GEULEN & KLINGER
Rechtsanwälte

Dr. Reiner Geulen
Prof. Dr. Remo Klinger
Dr. Caroline Douhaire LL.M.

10719 Berlin, Schaperstraße 15
Telefon +49/ 30 / 88 47 28-0
Telefax +49/ 30 / 88 47 28-10
E-Mail geulen@geulen.com
klinger@geulen.com
douhaire@geulen.com

www.geulenklinger.com

Per E-curia
Gerichtshof der Europäischen Union
Kanzlei

L-2925 LUXEMBURG

26. August 2020

Stellungnahme zu den
verbundenen Ersuchen um Vorabentscheidung C-148/20 bis C-150/20
Deutsche Lufthansa u.a.
(Vorlegendes Gericht: Amtsgericht Köln – Deutschland)

Für die Klägerinnen erklären wir zu den Ersuchen um Vorabentscheidung Folgendes:

A. Einleitung

1. Die Klägerinnen richten sich gegen die Übermittlung von Passenger Name Records (im Folgenden: „**PNR**“) durch die beklagte Luftverkehrsgesellschaft an die deutsche Fluggastdatenzentralstelle. Bei PNR handelt es sich um alle erdenklichen Daten und Vorgänge rund um eine Flugbuchung. Sie können Kontaktdaten, Gepäckangaben, Daten zu Begleitpersonen, Zahlungsinformationen und über ein Freitextfeld sogar nicht näher bestimmte Daten enthalten.

2. Die Übermittlung der PNR-Daten stützt sich auf das Fluggastdatengesetz vom 6. Juni 2017 (BGBl. I 1484; im Folgenden: „**FlugDaG**“). Mit dem FlugDaG setzte Deutschland die Richtlinie (EU) 2016/681 vom 27. April 2016 (im Folgenden: „**PNR-Richtlinie**“) um. Das FlugDaG verpflichtet die Fluggesellschaften einerseits zur Übermittlung von PNR-Daten zu Flügen aus Nicht-EU-Staaten nach Deutschland und von Deutschland in Nicht-EU-Staaten; insoweit erfüllt das FlugDaG zwingende Vorgaben der PNR-Richtlinie. Die Ausgangsverfahren zu den Rs. C-148/20

und Rs. C-150/20 betreffen derartige Flüge in bzw. aus Nicht-EU-Staaten. Das FlugDaG erfasst aber auch Flüge aus EU-Staaten nach Deutschland und umgekehrt; insoweit stützt sich das FlugDaG auf die Öffnungsklausel des Art. 2 PNR-Richtlinie. In diese Kategorie fällt das Ausgangsverfahren zur Rs. C-149/20.

3. Das vorlegende Gericht fragt, ob die PNR-Richtlinie mit Art. 7 und 8 GRCh vereinbar ist. Die Vorabentscheidungsverfahren geben dem Gerichtshof Gelegenheit, seine Ausführungen im Gutachten 1/15 vom 26. Juli 2017 (ECLI:EU:C:2017:592; im Folgenden: „**Gutachten 1/15**“) zu bekräftigen und zu ergänzen. Der Gerichtshof hat im Gutachten 1/15 bereits dargelegt, dass personenbezogene Daten nicht ohne Anlass massenhaft verarbeitet werden dürfen. Die PNR-Richtlinie lässt dies gleichwohl zu. Dies hat auch deshalb eine große Tragweite, weil bereits erwogen wird, die PNR-Richtlinie deutlich auszudehnen und auf die Datensätze der Passagiere von grenzüberschreitenden Zügen, Bussen und Fähren zu erstrecken (Ratsdokument vom 6. November 2019 – 12649/1/19 REV 1).

4. Gegenüber dem Gutachten 1/15 neu zu entscheiden sein wird, unter welchen Bedingungen die Mitgliedstaaten Algorithmen bei der Verhütung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität einsetzen dürfen. Denn die wesentlichste Neuerung der PNR-Richtlinie gegenüber der bisherigen Rechtslage – und der Grund für die Verarbeitung einer Vielzahl von ansonsten unnötigen Datenpunkten (Gepäck, Sitzplatz usw.) – ist der Abgleich der erhobenen Daten mit im Voraus festgelegten Kriterien (Art. 6 Abs. 3 lit. b, Abs. 4 PNR-Richtlinie). Die rechtliche Bewertung dieser Frage hat erhebliche Bedeutung für unsere Zukunft. Denn es ist zu erwarten, dass die Mitgliedstaaten künftig auch jenseits vom Flugverkehr Algorithmen in der Strafverfolgung und bei der Gefahrenabwehr einsetzen werden. Der Abgleich mit im Voraus festgelegten Kriterien rüttelt an den Grundfesten des Menschenbildes, das der GRCh zugrunde liegt. Denn mit dem Datenabgleich soll die Gefährlichkeit von Menschen anhand von alltäglichen Daten, die keinen Bezug zu einer konkreten Straftat haben, beurteilt werden. Die davon betroffenen Menschen werden allein durch algorithmische Berechnungen als potentielle Gefahrenquelle behandelt. Dies verletzt die grundsätzliche Gewährleistung des Art. 1 Satz 1 GRCh.

5. Der Gerichtshof wird schließlich klären können, ob – falls er die Ungültigkeit der PNR-Richtlinie feststellt – die nationalen Umsetzungsgesetze gleichwohl am Unionsrecht zu messen sind und das FlugDaG nicht weiter angewendet werden darf.

B. Rechtlicher Rahmen

6. Vor Inkrafttreten der PNR-Richtlinie regelte die Richtlinie 2004/82/EG vom 29. April 2004 (im Folgenden „**API-Richtlinie**“) die Verarbeitung von Fluggastdaten. Hiernach waren Grenzkontrollbehörden verpflichtet, auf Ersuchen eines Mitgliedstaats bei Flügen in das Gebiet der Europäischen Union im Einzelfall Fluggastdaten zur Verfügung zu stellen. Auf Grundlage der nationalen Umsetzungsgesetze war es dadurch bereits möglich, bestimmte Flugstrecken gezielt zu überprüfen. Der Abgleich von Fluggastdaten mit Fahndungsdatenbanken war ebenfalls möglich. Die an die Behörden übermittelten Daten waren im Allgemeinen 24 Stunden nach der Einreise zu löschen. Eine von der EU-Kommission im Jahre 2011 vorgeschlagene Ausweitung der Befugnisse lehnte der Ausschuss des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres im Jahre 2013 wegen rechtsstaatlicher Bedenken ab (Ausschussbericht vom 29. April 2013, A7-0150/2013). Nach dem Terroranschlag in Paris im November 2015 kehrte der Vorschlag in Form der PNR-Richtlinie zurück.

7. Die PNR-Richtlinie und das FlugDaG sollen der Verhinderung und Verfolgung von Terrorismus und schwerer Kriminalität dienen. Es geht dabei nicht um Gefahren für den Flugverkehr selbst. Der Anwendungsbereich der PNR-Richtlinie ist auch nicht auf grenzübergreifende schwere Kriminalität beschränkt, wie etwa noch das Fluggastdaten-Abkommen zwischen der EU und Kanada (im Folgenden das „**EU-Kanada-Abkommen**“; dazu unten Absatz Nr. 11 f.). Vielmehr ist eine lange Reihe an Straftaten erfasst (vgl. Anhang II der PNR-Richtlinie), die nicht mit Flugreisen bzw. dem grenzübergreifenden Verkehr zusammenhängen.

