GEULEN & KLINGER
Rechtsanwälte

Dr. Reiner Geulen
Prof. Dr. Remo Klinger
10719 Berlin, Schaperstraße 15
Telefon +49 / 30 / 88 47 28-0
Telefax +49 / 30 / 88 47 28-10
e-mail: klinger@geulen.com
geulen@geulen.com
www.geulenklinger.com

Verwaltungsgericht Wiesbaden
Mainzer Straße 124

65189 Wiesbaden

13. Mai 2019

KLAGE

und

ANTRAG AUF ERLASS EINER EINSTWEILIGEN ANORDNUNG

des Herrn **Emilio De Capitani**
…, Belgien,

- Kläger und Antragsteller-

Verfahrensbevollmächtigte:
Rechtsanwälte Dr. Reiner Geulen & Prof. Dr. Remo Klinger,
Schaperstraße 15, 10719 Berlin,

g e g e n

Bundesrepublik Deutschland,
vertreten durch das Bundeskriminalamt,
65173 Wiesbaden,

- Beklagte und Antragsgegnerin -

wegen: Speicherung, Verarbeitung und Übermittlung von Fluggastdaten gemäß FlugDaG

Vorläufiger Gegenstandswert der Klage: EUR 5.000,-

Vorläufiger Gegenstandswert des Anordnungsantrags: EUR 2.500,-

Namens und mit Vollmacht des Klägers (anbei) erheben wir

Klage

und beantragen,

> die Beklagte zu verpflichten, die Speicherung, Verarbeitung und Übermittlung der Fluggastdaten des Klägers hinsichtlich des Fluges mit der Nummer … am … um … Uhr von Brüssel (BRU) nach Berlin Tegel (TXL) sowie des Fluges mit der Nummer … am … um … Uhr von Berlin Tegel (TXL) nach Brüssel (BRU) zu unterlassen.

Ebenfalls wird im Verfahren der

einstweiligen Anordnung

nach § 123 Abs. 1 VwGO beantragt,

> es der Beklagten einstweilen zu untersagen, die Fluggastdaten des Klägers hinsichtlich des Fluges mit der Nummer … am … um … Uhr von Brüssel (BRU) nach Berlin Tegel (TXL) sowie des Fluges mit der Nummer … am … um … Uhr von Berlin Tegel (TXL) nach Brüssel (BRU) zu speichern, zu verarbeiten und zu übermitteln.

Wegen der grundsätzlichen Bedeutung der Sache, insbesondere wegen der sich stellenden Vorlagefragen zum EuGH, regen wir an, von einer Übertragung auf den Einzelrichter abzusehen.

Zur Klage- und Antragsbegründung tragen wir Folgendes vor:

Gliederung

A. Vorbemerkung

Der Kläger ist ehemaliger Leiter des Sekretariats des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres im EU-Parlament sowie Gastprofessor an der Queen Mary University of London und wehrt sich gegen die Speicherung, Verarbeitung und Übermittlung seiner personenbezogenen Daten zu Flügen von Brüssel nach Berlin und wieder zurück gemäß dem Fluggastdatengesetz. Nach diesem Gesetz müssen Fluglinien von sämtlichen Fluggästen, die nach Deutschland fliegen oder Deutschland verlassen, umfangreiche Datensätze an das Bundeskriminalamt übertragen, die neben Namen, Anschrift und Staatsangehörigkeit auch so sensible Daten wie Geburtsdatum, Telefonnummer, E-Mail-Adresse und Zahlungsinformationen sowie Angaben zu Begleitpersonen, zum Gepäck, zum Vielfliegereintrag und „allgemeine Hinweise“ in einem Freitextfeld enthalten. Diese Daten gleicht das Bundeskriminalamt einerseits mit Datenbanken ab, andererseits wendet es darauf sog. „Muster“ an, mit denen es neue Verdachtsmomente gegen Einzelpersonen gewinnen will. Die Daten bleiben fünf Jahre lang gespeichert, was mit erheblichen Sicherheitsrisiken für Fluggäste wie dem Kläger verbunden ist.

Diese neue Form der Massenüberwachung fügt sich nahtlos ein in die zunehmenden Bestrebungen der öffentlichen Hand, Bürgerinnen und Bürger total zu erfassen. Die Fluggastdatenspeicherung sticht aber aus der Vielzahl an Sicherheitsgesetzen dadurch noch heraus, dass ihre Notwendigkeit nicht einmal im Ansatz nachgewiesen ist, vielmehr die Daten von Millionen unbescholtenen Bürgerinnen und Bürgern zu Versuchszwecken gespeichert und verarbeitet werden.

Für den Abgleich der Fluggastdaten mit Datenbanken würden Angaben zur Person genügen (Name, Geburtsdatum usw.), wie sie schon bislang nach § 31a BPolG erhoben und aber auch 24 Stunden nach Einreise wieder gelöscht werden. Indem für den Abgleich nun deutlich mehr Daten deutlich länger gespeichert und verarbeitet werden, verletzt die neue Fluggastdatenspeicherung den Kläger in seinen Rechten. Grundrechtswidrig ist erst recht der Abgleich der Fluggastdaten mit „Mustern“, weil hiervon Fluggäste wie der Kläger unabhängig davon erfasst sind, ob sie vorbelastet sind, ob sie eine als kritisch eingestufte Flugroute nutzen oder dass sie während einer besonderen Gefahrenlage reisen. Nach einem Gutachten des EuGH weist der Musterabgleich zudem eine „gewisse“ Fehlerquote auf, der Europäische Datenschutzbeauftragte hält diese Fehlerquote sogar für „erheblich“. Entsprechend hoch ist die Gefahr ungerechtfertigter Folgemaßnahmen mit allen damit einhergehenden finanziellen und Ansehensverlusten oder gar Freiheitseinbußen.

Die dem Fluggastdatengesetz zugrundeliegende EU-Richtlinie verstößt gegen Art. 7 und 8 der EU-Grundrechte-Charta, wie sie der EuGH in seinem Gutachten zum Fluggastdaten-Abkommen zwischen der EU und Kanada ausgelegt und angewendet hat. Nach den unmittelbar übertragbaren Ausführungen des EuGH ist die Richtlinie zu unbestimmt, insbesondere durch die Verwendung eines Freitextfelds; ihr fehlen konkrete Voraussetzungen für die Speicherung und weitere Verwendung der Daten, stattdessen erfasst sie die Daten unzulässigerweise unterschiedslos; ihr fehlen nachvollziehbare zeitliche Grenzen für die Speicherung der Daten, insbesondere sieht sie keine Löschung der Daten nach Ausreise der Betroffenen vor; ihr fehlen Vorgaben für eine unabhängige Kontrolle der Verarbeitung der massenweise erhobenen Daten; und sie enthält keine ausreichenden Sicherungen bei einer Übermittlung der Daten an ausländische Dienste. Wir regen deshalb zur Wahrung der Grundrechte des Klägers an, das Verfahren auszusetzen und dem EuGH die Frage nach der Gültigkeit der Richtlinie vorzulegen.

Der Bundesgesetzgeber geht mit dem Fluggastdatengesetz aber noch weiter, als es die Richtlinie verlangt, wodurch die Speicherung der Fluggastdaten den Kläger auch in seinem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verletzt: Die Richtlinie schreibt nur die Übertragung von Daten zu außereuropäischen Flügen vor; das Fluggastdatengesetz erstreckt diese Pflicht auf innereuropäische Flüge. Die Maßstäbe des Bundesverfassungsgerichts zur massenweisen Speicherung personenbezogener Daten verletzt das Fluggastdatengesetz daher erst recht.

Der Kläger hat als aktiver Datenschützer ein hohes Interesse an der Unterbindung der Speicherung, Verarbeitung und Übermittlung seiner Daten, ohne dass es auf dieses besondere Interesse ankäme.

