnahmen denkbar sind, die weniger stark in die durch die Art. 7 und 8 der Charta anerkannten Rechte eingreifen und trotzdem den Zielen der in Rede stehenden Unionsregelung wirksam dienen. Die Regelung ist darüber hinaus nur im Hinblick auf das Ziel gerechtfertigt, dass sie nicht eine Verarbeitung erfasster Fingerabdrücke mit sich bringt, die über das zur Erreichung des Ziels Erforderliche hinausgeht. Dabei ist der Schutz personenbezogener Daten für das Grundrecht auf Achtung des Privatlebens von „besonderer Bedeutung“⁹.

Hinsichtlich des Ziels ist in die Abwägung einzustellen, dass Ausgangspunkt der Regelungen der Verordnung die Auffindung von rund 40.000 gefälschten Personalausweisen in den Jahren 2013-2017, also auf das Jahr umgerechnet 8.000 gefälschte Personalausweise ist. Ebenso wie bei der Erfassung und Speicherung von Fingerabdrücken in Reisepässen dürfte die Erfassung zwar kein „Vorgang intimer Natur“ sein.¹⁰ Dennoch handelt es sich um hochsensible Daten, wie die Behandlung biometrischer Daten im europäischen Sekundärrecht zeigt. Nach Art. 9 Abs. 1 DSGVO handelt es sich bei biometrischen Daten nämlich um besonders schützenswerte Daten.

28. Der beste Schutz personenbezogener Daten ist dabei ihre Nicht-Erhebung. Diesem Grundsatz der „Datensparsamkeit“ bzw. „Datenminimierung“ – ein Grundsatz des Europäischen Datenschutzrechts – widerspricht die Erfassung und Speicherung der Fingerabdrücke aller Personen. Wie oben dargelegt, dient die Erfassung und Speicherung zwar der Prüfung der Echtheit der Dokumente. Dabei handelt es sich aber bloß um ein Sicherheitsmerkmal unter vielen.

29. Während die Aufnahme von Sicherheitsmerkmalen wie mehrfarbigen Guillochen, Mikroschriften, UV-Aufdrucken, optisch variablen Farben, taktilen Merkmale etc. sinnvoll ist erschließt sich das für Fingerabdrücke nicht. In diesem Zusammenhang interessant ist, dass das Bundesministerium des Inneren die Erfassung und Speicherung der Fingerabdrücke auch gar nicht als Sicherheitsmerkmal aufführt, vgl. BMI, Der Personalausweis, Stand August 2021, abrufbar unter

⁹ vgl. EuGH, Urteil vom 8. April 2014 – C-293/12 und C-594/12 –, Rn. 48.

¹⁰ vgl. EuGH, Urteil vom 17. Oktober 2013 – C-291/12 –, Rn. 48; bestätigt durch: EuGH, Urteil vom 3. Oktober 2019 – C-70/18 –, Rn. 58.

<https://www.bmi.bund.de/DE/themen/moderne-verwaltung/ausweise-und-paesse/personalausweis/personalausweis-node.html>, dort „Aktualisierter Flyer zu den Sicherheitsmerkmalen des Personalausweises“, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/moderneverwaltung/ausweise/Flyer_Sicherheitsmerkmale_Personalausweis.html).

30. Es ist auch aus den Materialien der EU-Kommission nicht ersichtlich, dass gerade die Speicherung von Fingerabdrücken hier zu einer entscheidenden Erhöhung der Sicherheit hinsichtlich der Echtheit führt. Vielmehr dürften gerade andere Maßnahmen (Vereinheitlichung der Personalausweise, Festlegung von Mindeststandards etc.) einen viel größeren Nutzen haben.
31. Hervorzuheben ist auch, dass das höhere Fälschungs- und Dokumentenrisiko insbesondere auf den Unterschieden in den Sicherheitsstandards beruht (vgl. Erwägungsgrund 5 der EU-VO). Es ist daher nicht zu beanstanden, dass gemeinsame Sicherheitsstandards eingeführt werden. Diese Sicherheitsstandards orientieren sich gem. Art. 3 Abs. 1 Satz 2 EU-VO an den Spezifikationen und Mindestsicherheitsstandards des ICAO-Dokuments 9303. Das ICAO-Dokument 9303 sieht eine Verpflichtung zur Erfassung und Speicherung aber gerade nicht vor. Während die Aufnahme eines Gesichtsbildes verpflichtend ist, um die Anforderungen des ICAO-Dokuments 9303 zu erfüllen, ist dies hinsichtlich der Erfassung und Speicherung von Fingerabdrücken gerade nicht der Fall¹¹.
32. Hinsichtlich der Menge der Daten ist zu konstatieren, dass nunmehr die Fingerabdrücke aller EU-Bürgerinnen und EU-Bürger, in deren Staaten ein Personalausweis Pflicht ist, erfasst und (auf dem jeweiligen Chip) gespeichert sind.
33. Dieser großen Anzahl von Menschen, nämlich (wohl rund 85 % der rund 450 Millionen Einwohner), stehen pro Jahr 8.000 gefälschte Personalausweise entgegen. Dies zeigt exemplarisch die Unverhältnismäßigkeit auf.