8. Das FlugDaG setzt die Vorgaben der PNR-Richtlinie, die das vorlegende Gericht zutreffend dargestellt hat, wie folgt um: Die von der Luftverkehrsgesellschaft zu übermittelnden PNR-Daten enthalten neben Namen (§ 2 Abs. 2 Nr. 1 FlugDaG), Buchungscode (Nr. 2) und Staatsangehörigkeit (Nr. 8) auch so sensible Daten wie Geburtsdatum (ebenfalls Nr. 8), Anschrift, Telefonnummer, E-Mail-Adresse (alle drei Nr. 5) und Zahlungsinformationen (Nr. 10) sowie Angaben zu Begleitpersonen (Nr. 19), zum Gepäck (Nr. 7), „Angaben zum Vielfliegereintrag“ (Nr. 12) und – in einem Freitextfeld – „allgemeine Hinweise, einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen ...“ (Nr. 16). Diese Daten gleicht das Bundeskriminalamt (im Folgenden: „**BKA**“) einerseits mit Datenbanken ab, die der

Fahndung oder Ausschreibung von Personen oder Sachen dienen (§ 4 Abs. 2 Nr. 1 FlugDaG). Andererseits kann das BKA darauf sog. „Muster“ anwenden, mit denen es neue Verdachtsmomente gegen ihm bislang unbekannte Einzelpersonen gewinnen will (§ 4 Abs. 2 Nr. 2 FlugDaG). Die Muster entsprechen den im Voraus festgelegten Kriterien nach Art. 6 Abs. 3 lit. b PNR-Richtlinie. Die Muster sollen auf empirischer, kriminalistischer Erfahrung basieren, also die Reisemuster bekannter Straftäter widerspiegeln. Außerdem kann das BKA im Einzelfall auf ein Ersuchen einer Behörde bestimmte Daten übermitteln (§ 4 Abs. 5 Satz 1 FlugDaG). Zweck der Datenverarbeitung ist es, Personen zu identifizieren, die eine der angeführten Straftaten begangen haben oder innerhalb eines übersehbaren Zeitraums begehen werden (§ 4 Abs. 1 FlugDaG). Alle Daten bleiben fünf Jahre lang gespeichert (§ 13 Abs. 1 Satz 1 FlugDaG). Zwar werden die Daten nach sechs Monaten depersonalisiert (§ 5 Abs. 1 FlugDaG). Allerdings kann die Depersonalisierung umgekehrt werden, wenn ein Ersuchen nach § 4 Abs. 5 FlugDaG es erfordert (§ 5 Abs. 2 FlugDaG).

9. Das BKA leitet bei Treffern die Datensätze und Verarbeitungsergebnisse zur Einleitung weiterer Maßnahmen an die Sicherheitsbehörden weiter (§ 6 Abs. 1 und 2 FlugDaG). Das BKA kann ferner unter den Voraussetzungen des § 7 Abs. 3 FlugDaG die Daten an die PNR-Zentralstellen anderer Mitgliedstaaten übermitteln sowie nach § 10 Abs. 1 FlugDaG an die Behörden von Drittstaaten. Voraussetzung für die Übermittlung an Drittstaaten ist in der Regel ein Angemessenheitsbeschluss nach Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 (im Folgenden: „**JI-Richtlinie**“), vgl. § 78 Abs. 1 des Bundesdatenschutzgesetzes in der Fassung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 30. Juni 2017 (BGBl. I, 2097; im Folgenden: „**BDSG**“). PNR-Daten können jedoch nach § 80 BDSG auch ohne Angemessenheitsbeschluss oder Garantien an Drittstaaten übermittelt werden, wie es Art. 38 JI-Richtlinie vorsieht.

10. Die Verarbeitung von PNR-Daten greift in das Recht auf Achtung des Privatlebens (Art. 7 GRCh) und in das Recht auf Schutz der personenbezogenen Daten (Art. 8 GRCh) ein. Der Gerichtshof hat den Schutz der Privatsphäre durch Art. 7 und 8 GRCh in mehreren Entscheidungen konkretisiert. Für die vorgelegten Fragen von besonderer Bedeutung sind seine Urteile vom 8. April 2014, Digital Rights Ireland u.a. - C-293/12 und C-594/12 (ECLI:EU:C:2014:238; im Folgenden: „**DRI**“) –,

sowie vom 21. Dezember 2016, Tele2 Sverige und Watson u.a. - C-203/15 und C-698/15 (ECLI:EU:C:2016:970). In beiden Fällen führte er aus, dass der persönliche Anwendungsbereich der dort gegenständlichen Vorratsspeicherung von Telekommunikationsverkehrsdaten (im Folgenden: „**VDS**“) zu weit war, weil sämtliche Personen betroffen waren, also auch solche, bei denen keinerlei Anhaltspunkt dafür bestand, dass ihr Verhalten in einem auch nur mittelbaren Zusammenhang mit schweren Straftaten stehen könnte (Rn. 56-58 in DRI); dass der sachliche Anwendungsbereich der VDS zu weit war, weil sie anlasslos erfolgte (Rn. 59 in DRI); dass eine unabhängige Kontrolle nicht gewährleistet war (Rn. 62 in DRI); und dass die Speicherfristen nicht hätten unterschiedslos gelten dürfen (Rn. 63 f. in DRI).

11. Zudem hat der Gerichtshof in seinem Gutachten 1/15 zum EU-Kanada-Abkommen speziell zur Verarbeitung von PNR-Daten Stellung genommen. Das Europäische Parlament hatte dem Gerichtshof die Frage vorgelegt, ob die im EU-Kanada-Abkommen vorgesehene Verarbeitung und Übermittlung von PNR-Daten mit den Art. 7, 8 und 52 Abs. 1 GRCh vereinbar ist.

12. Der Gerichtshof führte aus, dass
    - u.a. folgende der vorgesehenen Datenkategorien nicht bestimmt genug formuliert waren:
        - Rubrik 5 („Verfügbare Vielflieger- und Bonus-Daten [Gratisflugscheine, Upgrades usw.]“), weil der Begriff „usw.“ zu unbestimmt sei und weil unklar bleibe, ob mit der Formulierung Informationen allein über die Teilnahme der Fluggäste an Bonusprogrammen gemeint sind oder sämtliche Informationen über die Flüge und Buchungen, die im Rahmen solcher Programme durchgeführt werden (Rn. 157 in Gutachten 1/15).
        - Rubrik 17 („[a]llgemeine Eintragungen einschließlich OSI- (Other Supplementary Information), SSI- (Special Service Information) und SSR-Informationen (Special Service Request)“), weil es sich dabei um ein Freitextfeld handele. Eine solche Rubrik enthalte keine Angaben über Art und Umfang der zu übermittelnden Informationen und könne selbst Informationen umfassen, die keinerlei Bezug zum Zweck der Übermittlung der PNR-Daten haben. Da die in dieser Rubrik genannten Informationen lediglich beispielhaft genannt würden, wie aus der Verwendung des Wortes „einschließlich“ hervorgehe, begrenze sie nicht Art und Umfang der Informationen, die von ihr erfasst werden können (Rn. 160).