B. Tatbestand

Die Klage richtet sich gegen Maßnahmen der Speicherung, Verarbeitung und Weiterleitung von Daten durch die Beklagte auf Grundlage des Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – im Folgenden „**FlugDaG**“). Das Gesetz ist überwiegend am 10. Juni 2017 in Kraft getreten. Die Strafbewehrung der Nichtbefolgung (§ 18 FlugDaG) sowie die Regelungen zur Übermittlung von Fluggastdaten an ausländische Stellen (§§ 7-10 FlugDaG) sind am 25. Mai 2018 in Kraft getreten.

Das FlugDaG dient – wie bereits sein voller Name verrät – der Umsetzung der Richtlinie 2016/681 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung,

Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität vom 27. April 2016 (im Folgenden „**PNR-Richtlinie**“).

Die Klage erstreckt sich auf die Speicherung eines umfangreichen, den Kläger betreffenden Datensatzes, dessen automatisierten Abgleich mit kriminalitätstypischen sog. „Mustern“ und diversen Datenbanken sowie dessen mögliche Weiterleitung an in- und ausländische Stellen.

Die Klage steht in inhaltlichem Zusammenhang mit vom Unterzeichner namens anderer Kläger*innen eingelegten zivilrechtlichen Klagen, die sich gegen die Übermittlung der Datensätze durch die Fluggesellschaften an die Beklagte richten, sowie im Zusammenhang mit einem gegen die Beklagte geführten Parallelverfahren.

I. Der Kläger

Der Kläger ist italienischer Staatsbürger und lebt in Brüssel, Belgien. Er war Leiter des Sekretariats des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres im EU-Parlament (sog. LIBE-Ausschuss), ist Gastprofessor der Queen Mary University of London, Department of Law, und Executive Director der Fundamental Rights European Experts Group – FREE Group. Er blieb also auch nach seiner Pensionierung aus dem EU-Parlament im Dezember 2011 für die Transparenz der öffentlichen Hand und den Schutz personenbezogener Daten aktiv.

Für ein Arbeitstreffen mit der Gesellschaft für Freiheitsrechte e.V. möchte der Kläger am 2. November 2019 von Brüssel nach Berlin und am 5. November 2019 wieder zurück reisen. Dokumentation der Flugbuchung anbei als

Anlage K 1

Es ist für den Kläger vollkommen unverständlich, warum von diesen Flügen Daten in bis zu 19 Kategorien zur Überprüfung an das Bundeskriminalamt übermittelt und dort fünf Jahre lang gespeichert werden sollen. Er möchte nicht, dass über einen Abgleich der dafür notwendigen Daten mit Datenbanken von gesuchten Personen oder Sachen hinaus Daten von ihm zum Abgleich mit für ihn völlig undurchsichtigen „Mustern“ genutzt werden. Der Kläger sieht insbesondere nicht ein, warum es erforderlich sein soll, von einem unbescholtenen Bürger wie ihm über Jahre bei einer Polizeibehörde seine Telefonnummer, seine E-Mail-Adresse, seine Gepäckangaben, seine Zahlungsinformationen, ominöse „allgemeine Hinweise“ und viele weitere Daten zu speichern und zu verarbeiten. Dass die Sicherheitsbehörden sich von einer solchen neuen Vorratsdatenspeicherung belastbare Erkenntnisse über verdächtige Flugbewegungen erhoffen dürfen, ist nirgends hinreichend dargelegt, geschweige denn

belegt, jedenfalls rechtfertigt das nicht die Speicherung und Verarbeitung seiner Daten oder gar die Übermittlung seiner Daten an Dritte. Er hat Sorge, dass er ungerechtfertigten Maßnahmen ausgesetzt wird, nach der durch ihn nicht verhinderbaren Übermittlung seiner Daten an anderen Staaten zum Beispiel auch bei der Einreise in diese Staaten Probleme bekommt, ohne dafür Anlass gegeben zu haben.

In der geplanten Speicherung, Verarbeitung und Übermittlung seiner Daten sieht der Kläger deshalb – bestätigt durch ein Gutachten des EuGH zum PNR-Abkommen zwischen Kanada und der EU – eine Verletzung seiner Grundrechte. Erst recht für inakzeptabel hält er, dass das FlugDaG nicht nur außereuropäische Flüge erfasst, sondern über das Pflichtprogramm der PNR-Richtlinie hinaus auch innereuropäische Flüge wie den seinen.

II. Europarechtlicher Hintergrund der angegriffenen Maßnahmen

Am 27. April 2016 beschlossen das Europäische Parlament und der Rat der Europäischen Union die PNR-Richtlinie mit dem erklärten Ziel der „Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität“ (siehe Erwägungsgrund Nr. 10). Bis dahin hatte im Wesentlichen die Richtlinie 2004/82/EG vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln (im Folgenden „**API-Richtlinie**“), die Verwendung von Fluggastdaten geregelt. Hiernach waren Grenzkontrollbehörden verpflichtet, auf Ersuchen eines Mitgliedstaats bei Flügen in das Gebiet der Europäischen Union im Einzelfall Fluggastdaten zur Verfügung zu stellen. Strafverfolgungsbehörden verwandten die API-Richtlinie mitunter als Grundlage zur Identifizierung von bereits verdächtigen bzw. zur Fahndung ausgeschriebenen Personen. Zu übermitteln war ein Datensatz, dessen Umfang hinter dem in der PNR-Richtlinie vorgesehenen zurückblieb (vgl. Art. 3 Abs. 2 API-Richtlinie). Eine Rechtsgrundlage für eine Erfassung aller Fluggäste zwecks umfassender Verdächtigen- und Verdachtsgewinnung sah die EU-Kommission hierin jedoch nicht.

> Vgl. den Vorschlag der EU-Kommission für die Richtlinie, COM/2011/0032, S. 7 f.

Eine von der EU-Kommission im Jahre 2011 vorgeschlagene Ausweitung der diesbezüglichen Befugnisse lehnte der Ausschuss des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres im Jahre 2013 aufgrund rechtsstaatlicher Bedenken noch ab.

> Vgl. Ausschussbericht vom 29. April 2013, abrufbar unter https://bit.ly/2Hoqcmv (zuletzt abgerufen am 3. Mai 2019).

Im Nachgang der terroristischen Anschläge in Paris im November 2015 kehrte der Vorschlag einer umfassenden Fluggastdatenrichtlinie auf die politische Tagesordnung der EU zurück.

Die PNR-Richtlinie verpflichtet die Mitgliedstaaten, eine sog. „PNR-Zentralstelle“ (Art. 4 Abs. 1 PNR-Richtlinie) einzurichten unter Bindung an die Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (Art. 6 Abs. 2 PNR-Richtlinie). Hierbei handelt es sich gem. Art. 3 Nr. 8 PNR-Richtlinie um „terroristische Straftaten“, die nach nationalem Recht Straftaten im Sinne der Art. 1 Nr. 8 und Nr. 9 des Rahmenbeschlusses 2002/475/JI sind, sowie um die in Anhang II der PNR-Richtlinie aufgeführten strafbaren Handlungen, die als „schwere Kriminalität“ nach dem nationalen Recht eines Mitgliedstaats mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind.

