6 K 2132/19.WI.A

VERWALTUNGSGERICHT WIESBADEN

BESCHLUSS

In dem Verwaltungsstreitverfahren

….

Kläger

bevollmächtigt:

Rechtsanwälte …

gegen

Bundesrepublik Deutschland,
vertreten durch das Bundesamt für Migration und Flüchtlinge,
…..

Beklagte

wegen

Asylrechts

hat das Verwaltungsgericht Wiesbaden - 6. Kammer - durch

Vorsitzenden Richter am VG Schild

als Einzelrichter

am 27. Januar 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:

1. **Führt eine fehlende bzw. unterlassende oder unvollständige Rechenschaftspflicht eines Verantwortlichen nach Art. 5 der Verordnung (EU) 2016/679 des Europäischen 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), z.B. durch ein fehlendes oder unvollständiges Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO oder eine fehlende Vereinbarung über ein gemeinsames Verfahren nach Art. 26 DS-GVO dazu,**
   dass die Datenverarbeitung unrechtmäßig im Sinne der Art. 17 Abs. 1 lit. d) DS-GVO und Art. 18 Abs. 1 lit. b) DS-GVO ist, sodass ein Löschungs- bzw. Beschränkungsanspruch des Betroffenen besteht?

2. **Falls Frage 1 zu bejahen ist: Führt das Bestehen eines Löschungs- oder Beschränkungsanspruchs dazu, dass die verarbeiteten Daten in einem Gerichtsverfahren nicht zu berücksichtigen sind? Dies jedenfalls dann, wenn die betroffene Person der Verwertung im gerichtlichen Verfahren widerspricht?**

3. **Falls Frage 1 zu verneinen ist: Führt ein Verstoß eines Verantwortlichen gegen Art. 5, 30 oder 26 DS-GVO dazu, dass ein nationales Gericht bei der Frage der gerichtlichen Verwertung der Datenverarbeitung die Daten nur berücksichtigen darf, wenn der Betroffene der Verwertung ausdrücklich zustimmt?**

I.

1 Der Kläger wendet sich vorliegend gegen einen ablehnenden Bescheid des Bundesamtes für Migration und Flüchtlinge und begehrt die Zuerkennung der Flüchtlingseigenschaft nach § 3 AsylG. Dem Bescheid der Beklagten liegt die sogenannte elektronische Bundesamtsakte MARIS zugrunde, welche auch im Rahmen eines gemeinsamen Verfahrens nach Art. 26 dem Gericht über das Elektronische Gerichts- und Verwaltungspostfach (EGVP) übermittelt wird. Bezüglich der Fragen zur vollständigen Aktenübermittlung wird auf die dem EuGH bereits vorgelegten Fragen (EuGH, Az. C-564/21; Verwaltungsgericht Wiesbaden, Beschluss vom 03.09.2021, Az. 6 L 582/21.WI.A) Bezug genommen.

2 Vorliegend bestehen Zweifel, ob ein Verzeichnis der Verarbeitungstätigkeiten überhaupt bzw. vollständig bezüglich der sogenannten elektronischen MARIS-Akte bei der Beklagten vorliegt. Auch existiert keine Vereinbarung bzw. gesetzliche Regelung bezüglich des Verfahrens zur elektronischen Aktenübermittlung und der Bestimmung der Verantwortlichkeiten in diesem Verfahren. Diese Unterlagen wurden von dem Gericht im Laufe des Verfahrens angefordert. Die Beklagte hat die Vorlage jedoch verweigert, unter anderem da hinsichtlich des EGVP eine Vereinbarung nach Art. 26 DS-GVO nicht vorliege.

3 Es stellt sich somit die Frage, wie zumindest in Falle einer (formellen) Rechtswidrigkeit der Verarbeitung der personenbezogenen Daten des Klägers bei der Beklagten durch das Gericht umzugehen ist. Denn nach der Richtlinie 2013/32/EU des Europäischen Parlaments und des Rates vom 26.06.2013 (ABl. L 180 vom 29.6.2013, S. 60) findet bei Asylverfahren nach nationalem Recht die DS-GVO Anwendung. Weder das Asylgesetz (AsylG), noch die Verfahrensordnung (VwGO) enthalten dazu Aussagen.

II.

1. Charta der Grundrechte der Europäischen Union (GrCh)

4 **Artikel 7 GrCh**
Achtung des Privat- und Familienlebens

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

5 **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.