- die zur automatisierten Verarbeitung von PNR-Daten verwendeten Modelle und Kriterien spezifisch und zuverlässig sein müssten, das heißt die „Identifizierung von Personen ermöglichen, gegen die ein begründeter Verdacht der Beteiligung an terroristischen Straftaten oder grenzübergreifender schwerer Kriminalität bestehen könnte“ (Rn. 172);
- die durch automatisierte Datenverarbeitung erzielten Resultate vor nachteiligen Auswirkungen auf die betreffenden Fluggäste individuell überprüft werden müssten, weil Nachteile nicht allein auf dieser Grundlage getroffen werden dürften (Rn. 173);
- die Verwendung der PNR-Daten grundsätzlich einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterliegen müsste (Rn. 202);
- die dauerhafte Speicherung der PNR-Daten von Fluggästen nach ihrer Ausreise aus Kanada nur für Personen in Betracht kommen durfte, bei denen objektive Anhaltspunkte dafür bestehen, dass von ihnen eine Gefahr im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität ausgehen könnte (Rn. 204 ff.);
- eine Weitergabe personenbezogener Daten in Drittländer erfordere, dass ein Beschluss der Kommission gemäß Art. 25 Abs. 6 der Richtlinie (EU) 95/46 (jetzt: Art. 36 JI-Richtlinie) gefasst worden ist, wonach das Drittland ein angemessenes Schutzniveau für die Daten gewährleistet;
- eine – nachträgliche – individuelle Information der Fluggäste erforderlich ist, wenn objektive Anhaltspunkte vorliegen, die eine Verwendung der PNR-Daten über die systematischen/automatisierten Prüfungen hinaus rechtfertigen (Rn. 223).

13. Für die Ausgangsverfahren ist zudem von Bedeutung, dass Art. 2 Abs. 1 JI-Richtlinie auf die Verarbeitung personenbezogener Daten durch die zuständigen (nationalen) Behörden zu den in Art. 1 Abs. 1 JI-Richtlinie genannten Zwecken anwendbar ist. Zu diesen Zwecken gehören die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, die Strafvollstreckung sowie der Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit. Die Verarbeitung von Fluggastdaten dient nach § 1 Abs. 2 FlugDaG der Verhütung und Verfolgung von terroristischen Straften und schwerer Kriminalität. Damit fällt die vom FlugDaG erlaubte Verarbeitung von Fluggastdaten in den Anwendungsbereich der JI-Richtlinie, sofern die PNR-Richtlinie ungültig sein sollte. Die Datenverarbeitung nach

dem FlugDaG hätte sich in diesem Fall an der JI-Richtlinie sowie den Art. 7 und 8 GRCh und der zugehörigen Rechtsprechung des Gerichtshofs (vgl. Erwägungsgrund 46 der JI-Richtlinie) zu messen.

C. Sachverhalt und Vorabentscheidungsersuchen

14. Die Verarbeitung von PNR-Datensätzen betrifft eine große Zahl an Menschen. Für Deutschland hat das Statistische Bundesamt ermittelt, dass im Jahr 2019 über 100 Millionen Passagiere von Deutschland ins Ausland geflogen sind; dabei sind die Flüge von kleinen Flughäfen ebenso wenig erfasst wie die Passagiere, die vom Ausland nach Deutschland flogen (vgl. Pressemitteilung vom 18. Februar 2020, beigefügt als Anlage 1). Das Bundesverwaltungsamt rechnete für Deutschland mit jährlich rund 170 Mio. Fluggästen, für die 340 Millionen Datensätze anfallen würden. (vgl. die Gesetzesbegründung für das FlugDaG, Auszug beigefügt als Anlage 2).

15. Der Umfang der PNR-Daten (vgl. Anhang I der PNR-Richtlinie) lässt umfassende Rückschlüsse auf das Privat- und das Geschäftsleben der Betroffenen zu, nämlich wer wann wohin gereist ist, in wessen Begleitung, welches Zahlungsmittel sie genutzt haben, welche Kontaktdaten sie angegeben haben oder ob sie mit leichtem oder schwerem Gepäck gereist sind. Über das Freitextfeld können auch diverse weitere Daten anfallen, deren Inhalt unklar ist. So können – insbesondere bei Vielfliegern, aber nicht nur bei ihnen – detaillierte Persönlichkeitsprofile entstehen (vgl. dazu auch Gutachten 1/15, Rn. 128).

16. Die Klägerinnen haben als Parlamentsabgeordnete, prominente Aktivistin bzw. Rechtsanwältin ein besonderes Interesse an der Vertraulichkeit ihrer Reisebewegungen. Sie begehren deshalb von der Beklagten, dass sie keine PNR-Daten zu Flügen der Klägerinnen an die deutschen Behörden übermittelt. Deutschland ist der Beklagten als Streithelferin beigetreten. Die Klägerinnen hätten mit ihren Klagen Erfolg, wenn kein Rechtsgrund für die Übermittlung von PNR-Datensätze durch die Beklagte an deutsche Behörden besteht. Einen solchen Rechtsgrund sieht die Beklagte in den Vorschriften des FlugDaG, das wiederum auf der PNR-Richtlinie beruht. Für die Ausgangsverfahren ist erheblich, ob die PNR-Richtlinie gültig ist; Zweifel daran bestehen insbesondere im Hinblick auf die Fragen, die das vorlegende Gericht formuliert hat.

17. Für den Fall, dass der Gerichtshof die PNR-Richtlinie für ungültig hält, stellt sich die Frage nach der Vereinbarkeit des FlugDaG mit dem sonstigen Unionsrecht. Denkt man die PNR-Richtlinie weg, fällt das FlugDaG in den Anwendungsbereich der JI-Richtlinie (siehe oben Absatz Nr. 13) und damit des Unionsrechts insgesamt. Daher sollte der Gerichtshof ebenfalls klären, ob eine PNR-Datenverarbeitung nach dem FlugDaG mit den Anforderungen der JI-Richtlinie im Lichte der Art. 7 und 8 GRCh vereinbar ist. Der Gerichtshof ist dazu nach hergebrachten Rechtsgrundsätzen in diesem Verfahren befugt.

D. Rechtliche Würdigung

I. Zur Vorlagefrage 1 (Bestimmtheit)

18. Den Ausführungen des vorlegenden Gerichts zur mangelnden Unbestimmtheit von Nr. 8 und 12 des Anhangs I der PNR-Richtlinie ist lediglich hinzuzufügen, dass die entsprechenden Vorschriften des FlugDaG (§ 2 Abs. 2 Nr. 12 und 16) aus denselben Gründen wie Nr. 8 und 12 des Anhangs II der PNR-Richtlinie zu unbestimmt sind. Das ergibt sich ohne Weiteres aus den oben dargestellten Ausführungen im Gutachten 1/15 (Absatz Nr. 12).

II. Zur Vorlagefrage 2 (Umfang der Datenverarbeitung)

19. Die PNR-Richtlinie und das FlugDaG erfassen unterschiedslos alle internationalen Flüge und damit alle Menschen, die Deutschland mit dem Flugzeug erreichen oder verlassen. Sämtliche verfügbaren PNR-Daten werden bei der PNR-Zentralstelle zusammengeführt und automatisiert mit Datenbanken und im Voraus festgelegten Kriterien abgeglichen. Das ist unverhältnismäßig.