¹¹ vgl. INTERNATIONAL CIVIL AVIATION ORGANIZATION, Doc 9303, Machine Readable Travel Documents, Eighth Edition, 2021, Part 9: Deployment of Biometric Identification and Electronic Storage of Data in MRTDs, S. 8.

34. Außerdem liegt der Zweck des Personalausweises – im Gegensatz zu dem des Reisepasses – primär gar nicht darin, ein Reisedokument zu sein. Nur in dieser Randfunktion wird aber das Erfordernis der Erfassung und Speicherung von Fingerabdrücken begründet. Das heißt: Wegen einer bloßen untergeordneten Funktion, über die Bürgerinnen und Bürger auch nicht eigenständig oder freiwillig entscheiden können, wird ein Dokument, das sie zwangsweise zu anderen (primären) Zwecken benötigen, mit hochsensiblen Daten ausgestattet.
35. Deshalb kann man die Rechtsprechung des EuGH zu Fingerabdrücken in Reisepässen hinsichtlich der Prüfung der Verhältnismäßigkeit auch nur eingeschränkt heranziehen. So hat auch die EU-Kommission ausgeführt: „As regards the inclusion of fingerprints, account has to be taken of the case law of the Court of Justice. The Court concluded in C-291/12 ('Michael Schwarz v Stadt Bochum') that although the taking and storing of fingerprints in passports constitutes an infringement of the rights to respect for private life and the protection of personal data, the inclusion of fingerprints in passports is lawful given the general objective of preventing illegal entry into the EU and the protection of fraudulent use of passports. However, given that the ID cards serve more purposes than crossing the border and given the different traditions in Member States for the use of ID cards, it is not self-evident that the same conclusion could be drawn“¹².
36. Schlussendlich ist zu beachten, dass auch die Europäische Kommission selbst zunächst keine Verpflichtung zur Erfassung und Speicherung von Fingerabdrücken präferiert hat¹³. Alternative Szenarien sahen eine Pflicht nicht vor. Hinsichtlich von Personalausweisen gab es die „Option ID Soft)“ die „Option ID 1)“, die „Option ID 2)“ und die „Option ID 3)“. Erst die „Option ID 2)“ sah die verpflichtende Erfassung und Speicherung von Fingerabdrücken vor. In dem Dokument wird festgehalten: „Therefore, ID 1) is identified as the preferred option in both optimal solutions. Although less effective than ID 2), it is more efficient and proportional. ID 1) also address all specific objectives satisfactorily and leaves the Member States as much scope as possible for national decisions about a document that they regard as an “expression of the identity of their country“¹⁴“

¹² SWD(2018) 110 final, S. 60

¹³ vgl. SWD(2018) 110 final

¹⁴ SWD(2018) 110 final, S. 52

37. Zusammengefasst: Es werden hochsensible Daten aller Personen ohne ihren Willen erfasst und gespeichert und dies für Zwecke, die auch auf andere, das Persönlichkeitsrecht weniger beeinträchtigende Weise erreicht werden können und zudem das Dokument nur in seiner Rand- und Nebenfunktion als Reisedokument betreffen.

38. Verstoß gegen Art. 35 Abs. 10 DS-GVO

Mit dem vorliegenden Gericht und dem Europäischen Datenschutzbeauftragten in seiner Stellungnahme vom 10.08.2018 ist der Kläger der Auffassung, dass bei Erlass der Verordnung eine unzureichende Risikofolgenabschätzung erfolgt ist. Der europäische Datenschutzbeauftragte hat in dieser Stellungnahme darauf hingewiesen, dass im Kontext des Ordnungsgebungsprozesses zwar eine Folgenabschätzung erfolgt ist¹⁵ diese aber zu dem Ergebnis kam, dass eine verpflichtende Speicherung des Gesichtsbildes und eine fakultative Speicherung des Fingerabdrucks am geeignetsten sei¹⁶. Da dieser Folgenabschätzung nicht gefolgt wurde, wies der Europäische Datenschutzbeauftragte darauf hin, dass nicht davon ausgegangen werden könne, dass die Folgenabschätzung für den Zweck der Einhaltung von Art. 35 Abs. 10 DSGVO genüge. Der Europäische Datenschutzbeauftragte empfahl, „die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung biometrischer Daten (Gesichtsbild in Kombination mit Fingerabdrücken) erneut zu prüfen.“¹⁷ Eine solche Prüfung ist nicht erfolgt.

39. Beantwortung der Rechtsfragen.

Der Kläger ist deshalb der Ansicht, dass die Vorlagefragen des Verwaltungsgerichts Wiesbaden so zu beantworten sind, dass festgestellt wird, dass 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

¹⁵ (SWD(2018) 110 final v. 17.04.2018)

¹⁶ Stellungnahme, S. 13 Rn. 31).

¹⁷ Stellungnahme, S. 13 Rn. 33)

Recht auf Freizügigkeit ausüben (ABl. L 188 vom 12.07.2019, S. 67) gegen Art. 77 Abs. 3 AEUV, gegen Art. 7 und 8 GrCh und gegen Art. 35 Abs. 10 DS-GVO verstößt und diesem Grund ungültig ist.

Achelpöhler

Rechtsanwalt