2. 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)

6 Erwägungsgrund 82

Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.

7 Artikel 5 DS-GVO
Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

8 Artikel 9 DS-GVO
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.

9 Artikel 17 DS-GVO
Recht auf Löschung („Recht auf Vergessenwerden“)

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

10 Artikel 18 DS-GVO
Recht auf Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

a) die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,
b) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;

c) der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder

d) die betroffene Person Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

(2) Wurde die Verarbeitung gemäß Absatz 1 eingeschränkt, so dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden.

(3) Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Absatz 1 erwirkt hat, wird von dem Verantwortlichen unterrichtet, bevor die Einschränkung aufgehoben wird.

11 Artikel 26 DS-GVO
Gemeinsam Verantwortliche

(1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und Artikel 14, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

12 Artikel 30 DS-GVO
Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
b) die Zwecke der Verarbeitung;
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, das Folgendes enthält:

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz1.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn, die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10.

13 Artikel 94
Aufhebung der Richtlinie 95/46/EG

(1) Die Richtlinie 95/46/EG wird mit Wirkung vom 25. Mai 2018 aufgehoben.

(2) Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung. Verweise auf die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten gelten als Verweise auf den kraft dieser Verordnung errichteten Europäischen Datenschutzausschuss.

3. RICHTLINIE 2013/32/EU DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 26. Juni 2013 zu gemeinsamen Verfahren für die Zuerkennung und Aberkennung des internationalen Schutzes (ABl. EU L 180 S. 60)

14 Erwägungsgrund 52

Die Verarbeitung personenbezogener Daten in den Mitgliedstaaten gemäß dieser Richtlinie erfolgt nach Maßgabe der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

4. Bundesdatenschutzgesetz BDSG (eigeführt durch Art. 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU vom 30.06.2017, BGBl. I S. 2097)

15 § 43 Abs. 3 BDSG
Bußgeldvorschriften

…

(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.

III.

16 Nach Erwägungsgrund 52 der Richtlinie 2013/32/EU erfolgt die Verarbeitung personenbezogener Daten bei Asylverfahren in den Mitgliedstaaten gemäß dieser Richtlinie nach Maßgabe der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Die Richtlinie 95/46/EG wurde mit Wirkung vom 25.05.2018 aufgehoben, Art. 94 Abs. 1 DS-GVO. Jedoch gelten Verweise auf die aufgehobene Richtlinie 95/46/EG als Verweise auf die vorliegende DS-GVO, Art. 94 Abs. 1 DS-GVO. Mithin findet die DS-GVO auf Verfahren für die Zuerkennung des internationalen Schutzes vollständig Anwendung.

17 Bereits die Richtlinie 95/46/EG sah eine Dokumentation von automatisierten Verarbeitungen vor, die sog. Meldung, Art. 18 Richtlinie 95/46/EG. Der Inhalt der Meldung nach Art. 19 Richtlinie 95/46/EG entsprach im Wesentlichen dem nunmehrigen Art. 30 DS-GVO, wobei sich die neue Norm auf alle Formen der Verarbeitung, also auch auf Dateisysteme, bezieht.

18 Unter der Geltung der Richtlinie 95/46/EG verfügte die Beklagte nur über ein sehr rudimentäres Verarbeitungsverzeichnis als Meldung im Sinne der Richtlinie 95/46/EG (§ 4e BDSG alt) bezüglich der elektronischen MARIS-Akte. Besondere Regelungen zu dem Umgang von besonderen Kategorien personenbezogener Daten nach Art. 9 DS-GVO (Art. 8 Richtlinie 95/46/EG) enthielt das damalige Verarbeitungsverzeichnis (die Meldung) nicht. Solche besonderen Regelungen zu dem Umgang mit Daten nach Art. 9 und Art. 10 DS-GVO dürften auch bis heute nicht vorliegen. Denn Gesundheitsdaten, wie auch Religionsdaten werden ebenso wie strafrechtliche Verurteilungen, als sog. „normale Unterlagen“ allgemein in die elektronische MARIS-Akte aufgenommen. Ein besonderer Schutz der Datensicherheit ist nicht erkennbar, außer dass es wohl eine Zugriffsprotokollierung gibt. Allerdings kann die Akte eines Asylbewerbers von jedem Außenstandort der Beklagten in ganz Deutschland ebenso eingesehen werden, wie von der Zentrale selbst.