1. Tatsächliche Grundlagen der Verhältnismäßigkeitsprüfung

20. Die Kommission vermochte in ihrem Richtlinienvorschlag KOM(2011) 32 vom 2. Februar 2011 (dort S. 6) den Nutzen der PNR-Datenverarbeitung nicht zu belegen. Vielmehr gestand die Kommission im Richtlinienvorschlag ein, dass es auf EU-Ebene keine detaillierten Statistiken darüber gebe, inwieweit PNR-Daten dazu beitragen, Terrorismus oder schwere Kriminalität zu verhüten, aufzudecken, aufzuklären oder strafrechtlich zu verfolgen. Die Evaluation der PNR-Datenverarbeitung nach Art. 19 PNR-Richtlinie durch die Kommission führt zu keiner anderen

Bewertung. In ihrem Bericht vom 24. Juli 2020, COM(2020) 305 final (im Folgenden: „**Evaluationsbericht**“), bzw. dem begleitenden Commission Staff Working Document vom selben Tag, SWD(2020) 128 final (im Folgenden: „**Arbeitspapier**“), führt die Kommission zwar anekdotisch Fälle auf, in denen der Abgleich mit Datenbanken und mit im Voraus festgelegten Kriterien zur Strafverfolgung und Gefahrenabwehr beigetragen haben soll. Dass bei der Verarbeitung von mehreren Hundert Millionen PNR-Datensätzen einzelne Ermittlungserfolge zu verzeichnen sind, belegt aber weder die Notwendigkeit noch die Verhältnismäßigkeit der PNR-Richtlinie.

21. Dazu hätte die Kommission in ihrem Evaluationsbericht einerseits zeigen müssen, dass

    (1) die Ermittlungserfolge tatsächlich nur durch die Verarbeitung von PNR-Daten möglich wurden – und dass dafür nicht etwa die ggf. erweiterte Verarbeitung von API-Daten genügt hätte – und dass

    (2) Anzahl und Gewicht der Ermittlungserfolge so schwer wiegen, dass sie die anlasslose Massenüberwachung des Flugverkehrs rechtfertigen, insbesondere

    (3) mit Blick auf Ermittlungsmaßnahmen gegenüber Personen, die zu Unrecht einer Straftat verdächtigt wurden (falsch-positive Treffer).

    Der Evaluationsbericht bietet dazu keine Daten. Die Kommission schreibt zu Punkt (1) selbst, die PNR-Datenverarbeitung habe zur Identifikation von „möglichen“ Straftätern nur „beigetragen“ („*contributed*“) (Evaluationsbericht S. 7). Es sei „häufig nicht möglich“ („*often not possible*“), den Nutzen von PNR-Daten zu isolieren und zu quantifizieren. Zu Punkt (2) trägt sie lediglich Fallstudien vor, nicht aber Statistiken (Arbeitspapier, S. 29 f., 32 f.). Besonders schwer wiegt in diesem Zusammenhang aber Punkt (3), dass nämlich die Kommission – wohl auch, weil Art. 20 Abs. 2 PNR-Richtlinie keine Statistiken dazu verlangt – den Anteil von falsch-positiven Treffern weder darstellt noch in die Gesamtbeurteilung der Verhältnismäßigkeit der Maßnahme einbezieht. Für eine Gesamtbeurteilung zentral sind aber die Zahl falsch-positiver Treffer und das Gewicht der Maßnahmen, die gegen zu Unrecht Verdächtigte ergriffen wurden.

22. Auf Grundlage der Statistiken nach Art. 20 Abs. 2 PNR-Richtlinie hat die Kommission lediglich ermittelt, wie hoch der Anteil an Fluggästen ist, bei denen eine weitere Überprüfung erfolgte. Diesen Wert gab die Kommission mit 0,59 % an; in 0,11 % der Fälle hatten die Fluggastdatenzentralstellen PNR-Daten an andere

Behörden weitergeleitet (Arbeitspapier, S. 28). Diese Zahlen muten zunächst gering an; das täuscht jedoch, weil die Datenbasis so groß ist: Das PNR-Datenverarbeitungsregime erfasst unterschiedslos alle internationalen Fluggäste in der EU. Selbst wenn man von nur 100 Millionen betroffenen Fluggästen ausginge, würde das die weitere Überprüfung von 590.000 Personen bedeuten; die PNR-Daten von 110.000 Fluggästen würden an andere Behörden weitergeleitet. Die tatsächlichen Zahlen werden deutlich höher liegen; leider enthält der Evaluationsbericht keine Angaben zur Anzahl der verarbeiteten PNR-Datensätze.

23. Einen Eindruck von den zu berücksichtigenden Fehlerquoten bieten Zahlen aus dem Schriftsatz der Bundesrepublik Deutschland vom 9. September 2019 (S. 11 ff.) in einem Verfahren vor dem Verwaltungsgericht Wiesbaden (Aktenzeichen 6 K 806/19.WI; dieses Verfahren ist ebenfalls ausgesetzt und dem Gerichtshof zur Vorabentscheidung vorgelegt worden als Rs. C-222/20; Auszüge des Schriftsatzes als Anlage 3). Danach hatte das BKA bis zum 14. August 2019 insgesamt 31.617.068 PNR-Datensätze überprüft, was zu 237.643 technischen Treffern führte, von denen nach individueller Überprüfung nur 910 fachliche Treffer übrigblieben. Das entspricht einer technischen Fehlerquote von knapp 99,6 %. Die Prozessvertreter Deutschlands führten weiter aus, dass von 910 an die Bundespolizei und/oder den Zoll ausgeleiteten fachlichen Treffern in 396 Fällen Fahndungsmaßnahmen leerliefen. Unter diesen Fällen war eine nicht näher bezifferte Zahl an Fluggästen, die „nicht identisch mit der zur Fahndung ausgeschriebenen Person“ waren (Schriftsatz vom 9. September 2019, S. 14). Diese echten falschen Verdächtigungen sind folglich zur Fehlerquote hinzuzurechnen. Die falschen Verdächtigungen zeigen außerdem die negativen Nebenwirkungen des Abgleichs mit Datenbanken und lassen erahnen, zu wie vielen Falschverdächtigungen es bei Abgleichen mit im Voraus festgelegten Kriterien kommen kann.

Die Angaben widersprechen schließlich der Aussage des Arbeitspapiers auf S. 28, die individuelle Überprüfung von technischen Treffern sichere „den Ausschluss von sogenannten ‚falsch-positiven Treffern‘“ (*„... ensures the elimination of the so-called ‘false positive matches‘ ...“*). Von den 514 „erfolgreich“ durchgeführten Fahndungsmaßnahmen (910 Treffer minus 396 Leerläufe) waren 447 reine Vorfeldmaßnahmen, nämlich verdeckte Kontrollen und Aufenthaltsermittlungen, die nicht unmittelbar der Gefahrenabwehr oder Strafverfolgung dienen. Die Überprüfung von 31.617.068 PNR-Datensätzen mündete damit in nur 57 Festnahmen und 10

gezielten offenen Kontrollen, was 0,0002 % entspricht. Unklar ist, welche dieser Festnahmen berechtigt waren und was aus ihnen folgte.