Die Mitgliedstaaten haben gem. Art. 8 Abs. 1 PNR-Richtlinie allen Fluggesellschaften aufzuerlegen, für alle Flüge im Anwendungsbereich der Richtlinie einen in Anhang I der Richtlinie definierten Datensatz (im Folgenden „**PNR-Daten**“) mittels der „Push-Methode“ (Art. 3 Nr. 7 PNR-Richtlinie) an die PNR-Zentralstellen desjenigen Mitgliedstaates zu übermitteln, in dessen Hoheitsgebiet die betreffenden Flüge ankommen oder von dem sie abgehen. „Push“-Methode bedeutet, dass die Fluggesellschaften selbst den Datensatz aktiv übertragen müssen (im Gegensatz zur „Pull“-Methode, bei der der Empfänger Daten an sich ziehen kann). Die PNR-Zentralstellen haben die PNR-Daten gem. Art. 6 PNR-Richtlinie zu verarbeiten. In Anhang I Nr. 12 unter „Allgemeine Hinweise“ ist ein Freitextfeld vorgesehen, das vielfältige, vom Gesetzgeber nicht abschließend bestimmte Informationen enthalten kann.

Gem. Art. 9 Abs. 2 Satz 1 PNR-Richtlinie kann die PNR-Zentralstelle eines jeden Mitgliedstaats in einer begründeten Anfrage an die PNR-Zentralstelle jedes anderen Mitgliedstaats die Übermittlung der dort gespeicherten PNR-Daten und Verarbeitungsergebnisse anfordern. Hierbei hat sie gem. Art. 9 Abs. 2 Satz 2 PNR-Richtlinie ihre Anfrage auf ein konkretes Datenelement bzw. eine konkrete Kombination von Datenelementen zu richten. Unter im Wesentlichen gleichen Voraussetzungen können nationale PNR-Zentralstellen gem. Art. 10 Abs. 2 Satz 1 PNR-Richtlinie PNR-Daten infolge einer begründeten Anfrage an die europäische Strafverfolgungsbehörde Europol übermitteln.

Auch an Drittstaaten dürfen die Mitgliedstaaten gem. Art. 11 Abs. 1 PNR-Richtlinie PNR-Daten und Verarbeitungsergebnisse übermitteln, wenn die gleichen Voraussetzungen erfüllt sind, die bezüglich anderer Mitgliedstaaten gelten. Zusätzlich muss im jeweiligen Drittstaat ein angemessenes Datenschutzniveau i.S.v. Art. 13 Abs. 1 lit. d) des Rahmenbeschlusses 2008/977/JI PNR-Richtlinie herrschen (Art. 11 Abs. 1 lit. a) PNR-Richtlinie). Der

Rahmenbeschluss 2008/977/JI wurde inzwischen abgelöst von der Richtlinie 2016/680 (im Folgenden: „**Datenschutz-Richtlinie**“); Verweise auf den Rahmenbeschluss gelten als Verweise auf die Datenschutz-Richtlinie (vgl. deren Art. 59). Damit ist der Verweis in Art. 11 PNR-Richtlinie nun als Verweis auf Art. 35 ff. Datenschutz-Richtlinie zu verstehen. Folglich ist vor Übermittlung an einen Drittstaat grundsätzlich ein sog. Angemessenheitsbeschluss der EU-Kommission erforderlich (Art. 36 Datenschutz-Richtlinie). Weiter muss die Übermittlung für die in Art. 1 Abs. 2 PNR-Richtlinie genannten Zwecke erforderlich sein (Art. 11 Abs. 1 lit. b) PNR-Richtlinie). Außerdem muss sich der Drittstaat verpflichten, die PNR-Daten nicht ohne Zustimmung des jeweiligen Mitgliedstaats an einen anderen Drittstaat weiterzuleiten (Art. 11 Abs. 1 lit. c) PNR-Richtlinie). Zu diesen streng anmutenden Vorgaben existieren jedoch wesentliche Ausnahmen in Art. 38 Datenschutz-Richtlinie. Danach kann ein Mitgliedstaat auch ohne Angemessenheitsbeschluss oder Garantien (PNR-)Daten übermitteln, wenn die dort genannten, teils äußerst vagen Voraussetzungen (vgl. etwa Art. 38 Abs. 1 lit. d) Datenschutz-Richtlinie: „... im Einzelfall für die in Artikel 1 Absatz 1 genannten Zwecke“) erfüllt sind.

Nach Ablauf von sechs Monaten sollen die PNR-Daten im Zuge einer „Depersonalisierung“ auf die unter Art. 12 Abs. 2 PNR-Richtlinie aufgeführten Kerndaten reduziert werden. Eine „Repersonalisierung“ ist jedoch unter den in Art. 12 Abs. 3 PNR-Richtlinie aufgeführten Voraussetzungen möglich, namentlich zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung terroristischer Straftaten oder schwerer Kriminalität (vgl. Verweis auf Art. 6 Abs. 2 lit. b PNR-Richtlinie).

Die Datenspeicherung, -verarbeitung und -weiterleitung nach der PNR-Richtlinie betrifft nur sog. „Drittstaatsflüge“. Dieser Begriff umfasst gem. Art. 3 Nr. 2 PNR-Richtlinie jeden Linien- oder Gelegenheitsflug einer Fluggesellschaft, der von einem Drittstaat aus startet und das Hoheitsgebiet eines Mitgliedstaats zum Ziel hat oder der vom Hoheitsgebiet eines Mitgliedstaats aus startet und einen Drittstaat zum Ziel hat. In beiden Fällen sind Flüge mit Zwischenlandungen im Hoheitsgebiet von Mitgliedstaaten oder Drittstaaten eingeschlossen. Art. 2 Abs. 1 PNR-Richtlinie gibt den Mitgliedstaaten jedoch die Möglichkeit, die Richtlinie auch auf sog. „EU-Flüge“ anzuwenden, also gem. Art. 3 Nr. 2 PNR-Richtlinie auf jeden Linien- oder Gelegenheitsflug einer Fluggesellschaft, der vom Hoheitsgebiet eines Mitgliedstaats aus startet und das Hoheitsgebiet eines oder mehrerer anderer Mitgliedstaaten zum Ziel hat, ohne Zwischenlandungen im Hoheitsgebiet eines Drittstaats.

III. Gegenstand und Inhalt des FlugDaG

Das FlugDaG setzt die PNR-Richtlinie um. § 1 Abs. 1 FlugDaG bestimmt das

Bundeskriminalamt (BKA) als Fluggastdatenzentralstelle (Äquivalent zur PNR-Zentralstelle), die das Fluggastdatensystem zu verantworten hat. Die Verarbeitung der Daten findet beim Bundesverwaltungsamt (BVA) als „Auftragsverarbeiter“ der Fluggastdatenzentralstelle statt. Die Modalitäten der Zusammenarbeit werden in einer Vereinbarung gem. § 62 BDSG festgelegt. Gem. § 2 Abs. 3 FlugDaG betrifft die Übermittlungspflicht alle zivilen Flüge, die in Deutschland starten und in einem anderen Land landen oder die von einem anderen Staat aus starten und in Deutschland landen oder zwischenlanden, also auch Intra-EU-Flüge. Das FlugDaG geht damit über die Mindestharmonisierung durch die PNR-Richtlinie hinaus, vgl. Art. 2 PNR-Richtlinie. Infolgedessen rechnet das Bundesverwaltungsamt für Deutschland mit jährlich rund 170 Mio. Fluggästen, für die 340 Millionen Datensätze anfallen würden.

> Vgl. die Gesetzesbegründung, BT-Drs. 18/11501, S. 23.

Laut Eurostat wären ohne Intra-EU-Flüge nur rund 65 Mio. Fluggäste betroffen.

> Vgl. Eurostat, Air Transport Statistics 2016, online unter https://bit.ly/2vy5ISK (zuletzt abgerufen am 3. Mai 2019).