19 Gerade im Hinblick auf die Aktenführung und die Vorlage der Akten bei Gericht hegt das Gericht erhebliche Zweifel daran, dass die Beklagte die Vorgaben von Art. 5 Abs. 1 DS-GVO i.V.m. z.B. Art. 26 und 30 DS-GVO einhält. Entgegen der Auflage des Gerichts wurde das Verzeichnis der Verarbeitungstätigkeiten nicht vorgelegt. Es ist insoweit beabsichtigt, den Behördenleiter der verantwortlichen Stelle, also der Beklagten, im Hinblick auf seine Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO nach der Entscheidung des EuGH anzuhören.

20 Vor einer Anhörung muss aber geklärt werden, ob das Unterlassen von Verpflichtungen nach der DS-GVO und eine damit einhergehende Rechtswidrigkeit der Datenverarbeitung zu einer Sanktion, wie dem Löschen der Daten nach Art. 17 Abs. 1 lit. d) DS-GVO oder einer Einschränkung der Verarbeitung nach Art. 18 Abs. 1 lit. b) DS-

GVO führt. Dies zumindest dann, wenn die betroffene Person, hier der Kläger, dies verlangt. Denn andernfalls wäre das Gericht gezwungen, sich im Rahmen des gerichtlichen Verfahrens an einer rechtswidrigen Datenverarbeitung zu beteiligen. Die Behörde könnte ständig sanktionslos gegen die DS-GVO verstoßen.

21 In einem solchen Fall könnte nur die Aufsichtsbehörde nach Art. 58 DS-GVO tätig werden. Ein Erlass eines Bußgeldes gegen die Behörde käme jedoch nach dem nationalen Recht nicht in Betracht. Gemäß § 43 Abs. 3 BDSG - beruhend auf Art. 83 Abs. 7 DS-GVO - werden gegen Behörden und sonstige öffentliche Stellen keine Geldbußen verhängt. Es gäbe keinen Anreiz für die Behörde, sich rechtmäßig zu verhalten. Dies mit der Folge, dass die Vorgaben der RL 2013/32/EU ebenso wenig eingehalten würden, wie die DS-GVO selbst.

22 Der EuGH hat bereits entschieden, dass zum Zeitpunkt der Verarbeitung die „Meldung“ (heute das Verzeichnis der Verarbeitungstätigkeiten) vollständig vorliegen muss, jedoch nicht früher (Rechtssachen C‑92/09 und C‑93/09, Urteil vom 09.11.2011, ECLI:EU:C:2010:662, Rn. 95 ff.). Vorliegend erfolgt die Datenverarbeitung der personenbezogenen Daten des Klägers bereits seit dem Datum der Asylantragstellung am 07.05.2019 durch die Beklagte. Damit müsste zumindest nach der Rechtsprechung des EuGH zum Zeitpunkt der Verarbeitung – also zum Zeitpunkt der Asylantragsstellung des Klägers - ein Verzeichnis der Verarbeitungstätigkeiten bezüglich der MARIS-Akte (und damit für Asylakte des Klägers) vollständig vorliegen, was aber nicht der Fall ist.

23 Was in diesem Fall gilt, hat der EuGH bisher weder nach der Richtlinie 95/46/EG, noch nach der DS-GVO entschieden. Stellt man darauf ab, dass zum Nachweis der Einhaltung der DS-GVO der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen soll (Erwägungsgrund 82 DS-GVO) stellt sich die Frage, welche Konsequenz sich aus dem Unterlassen der verantwortlichen Stelle ergibt. Denn dann kann der Rechenschaftspflicht nach Art. 5 DS-GVO nicht nachgekommen werden.

24 Zwar regelt Art. 83 Abs. 5 lit. a) DS-GVO, dass ein Verstoß gegen die Rechenschaftspflicht nach Art. 5 DS-GVO mit Geldbußen von bis zu 20 000 000 EUR geahndet werden kann. Dies findet aber - wie bereits ausgeführt - auf Bundesbehörden nach § 43 Abs. 3 BSDG, keine Anwendung. Allerdings regelt Art. 17 Abs. 1 lit. d) DS-GVO, dass unrechtmäßig verarbeitete Daten zumindest auf Verlangen der betroffenen Person zu löschen sind.