24. An mehreren Stellen des Evaluationsberichts geht die Kommission hingegen davon aus, dass alle Überprüfungen gerechtfertigt und damit ein Erfolg waren (s. etwa Arbeitspapier S. 24: „In einigen Fällen führte die Nutzung von PNR-Daten zur Festnahme von Personen, die den Polizeibehörden zuvor nicht bekannt waren ..." - „*In some instances, the use of PNR data resulted in the arrest of persons previously unknown to the police services* ..."; oder Arbeitspapier S. 28: „Ein noch kleinerer Teil [der Daten von allen Fluggästen] wurde an die zuständigen Behörden übermittelt. Das bedeutet, dass die PNR-Systeme insgesamt gezielte Treffer lieferten ..." - „*An even smaller fraction of [the data of all passengers] was transmitted to competent authorities. This means that, overall, PNR systems deliver targeted results …"*).

25. Das zeigt ein Grundproblem des Evaluationsberichts. Die Kommission geht von einem „Erfolg" bereits dann aus, wenn ein „Verdächtiger" identifiziert ist, ohne dass sich der Verdacht bestätigen muss. Wer verdächtig ist, definieren die Behörden selbst durch die Aufnahme in Datenbanken und die Definition der im Voraus festgelegten Kriterien. Dadurch ist die Evaluation selbsterfüllend, ein Zirkelschluss.

26. Leider ist hier nicht der Raum, um auf die von der Kommission aufgeführten Einzelbeispiele „erfolgreicher" PNR-Datenverarbeitung (Arbeitspapier, S. 29 f. und 32 f.) einzugehen. Angemerkt sei aber, dass einzelne Erfolge für sich allenfalls die Eignung, nicht aber die Notwendigkeit oder gar die Verhältnismäßigkeit der PNR-Datenverarbeitung begründen können. Das Verhältnis zwischen der Masse der verarbeiteten Daten und der extrem geringen Zahl weitergehender (nicht notwendigerweise gerechtfertigter) Maßnahmen spricht vielmehr gegen die Verhältnismäßigkeit. Die radikale Erweiterung der PNR-Datenverarbeitung durch die PNR-Richtlinie löst damit den nach der Rechtsprechung des Gerichtshofs (DRI, Rn. 58) erforderlichen Zusammenhang zwischen den PNR-Daten der Betroffenen und den in Rede stehenden schweren Straftaten endgültig auf (dazu ab Absatz Nr. 27). Das gilt ganz besonders für den Abgleich der Fluggastdaten mit im Voraus festgelegten Kriterien (dazu ab Absatz Nr. 33).

2. Kein ausreichender Zusammenhang zwischen PNR-Daten und verfolgtem Ziel

27. In DRI kritisierte der Gerichtshof, dass die Richtlinie (EU) 2006/24/EG „die Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises [beschränkte], der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten“ (DRI, Rn. 59). Für die PNR-Richtlinie gilt das Gleiche.

28. Sie erfasst unterschiedslos alle internationalen Fluggäste. Weder beschränkt sie die Datenverarbeitung auf besonders relevante Flugrouten noch auf bestimmte Zeiträume. Sie ist auch nicht beschränkt auf die Identifizierung von Personen, gegen die bereits ein begründeter Verdacht besteht. Die Richtlinie soll ausdrücklich selbst Personen identifizieren, die den Behörden bislang unbekannt sind (in den Worten der EU-Kommission: es sollen „bisher ‚unbekannte‘ Verdächtige identifiziert“ werden, Richtlinienvorschlag KOM(2011) 32 vom 2. Februar 2011, S. 4.). Die auf Grundlage der PNR-Richtlinie erhobenen Daten dürfen zudem für die Verhütung, Aufdeckung, Ermittlung und Verfolgung einer Vielzahl von Straftaten verarbeitet werden. Viele dieser Straftaten haben ein weit geringeres Gewicht als terroristische Straftaten, Menschen- oder Waffenhandel. Dies gilt etwa für Betrugsdelikte (Anhang II Nr. 7 PNR-Richtlinie), Geldwäsche (Nr. 8), illegale Einreise (Nr. 11), Kulturgüterhandel (Nr. 16) oder Produktpiraterie (Nr. 17). Es ist – anders als etwa im EU-Kanada-Abkommen – nicht einmal ein grenzübergreifender Bezug der Straftaten erforderlich. Vor allem aber – und darin unterscheidet sie sich erheblich von der VDS – ist für die staatliche PNR-Datenverarbeitung kein konkreter Verdacht erforderlich, sondern sie betrifft jeden Fluggast. Dadurch ist kein ausreichender Zusammenhang zwischen dem Verhalten der Betroffenen – Reisen in einem Flugzeug – und dem massenhaften Eingriff in ihre Grundrechte aus Art. 7 und 8 GRCh gegeben.

29. Eine grundrechtskonforme Verarbeitung der PNR-Daten scheidet auf Basis der PNR-Richtlinie aus. Die Richtlinie differenziert dazu nicht ausreichend nach Mittel und Zweck differenzieren. So könnte bei einer Person, die zur Fahndung ausgeschrieben ist, zumindest bei Flügen ohne Passkontrolle der Abgleich der PNR-

Daten sämtlicher Flüge und Passagiere mit einer Datenbank notwendig sein. Für einen solchen Abgleich bedarf es aber nicht der Gesamtheit der in Anhang I der PNR-Richtlinie aufgeführten Daten.

30. Der Abgleich mit im Voraus festgelegten Kriterien mag für eng begrenzte Fälle ganz besonders schwerwiegender, grenzübergreifender Kriminalität ein verhältnismäßiges Mittel sein (wahrscheinlich aber selbst das nicht, dazu unten Absatz Nr. 33 ff.). Aber der Abgleich mit im Voraus festgelegten Kriterien wird nie die Aufdeckung, Ermittlung, Verfolgung oder gar Verhütung z.B. einer Betrugsstraftat (Anhang II Nr. 7 PNR-Richtlinie) leisten können. Die PNR-Richtlinie darf dies nicht erlauben.

31. Bei der retrograden Einzelfallanfrage wäre viel stärker zu differenzieren. Denn wann soll etwa die Aufklärung einer Computerstraftat (Anhang II Nr. 9) tatsächlich von PNR-Daten abhängen? Es ist völlig unverhältnismäßig, etwa zur Aufklärung von Betrugs- und Geldwäschedelikten (Anhang II Nr. 7 und 8), illegaler Einreise (Nr. 11), illegalem Kulturgüterhandel (Nr. 16) oder Produktpiraterie (Nr. 17) die PNR-Daten sämtlicher internationaler Fluggäste über Jahre hinweg zu speichern. Der bloße Umstand, dass ein Datum irgendwann irgendwie bei der Aufklärung irgendeiner Straftat helfen kann, rechtfertigt nicht seine zentrale Speicherung. Wäre dem so, wäre jede Form der Massenüberwachung gerechtfertigt, weil es immer sein könnte, dass das Gespeicherte einmal bei der Aufklärung irgendeiner Straftat helfen wird. Denn Personen, nach denen gefahndet wird, fliegen nicht nur mit dem Flugzeug, sie mieten Fahrzeuge, schließen Mobilfunkverträge, eröffnen Bankkonten und tun viele weitere Dinge, bei denen sie Daten angeben müssen, die zu ihrer Festnahme führen könnten. All diese Daten über jedermann stets dem Staat zuzuleiten, widerspricht dem Verhältnismäßigkeitsgrundsatz. Es ignoriert das Interesse der Betroffenen, nicht total erfasst zu werden. Im Übrigen würden für eine retrograde Recherche etliche PNR-Daten (Gepäck, Sitzplatznummer, allgemeine Hinweise etc.) nicht benötigt. Eine Speicherung bei den Fluggesellschaften würde ausreichen.