Die Liste der zu übermittelnden PNR-Daten wird in § 2 Abs. 2 FlugDaG definiert und entspricht der im Anhang II der PNR-Richtlinie enthaltenen Liste. Auch hier ist ein Freitextfeld vorgesehen (§ 2 Abs. 2 Nr. 16 FlugDaG). Zwar sieht § 13 Abs. 3 FlugDaG unverzügliche Löschungspflichten für alle PNR-Daten vor, die Angaben enthalten zur rassischen oder ethnischen Herkunft, zu den politischen Meinungen, zu den religiösen oder weltanschaulichen Überzeugungen, zur Mitgliedschaft in einer Gewerkschaft, zum Gesundheitszustand, zum Sexualleben oder zur sexuellen Orientierung einer Person. Wie dies insbesondere im nicht systematisierbaren, da im Erachten der übermittelnden Fluggesellschaft liegenden Freitextfeld IT-technisch oder verfahrensmäßig abgesichert werden soll, geht jedoch weder aus dem FlugDaG selbst noch aus der Gesetzesbegründung hervor. So bleibt denkbar, dass etwa durch besondere Essenswünsche (halal, koscher etc.) Rückschlüsse auf eine religiöse Überzeugung möglich sind.

Im Folgenden erläutern wir den Übermittlungs-, Verarbeitungs- und Weiterleitungsprozess der PNR-Daten in seiner zeitlichen Abfolge:

1. Übermittlung der PNR-Daten durch die Fluggesellschaften und Speicherung

Die Fluggesellschaften sind verpflichtet PNR-Daten gem. § 2 Abs. 5 Satz 1 Nr. 1 und 2 FlugDaG zu zwei separaten Zeitpunkten – erstens 48 bis 24 Stunden vor Abflug und zweitens nach dem Boarding des Flugzeugs – an die Fluggastdatenzentralstelle mittels der Push-

Methode elektronisch zu übermitteln. Die Zuwiderhandlung durch Fluggesellschaften ist in § 18 Abs. 1 und 2 FlugDaG mit einer Geldstrafe von bis zu fünfzigtausend Euro bewehrt.

Diese Daten verbleiben im Regelfall fünf Jahre in der vom BVA unterhaltenen, zentralen Datenbank, § 13 Abs. 1 FlugDaG. Die Speicherfrist für an andere Behörden weitergeleitete PNR-Daten sowie für Verarbeitungsergebnisse sind jedoch von dieser Speicherfrist entkoppelt. Auf die PNR-Daten sind gem. § 13 Abs. 4 Satz 3 FlugDaG die für die jeweilige Behörde geltenden Vorschriften anwendbar, die Verarbeitungsergebnisse sind gem. § 13 Abs. 4 Satz 2 FlugDaG erst zu löschen, wenn sie nicht mehr für die Information weiterer Behörden (i.S.v. § 6 Abs. 1 Satz 1, Abs. 2 Satz 1 FlugDaG) bzw. der Fluggastdatenzentralstellen weiterer Mitgliedstaaten oder die Generierung von Mustern relevant sind.

Ferner soll die Eingriffsintensität der Speicherung dadurch herabgesetzt werden, dass die PNR-Daten gem. § 5 Abs. 1 FlugDaG nach Ablauf von sechs Monaten ab ihrer Übermittlung durch die Fluggesellschaften vom Bundeskriminalamt als Fluggastdatenzentralstelle „depersonalisiert“ werden. Dies soll durch Unkenntlichmachung der in § 5 Abs. 1 FlugDaG aufgeführten Datenpunkte erfolgen (Name des Reisenden und der Mitreisenden, Zahlungsinformationen, Vielfliegereintrag, Freitextfeld usw.).

Die Bezeichnung dieses Prozesses als „Depersonalisierung“ ist jedoch unzutreffend oder zumindest systemwidrig. So ist es datenschutzrechtlich, wie IT-technisch üblich zwischen „Anonymisierung“ und „Pseudonymisierung“ zu unterscheiden. Während bei der Anonymisierung die Zuordnung eines Datensatzes zu einer individuellen Person gänzlich unmöglich wird, werden bei der Pseudonymisierung nur bestimmte Identitätsmerkmale durch Pseudonyme (bspw. Zahlenkombinationen) ersetzt, sodass eine individuelle Zuordnung der Datensätze zwar erschwert, aber unter Zuhilfenahme eines Schlüssels möglich bleibt. Diese Unterscheidung verwendet ausweislich §§ 46 Nr. 5, 71 Abs. 1 Satz 4 BDSG an sich auch der Gesetzgeber. So wird in § 46 Nr. 5 BDSG „Pseudonymisierung“ als unter Hinzuziehung von Schlüsseln reversibler Prozess beschrieben, während in § 71 Abs. 1 Satz 4 BDSG von einer Dichotomie der Begriffe „pseudonymisieren“ und „anonymisieren“ ausgegangen wird.

Obwohl die Begriffe „Depersonalisierung“ und „Unkenntlichmachung“ anderes suggerieren, zwingt § 5 Abs. 2 FlugDaG nur zu einer Pseudonymisierung. Denn die „Depersonalisierung“ ist im Sinne einer Wiederermöglichung der individuellen Zuordnung der PNR-Daten aufzuheben, wenn das BKA, die Landeskriminalämter, die Zollverwaltung, die Bundespolizei, die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst oder der Bundesnachrichtendienst (so die in § 6 Abs. 1 und Abs. 2 FlugDaG aufgezählten

Behörden; im Folgenden „**Sicherheitsbehörden**“) dies beantragen und es im Fall eines Abgleichs mit externen Daten der Sicherheitsbehörden nach § 4 Abs. 5 Satz 1 FlugDaG zur Verhütung oder Verfolgung von Straftaten nach § 4 Abs. 1 FlugDaG erforderlich ist (§ 5 Abs. 2 Satz 1 und Satz 4 FlugDaG). Diese „Repersonalisierung“ stellt also den ursprünglichen Datensatz wieder her und kann abweichend von § 5 Abs. 2 Satz 1 Nr. 2 FlugDaG bei Gefahr im Verzug auch durch Anordnung der Präsidentin bzw. des Präsidenten des BKAs ohne gerichtliche Genehmigung erfolgen (§ 5 Abs. 2 Satz 2 FlugDaG).

Zum Zwecke der Repersonalisierung bleiben die depersonalisierten PNR-Daten besonders berechtigten Mitarbeitern der Fluggastdatenzentralstelle weiterhin zugänglich.

2. Die Verarbeitung der PNR-Daten

Das BVA nimmt die PNR-Daten als Auftragsverarbeiter zentral entgegen, bereitet sie technisch auf, gleicht sie nach den fachlichen Vorgaben der Fluggastdatenzentralstelle (d.h. des BKA) automatisiert ab und sichtet sie in technischer Hinsicht, § 1 Abs. 3 FlugDaG.

Nachdem die Datensätze beim BVA eingegangen sind, werden sie gem. § 4 Abs. 2 FlugDaG mit bestehenden Datenbanken und zugleich mit sog. „Mustern“ abgeglichen. Dieser Abgleich erfolgt automatisiert vor Ankunft des Flugzeugs in Deutschland bzw. vor Abflug aus Deutschland. Vor einer Weiterleitung an andere Behörden infolge eines Treffers werden die Verarbeitungsergebnisse gem. § 4 Abs. 2 Satz 2 FlugDaG individuell überprüft.

a) Zweck des Abgleichs

In § 4 Abs. 1 FlugDaG deklarierter Zweck der Datenverarbeitung ist es, Personen zu identifizieren, die eine der in diesem Katalog angeführten Straftaten begangen haben oder innerhalb eines übersehbaren Zeitraums begehen werden. Während § 4 Abs. 1 Nr. 1 bis 4 FlugDaG konkrete Straftatbestände aufzählt, verweisen § 4 Abs. 1 Nr. 5 und 6 FlugDaG lediglich auf EU-Normen, insbesondere auf die Liste strafbarer Handlungen in Anhang II der PNR-Richtlinie, ohne diese in sich unbestimmte Liste näher zu konkretisieren oder eine Erheblichkeitsschwelle aufzustellen.