25 Das fehlende bzw. unvollständige Verzeichnis der Verarbeitungstätigkeiten führt zumindest im Lichte von Art. 5 DS-GVO zur Überzeugung des vorlegenden Gerichts zu einer „formellen“ Rechtswidrigkeit der Datenverarbeitung. Es stellt sich daher die Frage, ob in einem solchen Fall als Sanktionswirkung für ein Unterlassen nach Art. 5 DS-GVO i.V.m. Art. 30 DS-GVO nicht eine Löschung oder wenigstens Sperrung der Daten zu erfolgen hat. Denn andernfalls könnte, mangels einer möglichen Sanktion, eine wirksame Durchsetzung der DS-GVO nicht erfolgen.

26 Immerhin hatte - soweit bekannt - z.B. die Republik Frankreich unter der Geltung von Art. 18 ff. Richtlinie 95/46/EG im nationalen Recht geregelt, dass bei gerichtlichen Verfahren ein striktes gesetzliches Verwendungsverbot bezüglich derer personenbezogen Daten besteht, die nicht durch eine Meldung von der verantwortlichen Stelle an die Aufsichtsbehörde (CNIL) erfasst worden waren, da die Nutzung der Daten mangels Dokumentation rechtswidrig war. Damit erfolgte hier schon zumindest eine Sanktion dadurch, dass die Daten von dem Gericht nicht verarbeitet und verwendet werden durften. Unter der Geltung der DS-GVO soll auch in Portugal und bei anderen Mitgliedsstaaten das fehlende Verzeichnis der Verarbeitungstätigkeiten zu einem Verwertungsverbot führen. Ein Mechanismus, den es in der Bundesrepublik Deutschland im Rahmen der Umsetzung der Richtlinie 95/46/EU und auch unter der Geltung der DS-GVO nicht gibt. Hier wurde vielmehr der Grundstein für eine „Duldung“ der fehlenden Meldung gelegt.

27 Auch die elektronische Übermittlung der Akte und der Schriftsätze des Beklagte ist eine Datenverarbeitung i.S.v. Art. 4 Nr. 2 DS-GVO, welche die Grundsätze der Datenverarbeitung nach Art. 5 DS-GVO zu beachten hat. Daher ergeben sich auch hier Zweifel an einer formellen Rechtmäßigkeit der Datenverarbeitung durch übermitteln,

als für den Übertragungsweg der sogenannten elektronischen Bundesamtsakte, wie auch den Schriftsätzen der Beklagten. Auch hier fehlt es an einem Verzeichnis der Verarbeitungstätigkeiten und einer Regelung über die gemeinsame Verantwortlichkeit. Zwar existiert eine Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach vom 24.11.2017 (BGBl. I S. 3803, geändert durch Artikel 6 des Gesetzes vom 05.10.2021, BGBl. I S. 4607). Sie regelt die Übermittlung elektronischer Dokumente an die Gerichte der Länder und des Bundes. Dabei können die obersten Behörden des Bundes oder der Landesregierungen für ihren Bereich bei öffentlich-rechtlichen Stellen die Identität der Behörden oder juristischen Personen des öffentlichen Rechts prüfen, um diese zum Besonderen elektronischen Behördenpostfach (sog. BeBPo) zuzulassen. Die obersten Behörden des Bundes oder mehrere Landesregierungen können auch eine öffentlich-rechtliche Stelle gemeinsam für ihre Bereiche bestimmen. Wer dies tatsächlich ist, wurde nicht geregelt. Letztendlich steht dahinter wohl die sogenannte Bund-Länder-Arbeitsgruppe der Justizministerien (Bund-Länder-Kommission für Informationstechnik in der Justiz (BLK) Arbeitsgruppe IT-Standards in der Justiz). Welche Behörde oder Behörden für den Verzeichnisdienst des EGVP oder des BeBPos oder gar der notwendigen Serverstruktur verantwortlich zeichnet, ist nicht bekannt und nicht dokumentiert.

28 Auch sind keine entsprechenden gesetzlichen oder sonstigen schriftlichen Regelungen zwischen den Gerichten und Behörden, wie diese nach Art. 26 DS-GVO erforderlich wären, um die Verantwortlichkeiten zu regeln, vorhanden. Selbst in Bundesländern, die nach ihrer Rechtsverordnung das Modell des gemeinsamen Verfahrens gewählt haben (z.B. Hessen, VO über den elektronischen Rechtsverkehr bei hessischen Gerichten und Staatsanwaltschaften v. 26.10.2007 GVBl. I 699), fehlt es an einer entsprechenden datenschutzkonformen Umsetzung. In Hessen wird sogar in der VO geregelt, dass der elektronische Briefkasten ausschließlich auf den Servern des „Rechenzentrums“ der Justiz, also bei der Hessischen Zentrale für Datenverarbeitung (HZD) geführt wird. Dabei ist die HZD gerade nicht Teil der Justiz und allenfalls als Intermediär ein Auftragsverarbeiter nach Art. 28 DS-GVO.