32. Mit der großen Keule „Terrorismus“ in der Hand, schafft die PNR-Richtlinie in den Mitgliedstaaten gigantische Datenbanken. Darin können sich die Sicherheitsbehörden zu vielen anderen Deliktsformen und zu unterschiedlichen Zwecken bedienen. Ein ausgewogenes Verhältnis zwischen dem tatsächlichen Mehrwert dieser Datenbank, den jeweils auf sie angewandten Mitteln und den jeweils damit

verbundenen Grundrechtseingriffen gewährleistet die PNR-Richtlinie nicht. Erforderlich wären unterschiedliche (teils dezentrale) Datenbanken mit unterschiedlichen Datensätzen, unterschiedlicher Speicherdauer sowie unterschiedlichen Einsatzzwecken und Analysemethoden. Notwendig ist ein Verzicht auf die massenhafte Datenverarbeitung, wenn sie unverhältnismäßig ist, zum Beispiel in Bezug auf minder schwere Straftaten und solche ohne grenzübergreifenden Bezug.

3. Im Besonderen: Abgleich mit im Voraus festgelegten Kriterien

33. Der mit der PNR-Richtlinie erlaubte Abgleich mit im Voraus festgelegten Kriterien verstößt in ganz besonderem Maße gegen Grundrechte. Während beim Abgleich mit Datenbanken immerhin noch mit einem Beitrag zur Verhütung oder Verfolgung einer Straftat zu rechnen ist, ist dieser Zusammenhang beim Abgleich mit im Voraus festgelegten Kriterien vollkommen aufgelöst. Der heutige Stand der Technik bietet keine Gewähr dafür, dass wie auch immer definierte Kriterien mit hinreichender Wahrscheinlichkeit auf eine gefährliche Person hindeuten. Im Gegenteil hat die EU-Kommission bereits anlässlich des EU-Kanada-Abkommens gegenüber dem EuGH eingeräumt, dass eine „gewisse“ Fehlerquote bestehe; der Europäische Datenschutzbeauftragte hielt diese Fehlerquote sogar für „erheblich“ (Gutachten 1/15, Rn. 169 f.). Diese Fehlerquote kann durch individuelle Überprüfungen allenfalls reduziert, nicht aber eliminiert werden, wie schon ein Vergleich mit dem Abgleich von Datenbanken zeigt (oben Absatz Nr. 23).

34. Mit dem Musterabgleich geht die PNR-Richtlinie weit über die VDS hinaus. Die VDS soll allein dazu dienen, in Einzelfällen auf dezentral bei den Telekommunikationsanbietern gespeicherte Telekommunikationsverkehrsdaten zuzugreifen. Für den Zugriff erforderlich war ein konkreter Verdacht. Der Telekommunikationsverkehr sollte aber nicht anlasslos auf auffällige Muster hin untersucht werden.

35. Mit der Regelung wollen die Behörden „bisher ‚unbekannte‘ Verdächtige“ identifizieren (Richtlinienvorschlag KOM(2011) 32 vom 2. Februar 2011, S. 4.). Dieses Ziel wäre nur legitim, wenn die Person, die durch den Abgleich mit im Voraus festgelegten Kriterien identifiziert wird, (zu Recht) verdächtig ist. Der einzige einen Verdacht erregenden Umstand ist jedoch der Abgleich selbst. Es geht also nicht darum, „bisher ‚unbekannte‘ Verdächtige“ zu identifizieren, sondern der Abgleich mit im Voraus festgelegten Kriterien allein begründet einen Verdacht gegen die Betroffenen. Das ist ein großer Unterschied. Denn während in dem Fall eines

Datenbankabgleichs bereits Verdachtsmomente gegen den Betroffenen bestehen, die seine Aufnahme in die Datenbank begründen können, ist beim Abgleich mit im Voraus festgelegten Kriterien das einzig Verdächtige die von einem Algorithmus als verdächtig identifizierte Betrachtung der Fluggastdaten. Ob dieser Verdacht begründet ist, hängt entscheidend davon ab, ob der Algorithmus tatsächlich eine Person identifizieren kann, die eine Straftat begangen hat oder begehen wird. Dies geschieht allein aus einem Algorithmus heraus, sozusagen also aus dem Nichts. Es geht nicht um die Markierung einer Person, die mit einer als verdächtig registrierten Kreditkarte bezahlt hat oder den gleichen Namen wie ein registrierter Terrorverdächtiger oder „foreign fighter" trägt. Derlei Fälle könnte man mit Datenbanken aufspüren. Sondern es geht um die Markierung einer Person, deren Fluggastdaten aus anderen Gründen verdächtig sind. Ein besonders frappierendes Beispiel liefert das Arbeitspapier der Kommission, S. 24. Darin werden Personen als verdächtig genannt, „deren Gepäck nicht zur Dauer des Aufenthalts und ihrem Reiseziel passt" („*whose luggage does not correspond with the length of the stay and destination*"). Die persönliche Präferenz eines Menschen zur Wahl seiner Gepäcksmenge macht ihn zum Verdächtigen. Eine Vorschrift wie die PNR-Richtlinie, die eine so niedrige Verdachtsschwelle für Folgemaßnahmen zulässt, ist kein verhältnismäßiges Mittel zur Verhütung oder Verfolgung von Straftaten.

36. Ein derart geringer Zusammenhang zwischen Mittel und Zweck unterstellt, dass Algorithmen als solche über jeden Zweifel erhaben sind. Dieser Traum technikgläubiger Sicherheitspolitiker ist aber nichts weiter als ein Traum. Die PNR-Richtlinie stellt keine Anforderungen an die Leistungskraft der Vorhersagen der im Voraus festgelegten Kriterien auf. So wäre es möglich gewesen, den Anteil erträglicher falsch-positiver Treffer an der Gesamtzahl an Treffern zu benennen. Auch dies ist nicht geschehen.

37. Der von Art. 6 Abs. 4 PNR-Richtlinie erlaubte Einsatz von Algorithmen zur Gewinnung von Verdächtigen ist auch aus weiteren Gründen grundrechtswidrig. So erklärt zwar Art. 6 Abs. 4 Satz 1 PNR-Richtlinie, dass sie nicht diskriminierend wirken dürfen. Das genügt aber nicht, um eine Diskriminierung durch Algorithmen zuverlässig auszuschließen. In algorithmische Prozesse können sich ungewollt und unerkannt Vorurteile einschleichen. Denn Algorithmen werden von Menschen programmiert, selbstlernende Algorithmen werden von Menschen mit Trainingsdaten versorgt. In beiden Fällen ist nicht ohne Weiteres gewährleistet, dass die Analyseergebnisse des Algorithmus nicht durch bestimmte Vorurteile kompromittiert

sind. Die PNR-Richtlinie müsste spezifische Anforderungen stellen, die diskriminierende Kriterien zuverlässig ausschließen. Dass das notwendig gewesen wäre, ergibt sich auch aus dem Vortrag der der deutschen Prozessvertreter im bereits erwähnten Rechtsstreit vor dem Verwaltungsgericht Wiesbaden (Schriftsatz vom 9. September 2019, S. 3 f.; bereits vorgelegt als Anlage 3): Dort nennt sie als Beispiel das Kriterium von Flügen in die Türkei zur Ermittlung von „foreign fighters", die nach Syrien reisen möchten. Es ist offenkundig, dass Flüge zwischen Deutschland und der Türkei überdurchschnittlich von Menschen mit einem türkischen Migrationshintergrund genutzt werden. Die Nutzung eines solchen Kriteriums setzt sie somit einer stärkeren Gefahr weiterer Maßnahmen aus als Menschen mit einem anderen ethnischen Hintergrund.