Die Abgleiche sollen zweierlei erreichen: Einerseits – daher der Abgleich mit bereits bestehenden Datenbanken – die Identifikation von Personen, die bereits im Zusammenhang mit terroristischen Straftaten oder schwerer Kriminalität in Erscheinung getreten sind. Andererseits soll im Abgleich mit sog. „Mustern“ eine „andere, neue Art und Weise“ der Kriminalitätsbekämpfung liegen.

So die Gesetzesbegründung, BT-Drs. 18/11501, S. 28.

So sollen solche Personen aus der Masse der Flugpassagiere herausgefiltert werden, die zwar noch nie strafrechtlich auffällig bzw. verdächtig geworden sind, deren Flugverhalten aber – ob zufällig oder nicht – nach kriminalistischer Erfahrung dem Flugverhalten jener Personen entspricht, die in Verbindung mit einschlägigen Straftaten bereits in Erscheinung getreten sind. Es handelt sich also um den Versuch einer Verdächtigengewinnung.

b) Abgleich mit bestehenden Datenbanken

In § 4 Abs. 2 Nr. 1 FlugDaG ist abstrakt bestimmt, dass der Abgleich mit solchen Datenbanken zulässig ist, die der Ausschreibung von Personen oder Sachen dienen. Der Gesetzgeber geht davon aus, dass in diesem Zuge ein Abgleich erfolgt mit den Datenbanken „Schengener Informationssystem", „INPOL-zentral" und der „Automated Search Facility – Stolen and Lost Travel Documents Database" (im Folgenden „**ASF-SLTD**"). Beim Schengener Informationssystem und dem INPOL-zentral handelt es sich um Fahndungslisten für Personen und Gegenstände, die innerhalb und außerhalb des Schengen-Bereichs gesucht werden. In der ASF-SLTD werden insbesondere als gestohlen gemeldete Gegenstände registriert, sodass erfasst werden kann, wenn ein Fluggast mit gestohlenem bzw. gefälschtem Ausweis- oder Passdokument reist.

Vgl. die Gesetzesbegründung, BT-Drs. 18/11501, S. 28.

c) Abgleich mit „Mustern"

Die Muster basieren auf empirischer, kriminalistischer Erfahrung. In ihnen sollen Profile bekannter Straftäter abgespeichert werden, deren Reiserouten, Zwischenlandungen, Aufenthaltsdauer usw. bezüglich bestimmter Delikte für typisch gehalten werden. Einer weiteren gesetzlichen Festlegung des Inhalts der Muster stehe die dynamische Vorgehensweise der Täter und die damit verbundene Schnelllebigkeit von Mustern entgegen. Es gelte zu verhindern, dass Täter ihre Vorgehensweisen so an Muster anpassen können, dass diese aufgrund starrer gesetzlicher Vorgaben ins Leere laufen. Als Beispielsdelinquenten zieht der Gesetzgeber den Drogenkurier heran, aus dessen Flugverhalten man originär verdachtsbegründend auf sich gleich verhaltende Fluggäste schließen könne.

Vgl. die Gesetzesbegründung, BT-Drs. 18/11501, S. 29.

Gem. § 4 Abs. 3 Satz 1 FlugDaG werden die Muster durch die Fluggastdatenzentrale unter der Anleitung der Sicherheitsbehörden erstellt. Auch die PNR-Daten selbst können dazu

analysiert werden (§ 4 Abs. 4 FlugDaG). Die Muster werden dann mindestens alle sechs Monate in Zusammenarbeit mit den Sicherheitsbehörden sowie dem/der Datenschutzbeauftragten der Fluggastdatenzentralstelle überprüft. Die/der Datenschutzbeauftragte der Fluggastdatenzentralstelle ist identisch mit dem/der Datenschutzbeauftragten des BKA (§ 12 Abs. 1 FlugDaG). Der/die Bundesbeauftragte für Datenschutz und Informationsfreiheit prüft die Erstellung und Anwendung der Muster mindestens alle zwei Jahre (§ 4 Abs. 4 Satz 8 FlugDaG).

Die Wirksamkeit der Anwendung von Mustern zur Verbrechensbekämpfung ist nicht durch Studien belegt, sondern experimentell. Es besteht keine Berichtspflicht der Fluggastdatenzentralstelle an Parlament oder Öffentlichkeit, sondern nur eine Berichtspflicht des/der Bundesbeauftragten für Datenschutz und Informationsfreiheit an die Bundesregierung (§ 4 Abs. 4 Satz 9 FlugDaG).

Beim automatisierten Abgleich der Datensätze mit den Mustern werden zunächst Plausibilitäten gebildet, also Entsprechungen mit dem Flugverhalten bekannter Straftäter gesucht. Anschließend werden „Gegenplausibilitäten“ gebildet, also die Datensätze mit in den Mustern (i.S.v. § 4 Abs. 3 Satz 5 FlugDaG) enthaltenen verdachtsentlastenden Prüfungsmerkmalen abgeglichen. Diejenigen Datensätze, bei denen nicht durch Gegenplausibilitäten wiederlegte Plausibilitäten bestehen, gibt das BVA zur individuellen Validierung an das BKA weiter. Der Gesetzgeber geht davon aus, dass hiervon insgesamt ca. 0,1 % aller Datensätze betroffen sein werden, während 99,9 % der Datensätze beim BVA verbleiben sollen. Diese Erwartungswerte schwanken jedoch. Bei einer im Rahmen der *CeBIT 2017* stattfindenden Demonstration des technischen Systems, das das BVA zur Datenverarbeitung einzusetzen gedenkt, wurden 0,07 % der Datensätze positiv identifiziert.

> Vgl. die Gesetzesbegründung, BT-Drs. 18/11501, S. 26, sowie *Alexander Sander* in der Stellungnahme der Digitalen Gesellschaft e.V. (S. 4) in Ausschussdrucksache 18(4)869 B.

Bei jährlich ca. 170 Mio. mit dem Flugzeug von und nach Deutschland beförderten Personen entspricht eine Positivquote von ca. 0,1 % 170.000 positiven Treffern.

3. Folgemaßnahmen, insbesondere Weiterleitung der Daten und Verarbeitungsergebnisse

Bezüglich dieser positiv identifizierten Datensätze erwägt die Fluggastdatenzentralstelle weitere Maßnahmen. Gerade diejenigen Personen, die vor Verarbeitung der PNR-Daten noch

nicht als verdächtig in Erscheinung getreten sind, sollen dann durch die Sicherheitsbehörden im Rahmen präventiv- oder repressiv-polizeilicher bzw. geheimdienstlicher Maßnahmen „weiter überprüft“ werden.

Vgl. die Gesetzesbegründung, BT-Drs. 18/11501, S. 25.

Die Fluggastdatenzentralstelle leitet die Datensätze und Verarbeitungsergebnisse zur Einleitung solcher Maßnahmen gem. § 6 Abs. 1, Abs. 2 FlugDaG an die Sicherheitsbehörden weiter. Für die in § 6 Abs. 1 FlugDaG genannten Behörden wird die in § 1 Abs. 2 und § 6 Abs. 3 FlugDaG enthaltene Zweckbindung gem. § 6 Abs. 4 FlugDaG insoweit aufgehoben, dass diese, soweit sie Aufgaben der Strafverfolgung wahrnehmen, die übermittelten Daten auch zu anderen Zwecken verwenden können, insbesondere zur Verfolgung anderer, nicht in § 4 Abs. 1 FlugDaG enthaltener Straftaten.