29 Bekannt ist nur, dass faktisch das Landesamt für Datensicherheit in Nordrhein-Westfalen als „Intermediär“ für die Administration und den Betreib des zentralen, länderübergreifenden Registerserver S.A.F.E. zuständig sein soll. Derzeit stehen folgende Registrierungsclients zur Verfügung: EGVP-Client zur Anlage eines Postfaches für die OSCI-Kommunikation, Registrierungsclient ZTR für die Registrierung zur Nutzung des Zentralen Testamentsregisters der Bundesnotarkammer, Registrierungsclient Zentrales Vollstreckungsportal für die Registrierung zur Nutzung des Zentralen Vollstreckungsportals. Die SAFE-ID soll unveränderbar sein und nur einmal vergeben werden (s. dazu SAFE – http://www.egvp.de/Drittprodukte/SAFE_Abbildungsvorschrift _SAFE_ID_Stand_Dez_2014.pdf). Daneben gibt es noch den Begriff der Govello-ID. Postfächer im EGVP werden durch eine eindeutige Identifikationsnummer (Govello-ID) bezeichnet. Die Govello-ID ist aus der Kennung „safe-sp1“ oder „govello“ sowie zweier Zahlenfolgen zusammengesetzt. Diese IDs sollen in einem Verzeichnisdienst registriert sein, der wohl von Nordrhein-Westfalen (IT-NRW) gepflegt wird. Wer tatsächlich für die Vergabe der Govello-ID im Bund-Länder-Verbund verantwortlich zeichnet, ist nicht geregelt.

30 Auf welcher datenschutzrechtlichen Basis das EGVP erfolgt, ist nicht bekannt. Bezüglich der Anfrage nach einer Vereinbarung nach Art. 26 DS-GVO hat sich die Beklagte geweigert, sich hierzu zu erklären und diese vorzulegen. Es ist insoweit auch fraglich, ob über das sogenannte besondere elektronische Behördenpostfach mangels der Bestimmung von Verantwortlichkeiten nach Art. 26 DS-GVO eine rechtmäßige Übermittlung erfolgen kann. Dies auch im Hinblick auf die Datensicherheit, da keines der Dokumente auf dem Übertragungsweg verschlüsselt ist.

31 So wird behauptet, dass das positive Recht es zurzeit nicht erfordere, dass das besondere elektronische Anwaltspostfach mit einer Ende-zu-Ende-Verschlüsselung zu konzipieren und zu betreiben ist (Anwaltsgerichtshof Berlin, Urteil vom 14.11.2019 – I AGH 6/18 –, Rn. 14 nach juris). Dafür, dass eine geforderte Ende-zu-Ende-Verschlüsselung dem Stand der Technik entspräche und diese deshalb von der Bundesrechtsanwaltskammer verwendet werden müsste, bestünden keine Anhaltspunkte

(Anwaltsgerichtshof Berlin, Urteil vom 14. November 2019 – I AGH 6/18 –, Rn. 83nach juris). Solche werden auch nicht vorgegeben (BGH, Urteil vom 22.03.2021 – AnwZ (Brfg) 2/20 –, BGHZ 229, 172-213, Rn 88). Zumindest in Hessen besteht zwischen dem Intermediär, der HZD, und dem jeweiligen Gericht - also auch dem Verwaltungsgericht Wiesbaden - keine Verschlüsselung der zu übermittelnden Nachrichten.

32 Hierauf kommt es vorliegend aber nicht an, denn das Verfahren entspricht einem Mailverfahren. Zu dem internetbasierten Gmail-Dienst hat der EuGH entscheiden, dass es sich um keinen Kommunikationsdienst handelt, da der Dienst keinen Internetzugang vermittele, der nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehe und daher kein „elektronischer Kommunikationsdienst“ ist (Urteil vom 13.06.2019, C‑193/18, ECLI:EU:C:2019:498). Damit handelt es sich bei dem EGVP um keinen Dienst, der unter die Richtlinie 2002/58/EG fällt (Art. 2 Abs. 4 DS-GVO). Mithin gilt die DS-GVO mit Folge, dass das EGVP und die angeschlossenen Verfahren in einem Verzeichnis der Verarbeitungstätigkeiten zu erfassen sind und die jeweilige Verantwortlichkeit als Verfahren mit vielen Verantwortlichen nach Art. 26 DS-GVO vereinbart werden muss. An beiden fehlt es vorliegend. Damit bestehen Zweifel an der Rechtmäßigkeit der Datenübermittlung.