38. Ein weiteres Problem ist die mangelnde Transparenz. Während ein Betroffener bei einem Treffer nach einem Datenbankabgleich noch darlegen kann, warum er zu Unrecht in der Datenbank steht, ist Vergleichbares bei einem Abgleich mit im Voraus festgelegten Kriterien nicht gewährleistet. Im schlimmsten Fall verstehen nicht einmal die Nutzer des Algorithmus, warum eine Person einen Treffer generiert. Selbst wenn ihnen aber die Kriterien bekannt sind, nach denen der Betroffene ausgewählt wurde, könnte dem Betroffenen – etwa aus Geheimhaltungsgründen – eine Offenlegung der Kriterien verweigert werden. Selbst wenn ihm die Kriterien offengelegt würden, hätte er keine Mittel, sich zu wehren. Er müsste darlegen, warum die Kriterien tatsächlich ungeeignet sind, einen Verdacht gegen ihn zu begründen. Dies kann er nicht. Es fehlt somit eine wesentliche Voraussetzung für einen effektiven Rechtsschutz.

39. Es ist schließlich wichtig, darauf hinzuweisen, dass der Gerichtshof im Gutachten 1/15 eine andere Konstellation zu beurteilen hatte, als sie die PNR-Richtlinie gestattet. In Rn. 171 des Gutachtens führt der Gerichtshof aus, dass „Art. 15 des geplanten Abkommens hinsichtlich der Folgen einer automatisierten Verarbeitung von PNR-Daten vor[sieht], dass Kanada ‚Entscheidungen, die einen Fluggast erheblich beeinträchtigen, nicht allein auf der Grundlage der automatisierten Verarbeitung von PNR-Daten' trifft." Nur auf dieser Basis war der Gerichtshof bereit, den Abgleich mit im Voraus festgelegten Kriterien – weitere Schutzvorkehrungen vorausgesetzt – für zulässig zu halten. Art. 15 des EU-Kanada-Abkommen verlangte damit aber, dass über die im Voraus festgelegten Kriterien hinaus irgendein weiterer Anhaltspunkt die Folgemaßnahmen begründen muss. Genau das ist aber in der PNR-Richtlinie deutlich abgeschwächt: In Erwägungsgrund 20 der PNR-

Richtlinie steht zwar noch dieselbe Formulierung wie im Gutachten 1/15. In Art. 6 Abs. 5 PNR-Richtlinie heißt es aber nur noch, dass jeder Treffer auf „andere, nicht-automatisierte Art individuell überprüft wird“; der Maßstab wird aber nicht näher bestimmt. Die individuelle Überprüfung erschöpft sich somit regelmäßig schlicht darin, die Übereinstimmung mit den im Voraus festgelegten Kriterien zu prüfen. Damit ist nichts gewonnen.

III. Zur Vorlagefrage 3 (Speicherdauer)

40. Rechtswidrig ist auch die unterschiedslose Dauer der Speicherung der PNR-Daten. Sie widerspricht den Maßgaben des Gerichtshofs, wonach die dauerhafte Speicherung der PNR-Daten von Fluggästen nach ihrer Ausreise nur für Personen in Betracht kommen darf, bei denen objektive Anhaltspunkte dafür bestehen, dass von ihnen eine Gefahr im Zusammenhang mit der Bekämpfung des Terrorismus und grenzüberschreitender schwerer Kriminalität ausgehen könnte (Gutachten 1/15, Rn. 204 ff.).

41. Daher müssten die Daten von Ausländern, die mit dem Flugzeug in einen Mitgliedstaat reisen, nach Ausreise mit dem Flugzeug aus demselben Mitgliedstaat wieder gelöscht werden. Dagegen wandte Deutschland ein, die Ausreise von Ausländern lasse sich nicht zuverlässig feststellen. Fluggäste könnten zum Beispiel innerhalb der EU weiterreisen und von dort in ihre Heimat zurückkehren, ohne dass das dem Mitgliedstaat bekannt würde, in den sie ursprünglich eingereist sind. Dieser Einwand überzeugt nicht. Die meisten Menschen, die in ein bestimmtes Land fliegen, verlassen es auf demselben Weg. Ein Abgleich von Ein- und Ausreise innerhalb der PNR-Datenbank eines Mitgliedstaats (sowie die Ermittlung von Staatsangehörigkeit und Wohnsitz) ist möglich (vgl. die entsprechenden PNR-Daten nach Anhang I Nr. 5 und 18). Das Problem von Menschen, die über Land oder über Wasser weiterreisen, könnte durch eine Obergrenze der Speicherung gelöst werden (z.B. 90 Tage, was der Dauer eines Schengen-Tourismus-Visums entspricht).

42. Selbst wenn es keine Möglichkeit gäbe, die Ausreise der Betroffenen festzustellen, würde dies nicht die Zulässigkeit einer jahrelangen Speicherdauer begründen. Vielmehr müssten diese Daten selbst dann sofort nach (ergebnislosem) Abgleich, also in der Regel unmittelbar nach der Einreise, wieder gelöscht werden. Denn wenn eine verhältnismäßige Lösung nicht umsetzbar ist, ist sie zu unterlassen.

43. Das in den beiden vorstehenden Absätzen aufgeworfene Problem tritt ohnehin nur bei der Einreise von Ausländern auf. Die aus Anlass der Ausreise von Ausländern verarbeiteten PNR-Daten könnten (und müssten) sofort gelöscht werden, wenn nicht im Einzelfall gerade ihre Ausreise eine Gefahr für den Mitgliedstaat begründet. Für die Daten von ausreisenden Inländern eines Mitgliedstaats gilt dasselbe. Auch wenn Inländer zurückkehren, müssten ihre Daten sofort nach Einreise gelöscht werden, wenn nicht gerade ihre Rückkehr eine Gefahr für den Mitgliedstaat begründet.

44. Der Einwand, dass durch eine kürzere Speicherdauer die retrograde Einzelfallanfrage erschwert würde, ist sicher richtig. Aber auch das kann nicht für sich genommen die jahrelange Speicherung der PNR-Daten aller Fluggäste rechtfertigen, weil sonst praktisch jede Form der massenhaften Datenspeicherung in jedem Lebensbereich gerechtfertigt wäre (dazu bereits Absatz Nr. 31).

IV. Zur Vorlagefrage 4 (Verfahrensgarantien)

45. Der Gerichtshof hat in seinem Gutachten 1/15 festgestellt, dass die Verarbeitung der gespeicherten PNR-Daten nach Einreise in das Zielland (dort: Kanada) nur zulässig ist, wenn sie grundsätzlich einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird (Gutachten 1/15, Rn. 202). Diese Vorgabe hält die PNR-Richtlinie nicht ein. Denn für die retrograde Recherche (Art. 6 Abs. 2 lit. b PNR-Richtlinie), die regelmäßig nach Einreise des Betroffenen erfolgt, ist eine Entscheidung durch ein Gericht oder eine unabhängige Verwaltungsstelle nicht erforderlich. Daran ändert die Prüfung der Aufhebung der Depersonalisierung durch eine Justizbehörde (Art. 12 Abs. 3 PNR-Richtlinie) nichts, weil die PNR-Richtlinie zumindest bis zur Depersonalisierung keine unabhängige Kontrolle vorsieht.