Die PNR-Zentralstelle kann gem. § 7 Abs. 3 FlugDaG ferner sowohl die PNR-Datensätze als auch die Verarbeitungsergebnisse an die PNR-Zentralstellen anderer Mitgliedstaaten übermitteln, wenn sich die Notwendigkeit der Übermittlung nach einem Abgleich herausstellt oder ein begründetes Ersuchen des Mitgliedstaates an die PNR-Zentralstelle ergeht, aus dem sich die Notwendigkeit der Übermittlung zur Verhütung oder Verfolgung der in § 4 Abs. 1 FlugDaG aufgeführten Straftaten ergibt, oder ein entsprechendes Ersuchen beim Luftfahrtunternehmen eingeht. Das Kriterium der Erforderlichkeit wird nicht näher spezifiziert, allerdings führt die Gesetzesbegründung beispielhaft auf, dass die Erforderlichkeit gegeben sei, wenn sich aufgrund einer Analyse von Fluggastdaten herausstellt, dass Schleuserbanden neue Routen in oder über einen anderen Mitgliedstaat nutzen, oder wenn vermehrt Personen, die mit terroristischen Straftaten in Verbindung stehen, in einen bestimmten Mitgliedstaat gereist sind.

Vgl. die Gesetzesbegründung, BT-Drs. 18/11501, S. 33.

Wenn ein ähnliches Ersuchen von Europol vorliegt, kann die Fluggastdatenzentralstelle die PNR-Datensätze sowie die Verarbeitungsergebnisse gem. § 9 Satz 1 FlugDaG auch an Europol übermitteln.

Darüber hinaus kann die Fluggastdatenzentralstelle gem. § 10 Abs. 1 FlugDaG die PNR-Daten und die Verarbeitungsergebnisse auch an die Behörden von Staaten übermitteln, die nicht Mitgliedstaaten der EU sind (im Folgenden „**Drittstaaten**“). Die Voraussetzungen hierfür entsprechen im Wesentlichen denen der §§ 7, 9 FlugDaG. Hinzu tritt jedoch, dass sich gem. § 10 Abs. 1 Nr. 2 FlugDaG diese Behörden verpflichten müssen, die Daten nur dann an die Behörden eines Drittstaates zu übermitteln, wenn dies zur Verhütung oder Verfolgung von

terroristischen Straftaten oder schwerer Kriminalität erforderlich ist, und vor der Weiterübermittlung die Einwilligung der Fluggastdatenzentralstelle eingeholt wird. Ferner hat die Fluggastdatenzentralstelle die §§ 78-80 BDSG zu beachten. Dies setzt voraus, dass die EU-Kommission bezüglich des Drittstaats einen Angemessenheitsbeschluss gem. Art. 36 Abs. 3 der Richtlinie 2016/680 gefasst hat. Dies ist bislang für Andorra, Argentinien, Kanada, die Faröer Inseln, Guernsey, Israel, die Isle of Man, Japan, Jersey, Neuseeland, die Schweiz, Uruguay sowie die USA der Fall.

Liste abrufbar unter https://bit.ly/2Jnzlbo (zuletzt abgerufen am 3. Mai 2019).

Weiter können PNR-Daten auch ohne Angemessenheitsbeschluss oder Garantien an Drittstaaten übermittelt werden – unter denselben vagen Voraussetzungen wie nach Art. 38 Datenschutz-Richtlinie, vgl. § 80 Abs. 1 BDSG.

4. Keine Unterrichtungspflicht

Das FlugDaG sieht nicht vor, betroffene Fluggäste über die PNR-Verarbeitung und -übermittlung oder etwaige Folgemaßnahmen zu unterrichten. So können gegen einen vormals nicht strafrechtlich in Erscheinung getretenen Fluggast infolge einer positiven Identifizierung Ermittlungsmaßnahmen eingeleitet und ihn betreffende Daten an Drittstaaten weitergeleitet werden, ohne dass sie oder er davon erfährt.

IV. Verfahrensverlauf

Der Kläger hat die Beklagte mit Schreiben vom 26. März 2019 zu der Erklärung aufgefordert, dass sie die Speicherung, Verarbeitung und Übermittlung der ihn betreffenden Fluggastdaten hinsichtlich des streitgegenständlichen Flugs unterlassen werde.

Anlage K 2

Daraufhin hat die Beklagte gegenüber dem Unterzeichner mit Schreiben vom 4. April 2019 erklärt, das geltende Recht anwenden und die Fluggastdaten des Klägers speichern und verarbeiten zu wollen.

Anlage K 3

Die vorliegende Klage war damit geboten.

C. Rechtliche Würdigung

Die vorbeugende Unterlassungsklage ist zulässig (dazu unter I.). Sie ist auch begründet, weil dem Kläger mangels wirksamer Rechtsgrundlage ein öffentlich-rechtlicher Anspruch auf Unterlassung der Erhebung, Speicherung und Verarbeitung seiner PNR-Daten zusteht. Denn die dem FlugDaG zugrundeliegende PNR-Richtlinie verletzt höherrangiges europäisches Recht und ist deshalb ungültig (dazu unter II.). Folglich verstößt das FlugDaG selbst gegen europäische Grundrechte (dazu unter III.). Soweit es von der PNR-Richtlinie eingeräumte Spielräume ausschöpft, verstößt das FlugDaG schließlich auch gegen das Grundgesetz (dazu unter IV.).

I. Zulässigkeit

Eine vorbeugende Unterlassungsklage setzt die begründete Besorgnis voraus, die Beklagte werde künftig durch ihr hoheitliches Handeln rechtswidrig in die Rechtssphäre des Klägers eingreifen.

> BVerwG, Urt. v. 22. Oktober 2014 – 6 C 7.13 (= ZD 2015, 322) –, Rn. 20.

Dieses Handeln muss sich bereits so konkret abzeichnen, dass es die für eine Rechtmäßigkeitsprüfung erforderliche Bestimmtheit aufweist.

> BVerwG, Urt. v. 13. Dezember 2017 – 6 A 6.16 (= DÖV 2018, 378) –, Rn. 12 m.w.N.

Das ist hier der Fall, denn die angegriffene PNR-Datenspeicherung und -verarbeitung wird sicher eintreten. Insbesondere fallen die Flüge des Klägers in den sachlichen Anwendungsbereich des § 2 Abs. 3 FlugDaG. Zudem hat der Kläger die Beklagte erfolglos zu der Erklärung aufgefordert, dass sie die streitgegenständlichen PNR-Daten nicht speichern und verarbeiten werde (vgl. Anlage K2).

Die Gewährung vorbeugenden Rechtsschutzes setzt ferner ein besonderes schützenswertes Interesse in dem Sinn voraus, dass es für den Betroffenen nicht zumutbar ist, auf den von der Verwaltungsgerichtsordnung für den Regelfall vorgesehenen nachgängigen Rechtsschutz verwiesen zu werden.

> BVerwG, Urt. v. 13. Dezember 2017 – 6 A 6.16 (= DÖV 2018, 378) –, Rn. 15 m.w.N.

Auch das ist hier der Fall. Denn die PNR-Datenspeicherung und -verarbeitung wird spätestens 24 Stunden vor Abflug erfolgen. Auch droht eine Weiterleitung an andere, auch ausländische Behörden. Nachgängiger Rechtsschutz könnte die Wirkung dieser Eingriffe nicht mehr beseitigen.

Der Kläger ist für den vorbeugend geltend gemachten Anspruch auf Unterlassung der PNR-Datenspeicherung und -verarbeitung auch analog § 42 Abs. 2 VwGO klagebefugt. Denn erfolgt ein vom Schutzbereich des informationellen Selbstbestimmungsrechts erfasster, relevanter Dateneingriff durch staatliche Stellen, ohne dass dies von einer wirksamen Ermächtigungsgrundlage abgedeckt wäre, können hieraus – unmittelbar gestützt auf Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG – Abwehransprüche resultieren (öffentlich-rechtlicher Unterlassungsanspruch).