33 Bei dem EGVP handelt es sich um ein Verfahren der Justizverwaltungen, die der zweiten Gewalt, der Exekutive, zuzuordnen sind und der Beklagten, die ebenfalls Teil der ausführenden Gewalt ist. Damit hat die Beklagte zur Überzeugung des Gerichts dafür zu sorgen, dass das elektronische Verfahren zur Datenübermittlung von Schriftsätzen und Akten im Einklang mit der DS-GVO steht.

34 Für das Gericht stellt sich im Rahmen der justiziellen Tätigkeit daher die Frage, wie mit den über das EGVP-System über das sogenannte Behördenpostfach gelieferten Daten umzugehen ist, wenn das Verfahren des EGVP und die damit verbundene Datenverarbeitung als solche nicht der DS-GVO entspricht.

35 Zumindest das Gericht hat die DS-GVO im Rahmen der justiziellen Tätigkeit zu beachten und zu befolgen. Dabei hat der EuGH in dem Urteil vom 09.07. 2020 (C-272/19 –, Rn 42 ff.; ECLI:EU:C:2020:535) ausdrücklich klargestellt, dass sich die Unabhängigkeit des nationalen Richters nur auf die persönliche Unabhängigkeit beschränke (Rn. 49) und nicht die Institution des Gerichtes als Ganzes einbezieht. Mithin die justizielle Tätigkeit nur im Rahmen der persönlichen Unabhängigkeit erfolgt.

36 Damit hat das vorlegende Gericht keinen Einfluss auf eine Rechtmäßigkeit der Datenverarbeitung der Justizverwaltung, da diese außerhalb der „Justiziellen Tätigkeit“ bei der zweiten Gewalt, der Exekutive, liegt. Das Gericht hat aber Europarecht zu beachten und einzuhalten. Wenn Verfahrensbeteiligte dagegen verstoßen, dürfte eine gerichtliche Datennutzung wohl nicht zulässig sein, da sich das Gericht ansonsten an einer rechtwidrigen Datenverarbeitung beteiligt. Im vorliegenden Fall kommt hierbei verschärfend hinzu, dass die Beklagte angesichts des bisherigen Schriftverkehrs wohl (bewusst) gegen europarechtliche Vorgaben verstößt.

37 Es liegt auch kein Fall vor, der eine gerichtliche Nutzung über Art. 17 Abs. 3 lit. e) DS-GVO zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen durch die Beklagte rechtfertigen würde. Zwar dienen die Daten dem Beklagten zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, Art. 17 Abs. 3 lit. b) DS-GVO. Damit wäre aber zugleich ein datenschutzrechtswidriges Tun auf Dauer legalisiert.

38 Mithin sind die vorgelegten Fragen von besonderer Bedeutung, wenn es um die Umsetzung der DS-GVO im gerichtlichen Verfahren geht. Das Ziel nach Art. 1 Abs. 2 DS-GVO, die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten zu fördern, würde konterkariert.

39 Insoweit dürfte es wenigstens für den Fall, dass die Frage 1 verneint wird, der Disposition der betroffenen Person oder besser der ausdrücklichen Zustimmung der betroffenen Person - hier des Klägers - bedürfen, dass seine Daten trotz formeller rechtswidriger Verarbeitung im gerichtlichen Verfahren genutzt werden dürfen.

40 Dies hätte allerdings auch zur Folge, dass im Falle einer Verweigerung die bei dem Beklagten verarbeiteten Daten, die diese in Form der sogenannten elektronischen MARIS-Behördenakte vorlegt, von dem Gericht nicht verarbeitet (verwendet) werden dürften. Dies hätte weiter zur Folge, dass eine Entscheidungsgrundlage bis zur Nachholung der Dokumentationspflichten nicht mehr bestünde. Der Ausgangsbescheid des Beklagten müsste immer aufgehoben werden. Eine Entscheidung über den geltend gemachten Asyl-Status wäre bis zur Nachholung der Dokumentationspflichten nicht möglich.

IV.

41 Der Beschluss ist unanfechtbar.