46. Dass im EU-Kanada-Abkommen auch sensible Daten betroffen waren, begründet kein anderes Ergebnis. Der Gerichtshof stützte seine Anforderung an das Verfahren nicht auf diesen Umstand. Es ging ihm allein darum, durch unabhängige Kontrollen zu gewährleisten, dass die Verarbeitung der PNR-Daten nach Einreise nur zugelassen wird, wenn sie auf neue Umstände gestützt werden kann, die eine solche Verwendung rechtfertigen (Gutachten 1/15, Rn. 196 ff., insbes. Rn. 200 ff.).

47. Weiter fehlt in der PNR-Richtlinie eine Bestimmung zur Benachrichtigung von Personen, deren Daten nach Art. 12 Abs. 3 PNR-Richtlinie repersonalisiert wurden (vgl. Gutachten 1/15, Rn. 223).

48. Unzureichend sind die verfahrensrechtlichen Vorkehrungen auch insoweit, als nur der Datenschutzbeauftragte der PNR-Zentralstelle regelmäßigen Zugang zu den im Voraus festgelegten Kriterien erhalten muss (Art. 6 Abs. 7 PNR-Richtlinie). Dieser wird nämlich von der PNR-Zentralstelle selbst ernannt (Art. 5 Abs. 1 PNR-Richtlinie), was keine ausreichende Gewähr für eine unabhängige Bewertung gewährleistet. Gerade mit Blick auf den Abgleich mit im Voraus festgelegten Kriterien ist das jedoch essentiell.

V. Zur Vorlagefrage 5 (Übermittlung in Drittstaaten)

49. Der Gerichtshof hat festgestellt, dass eine Weitergabe personenbezogener Daten in Drittstaaten erfordere, dass ein Beschluss der Kommission gemäß Art. 25 Abs. 6 der Richtlinie 95/46 (jetzt: Art. 45 Abs. 3 DSGVO) gefasst worden ist, wonach das Drittland ein angemessenes Schutzniveau für die Daten gewährleistet (Gutachten 1/15, Rn. 214). Diese Voraussetzung erfüllt die PNR-Richtlinie nicht.

50. Nach Art. 11 Abs. 1 lit. a PNR-Richtlinie dürfen PNR-Daten an Drittstaaten übermittelt werden, wenn die Bedingungen des Art. 13 des Rahmenbeschlusses 2008/977/JI erfüllt sind. Nach Art. 59 Abs. 1 JI-Richtlinie ist dieser Rahmenbeschluss aufgehoben, nach Abs. 2 gelten Verweise auf den Rahmenbeschluss als Verweise auf die JI-Richtlinie. Art. 13 des Rahmenbeschlusses 2008/977/JI entsprechen im Wesentlichen die Art. 36 bis 38 JI-Richtlinie. Nach Art. 13 Abs. 3 lit. a des Rahmenbeschlusses 2008/977/JI war es möglich, personenbezogene Daten an Drittstaaten auch ohne einen Angemessenheitsbeschluss zu übermitteln, wenn überwiegende berechtigte Interessen bestanden. Dem entspricht nunmehr Art. 38 JI-Richtlinie, wonach Datenübermittlungen an Drittstaaten unter anderem (Abs. 1 lit. d) möglich ist zu einem der in Art. 1 Abs. 1 JI-Richtlinie genannten Zwecke (Strafverfolgung und Gefahrenabwehr).

51. Damit können nach Art. 11 PNR-Richtlinie PNR-Daten auch dann an Drittstaaten übermittelt werden, wenn kein angemessenes Datenschutzniveau besteht. Ein solches Datenschutzniveau ist jedoch ein notwendiges Korrektiv für die anlasslose Erhebung massenhafter Fluggastdaten und ihre vielgestaltige Verarbeitung.

VI. Schicksal des FlugDaG bei Ungültigkeit der PNR-Richtlinie

52. Es entspricht der Rechtsprechung des Gerichtshofs, dass die Überprüfung der Gültigkeit einer Unionsvorschrift unabhängig von der Formulierung der Vorlagefragen nach allen rechtlichen Gesichtspunkten zu erfolgen hat (EuGH, Urteil vom 7. Juli 1981, Rewe, Rs. C-158/80, ECLI:EU:C:1981:163 Rn. 19 und 27). Daraus kann der Rechtsgedanke abgeleitet werden, dass der Gerichtshof die Gültigkeit einer Unionsvorschrift nicht nur nach allen rechtlichen Gesichtspunkten überprüft, sondern auch Aussagen über die sich daraus ergebenden Konsequenzen trifft. Dies gilt jedenfalls dann, wenn diese unzweifelhaft aus der Beantwortung der Vorlagefragen abzuleiten sind.

53. Ist die PNR-Richtlinie ungültig, bleibt das FlugDaG zunächst bestehen. Das FlugDaG fällt jedoch in den Anwendungsbereich der JI-Richtlinie und muss sich daher am Unionsrecht messen lassen (dazu oben Absatz Nr. 13). Dies begründet die Zuständigkeit des Gerichtshofs zur Bewertung der PNR-Datenverarbeitung nach dem FlugDaG.

54. Im Ergebnis ergibt sich für das FlugDaG nichts anderes als für die PNR-Richtlinie. Die JI-Richtlinie – namentlich Art. 4 (Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten), Art. 5 (Fristen für die Speicherung und Überprüfung), 8 (Rechtmäßigkeit der Verarbeitung) und Art. 11 (automatisierte Entscheidungsfindung im Einzelfall) – ist nämlich ebenfalls im Lichte der Art. 7 und 8 GRCh und der dazu ergangenen Entscheidungen des Gerichtshofs, konkretisiert im Gutachten 1/15, auszulegen. Da das FlugDaG die PNR-Richtlinie umgesetzt hat, widerspricht die Verarbeitung von PNR-Daten auf Grundlage des FlugDaG aus den oben dargelegten Gründen den Vorgaben der JI-Richtlinie im Lichte der Art. 7 und 8 GRCh.

55. Einer erneuten Vorabentscheidungsfrage zum Schicksal des FlugDaG bedarf es daher nicht. Dies sollte der Gerichtshof klarstellen.

E. Antwortvorschlag

Wir schlagen dem Gerichtshof vor, auf die Vorlagefragen wie folgt zu antworten:

Die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 ist mit Artikel 7 und 8 GRCh unvereinbar und daher ungültig.

Artikel 4, 5, 8 und 11 der Richtlinie 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 sind unter Berücksichtigung der Artikel 7 und 8 der Charta so auszulegen, dass sie einem nationalen Gesetz entgegenstehen, das die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 umgesetzt hat.

Prof. Dr. Remo Klinger
(Rechtsanwalt)

Anlagenverzeichnis

Anlage 1	Pressemitteilung Destatis	Absatz Nr. 14
Anlage 2	Auszug Gesetzesbegründung FlugDaG	Absatz Nr. 14
Anlage 3	Auszug Schriftsatz an VG Wiesbaden	Absätze Nr. 23 und 37