> OVG Lüneburg, Urt. v. 12. Februar 1991 – 9 L 246/89 (= NJW 1992, 192, 193); vgl. auch BVerwG, Urt. v. 13. Dezember 2017 – 6 A 6.16 (= DÖV 2018, 378) – , Rn. 22.

Dass es für die PNR-Datenspeicherung und -verarbeitung an einer wirksamen Rechtsgrundlage fehlt, legen wir im Folgenden dar.

II. PNR-Richtlinie verstößt gegen höherrangiges europäisches Recht

Die Erhebung, Speicherung und Verarbeitung von PNR-Daten durch die Beklagte auf Grundlage des FlugDaG ist bereits deshalb rechtswidrig und zu unterlassen, weil die dem Gesetz zugrundeliegende PNR-Richtlinie gegen höherrangiges europäisches Recht, namentlich gegen Art. 7 und 8 GRCh verstößt (dazu unter 2.). Wenn dieses Gericht zu derselben Überzeugung gelangt, muss es dem EuGH die Frage zur Entscheidung vorlegen, ob die PNR-Richtlinie mit Art. 7, 8 GRCh vereinbar ist (dazu unter 3.).

1. Bindung an die Grundrechtecharta

Die Organe der Europäischen Union sind nach Art. 51 Abs. 1 Satz 1 GRCh an die in der Charta verbrieften Grundrechte gebunden. Damit sind insbesondere auch von ihnen erlassene Richtlinien an diesen Grundrechten zu messen.

2. Verstoß gegen Art. 7 und 8 GRCh i.V.m. Art. 52 Abs. 1 Satz 2 GRCh

Der EuGH hat sich zu den Maßstäben der Art. 7 und 8 GRCh für den Umgang mit personenbezogenen Daten wiederholt geäußert (dazu unter a)). Nach diesen Maßstäben

greift die PNR-Datenspeicherung und -verarbeitung in diese Grundrechte ein (dazu unter b)), ohne dass sie gerechtfertigt werden kann (dazu unter c)).

a) Rechtsprechung des EuGH

aa) Allgemeine Maßstäbe

Art. 7 GRCh schützt u.a. das Privatleben. Erfasst ist davon insbesondere die freie Entscheidung des Einzelnen über seine persönliche Lebensführung sowie darüber, ob er diese zum Gegenstand öffentlicher Kenntnis und Erörterung macht.

> *Kingreen* in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, Rn. 3.

Nach Art. 8 GRCh hat zudem jede Person ein Recht auf Schutz der sie betreffenden personenbezogenen Daten. Dieses Grundrecht steht in engem Zusammenhang zum Grundrecht auf Achtung des Privatlebens.

> EuGH, Urt. v. 9. November 2010, Volker und Markus Schecke GbR und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 47.

Hinsichtlich der Behandlung personenbezogener Daten hat der EuGH deshalb den Schutzbereich beider Grundrechte einheitlich gezogen.

> Vgl. dazu eingängig das Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 121 ff. m.w.N.; des Weiteren Urt. v. 17. Oktober 2013, Schwarz, C-291/12, EU:C:2013:670, Rn. 24 ff.

In dieser Hinsicht erstrecken sich die beiden Grundrechte auf jede Information, die eine bestimmte oder bestimmbare natürliche Person betrifft.

> EuGH, Urt. v. 9. November 2010, Volker und Markus Schecke GbR und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 52; Urt. v. 24. November 2011, Asociación Nacional de Establecimientos Financieros de Crédito, C-468/10 und C-469/10, EU:C:2011:777, Rn. 42; Urt. v. 17. Oktober 2013, Schwarz, C-291/12, EU:C:2013:670, Rn. 26; vgl. auch Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 122.

Das schließt auch Daten mit ein, die sich auf die berufliche Sphäre des Betroffenen beziehen.

> Vgl. EuGH, Urt. v. 20. Mai 2003, Österreichischer Rundfunk u.a., C-465/00, C-138/01, C-139/01, EU:C:2003:294, Rn. 73 f. zu Art. 8 EMRK.

Laut der Rechtsprechung des EuGH begründet bereits die Weitergabe personenbezogener Daten an einen Dritten, etwa eine Behörde, unabhängig von der späteren Verwendung der übermittelten Informationen einen Eingriff in das Grundrecht aus Art. 7 GRCh. Dasselbe gilt für die Speicherung personenbezogener Daten und den Zugang zu den Daten für ihre Verwendung durch die Behörden. Für die Feststellung eines solchen Eingriffs kommt es nicht darauf an, ob die übermittelten Informationen als sensibel anzusehen sind oder ob die Betroffenen durch den Vorgang irgendwelche Nachteile erleiden.

> EuGH, Urt. v. 20. Mai 2003, Österreichischer Rundfunk u.a., C-465/00, C-138/01 und C-139/01, EU:C:2003:294, Rn. 74 und 75; Urt. v. 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 33 ff.; Urt. v. 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 87; vgl. auch Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 124.

Dies gilt entsprechend für Art. 8 GRCh.

> EuGH, Urt. v. 17. Oktober 2013, Schwarz, C-291/12, EU:C:2013:670, Rn. 25; Urt. v. 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 36; Gutachten des EuGH 1/15, v. 26. Juli 2017, EU:C:2017:592, Rn. 126.

Die in den Art. 7 und 8 der Charta niedergelegten Rechte können jedoch keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden.

> EuGH, Urt. v. 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 48; Urt. v. 17. Oktober 2013, Schwarz, C-291/12, EU:C:2013:670, Rn. 33; Urt. v. 5. Mai 2011, Deutsche Telekom AG, C-543/09, EU:C:2011:279, Rn. 51; vgl. auch Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 136.

Insbesondere die Gewährleistung der öffentlichen Sicherheit ist ein dem Gemeinwohl dienendes Ziel, das auch schwere Eingriffe in die in den Art. 7 und 8 GRCh niedergelegten Grundrechte rechtfertigen kann.

> EuGH, Urt. v. 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 42 und 44; Urt. v. 15. Februar 2016, N., C-601/15 PPU, EU:C:2016:84, Rn. 53; vgl. auch Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 148 f.

Der Schutz des Grundrechts auf Achtung des Privatlebens verlangt jedoch, dass sich die Ausnahmen vom Schutz personenbezogener Daten auf das absolut Notwendige beschränken,

> EuGH, Urteil vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C-73/07, EU:C:2008:727, Rn. 56; vom 9. November 2010, Volker und Markus Schecke GbR und Eifert, C-92/09 und C-93/09, EU:C:2010:662, Rn. 77; vom 8. April 2014, Digital Rights u.a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 52; vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 92; vom 21. Dezember 2016, Tele2 u.a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 96; vgl. auch Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 140,

was sich auch aus dem Verhältnismäßigkeitsgrundsatz in Art. 52 Abs. 1 Satz 2 GRCh ergibt.

In Bezug auf die Speicherung personenbezogener Daten muss die fragliche Regelung stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden personenbezogenen Daten und dem verfolgten Ziel herstellen.

> EuGH, Urt. v. 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 93; Urt. v. 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 110; vgl. auch Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 191.

Bei der Verwendung rechtmäßig gespeicherter personenbezogener Daten darf sich eine Unionsregelung nicht darauf beschränken, dass der Zugang zu solchen Daten einem der in der Regelung genannten Zwecke zu entsprechen hat, sondern sie muss auch die materiell- und verfahrensrechtlichen Voraussetzungen für die Verwendung der Daten festlegen.

> EuGH, Urt. v. 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 117 f. m.w.N.; vgl. auch Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 192.

Um diesen Erfordernissen zu genügen, muss die Bestimmung, die den Eingriff enthält, klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauch ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass der Eingriff auf das absolut Notwendige beschränkt wird. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden. Dies gilt insbesondere, wenn es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht.

> EuGH, Urt. v. 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 54 und 55; Urt. v. 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 109 und 117; Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 141; vgl. in diesem Sinne auch EGMR, 4. Dezember 2008, S. und Marper/Vereinigtes Königreich, 30562/04 und 30566/04, CE:ECHR:2008:1204JUD003056204, § 103.

Diese Rechtsprechung hat der EuGH insbesondere in den Urteilen zur Vorratsdatenspeicherung sowie in seinem Gutachten zum PNR-Abkommen zwischen der EU und Kanada weiter ausdifferenziert.

bb) Urteile des EuGH zur Vorratsdatenspeicherung

Die Richtlinie 2006/24 (im Folgenden „**VDS-Richtlinie**“) verpflichtete ursprünglich alle EU-Mitgliedstaaten, eine Vorratsspeicherung von Telekommunikations-Verbindungsdaten einzuführen. Am 8. April 2014 erklärte der EuGH sie für ungültig, da sie gegen Art. 7, 8 und 52 GRCh verstoße.

> EuGH, Urt. v. 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238.

Einen Eingriff in diese Grundrechte bejahte der EuGH mit der Erwägung, dass aus der Gesamtheit der von der VDS-Richtlinie erfassten Telekommunikations-Verbindungsdaten sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden, gezogen werden können, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren.

> EuGH, Urt. v. 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 27, 32 ff.

Diesen Eingriff zu Gunsten der Bekämpfung des internationalen Terrorismus und schwerer Kriminalität hielt der EuGH für nicht gerechtfertigt. Dabei hat er unter anderem mit folgenden Gesichtspunkten die fehlende Erforderlichkeit der VDS-Richtlinie begründet:

- Der sachliche Anwendungsbereich der VDS-Richtlinie erstrecke sich auf sämtliche Formen elektronischer Kommunikation, deren Nutzung stark verbreitet und im täglichen Leben jedes Einzelnen von wachsender Bedeutung sei; dadurch greife sie in

die Grundrechte fast der gesamten europäischen Bevölkerung ein (Rn. 56 des Urteils). Die erfassten Daten müssten auch keinen Zusammenhang zu einer bestimmten Bedrohung aufweisen, etwa nach Ort oder Zeitraum (Rn. 59).

- Der persönliche Anwendungsbereich der VDS-Richtlinie erstrecke sich auf sämtliche Personen, die elektronische Kommunikationsmittel nutzen, also auch auf Personen, bei denen keinerlei Anhaltspunkt dafür bestehe, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammengang mit schweren Straftaten stehen könnte; auch würden selbst Berufsgeheimnisträger erfasst (Rn. 58 des Urteils).
- Die VDS-Richtlinie enthalte keine hinreichenden verfahrensrechtlichen Vorkehrungen, die den Zugang zu den auf Vorrat gespeicherten Daten einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterwürfen (Rn. 62 des Urteils).
- Außerdem gälten die Speicherfristen für alle Daten, ohne dass nach ihrem etwaigen Nutzen oder den betroffenen Personen unterschieden würde (Rn. 63 f. des Urteils).

Diese Feststellungen zur Unverhältnismäßigkeit der Vorratsspeicherung von Telekommunikations-Verbindungsdaten hat der EuGH in einem zweiten Urteil bestätigt.

> EuGH, Urt. v. 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 99 ff., insbes. Rn. 105 f.

cc) Gutachten des EuGH zu PNR-Daten

Der EuGH hat des Weiteren in einem ausführlichen Gutachten speziell zum Umgang mit PNR-Daten Stellung bezogen.

> Gutachten des EuGH 1/15 v. 26. Juli 2017 (im Folgenden das „**Gutachten**").

Das Gutachten betraf das Fluggastdaten-Abkommen zwischen der EU und Kanada (im Folgenden das „**EU-Kanada-Abkommen**"). Das Europäische Parlament hatte dem EuGH 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.

Der EuGH verlangt zum Schutz personenbezogener Daten, dass im Fall ihrer Übermittlung aus der Union in ein Drittland der Fortbestand des durch das Unionsrecht gewährten hohen Niveaus des Schutzes der Grundfreiheiten und Grundrechte gewährleistet wird. Auch wenn sich die Mittel zur Gewährleistung eines solchen Schutzniveaus von denen unterscheiden können, die in der Union herangezogen werden, um Anforderungen, die sich aus dem

Unionsrecht ergeben, zu wahren, müssen sie sich gleichwohl in der Praxis als wirksam erweisen.

> Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 134; vgl. auch EuGH, Urt. v. 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 72 ff.

Das bedeutet: Was der EuGH schon im Zusammenhang mit einem internationalen PNR-Abkommen für unionsrechtswidrig erkannt hat, gilt erst recht für rein innereuropäische Regelungen („gleichwertig“).

Das Gutachten kam zu dem Schluss, dass das EU-Kanada-Abkommen in der dem EuGH vorgelegten Fassung mit den Art. 7, 8 und 52 Abs. 1 GRCh nicht vereinbar ist, weil

- Teile des EU-Kanada-Abkommens nicht bestimmt genug formuliert waren (dazu sogleich näher);
- die im Rahmen der automatisierten Verarbeitung von PNR-Daten verwendeten Modelle und Kriterien nicht spezifisch und zuverlässig sowie Diskriminierungen nicht ausgeschlossen waren, und dass nicht gewährleistet war, dass Kanada nur Datenbanken einsetzt, die im Zusammenhang mit der Bekämpfung des Terrorismus und schwerer Kriminalität stehen;
- eine Verwendung der Daten über den Zeitpunkt der Einreise hinaus keine neuen Umstände erfordert und keinem Prüfungsvorbehalt durch eine unabhängige Stelle unterliegt;
- eine Weitergabe von PNR-Daten an Drittstaaten möglich ist, ohne dass das EU-Kanada-Abkommen gewährleistet, dass die Drittstaaten ein angemessenes Schutzniveau im Sinne des Unionsrechts gewährleisten; und
- Betroffene über die Speicherung und Verwendung ihrer Daten nach einem Treffer nicht informiert werden.

Der EuGH hat unter anderem folgende Rubriken des EU-Kanada-Abkommens an PNR-Daten für zu unbestimmt gehalten:

- Rubrik 5 („Verfügbare Vielflieger- und Bonus-Daten [Gratisflugscheine, Upgrades usw.]“), weil der Begriff „usw.“ zu unbestimmt sei und weil unklar bleibe, ob mit ihr 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 (vgl. Rn. 157 des Gutachtens).
- 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 des Gutachtens).

b) PNR-Richtlinie greift in Art. 7 und 8 GRCh ein

Die PNR-Richtlinie greift tief ein in das Recht auf Achtung des Privatlebens und in das Recht auf Schutz der personenbezogenen Daten. Was der EuGH zur Speicherung von Telekommunikationsdaten festgestellt hat,

> EuGH, Urt. v. 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 27,

gilt auch für die Speicherung von PNR-Daten: Sie lassen umfassende Rückschlüsse auf das Privat- und das – ebenfalls geschützte – 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, von denen nicht einmal klar ist, welchen Inhalt sie haben. So können – insbesondere bei Vielfliegern, aber nicht nur bei ihnen – detaillierte Persönlichkeitsprofile entstehen. All diese Daten werden über Monate und – in „depersonalisierter“ Form – Jahre zentral gespeichert, werden dort automatisiert mit Datenbanken und Mustern abgeglichen und können an inländische Behörden sowie Behörden von anderen EU-Staaten und sogar Drittstaaten weitergeleitet werden. Die Betroffenen müssen also damit rechnen, dass jede ihrer Flugreisen diversen öffentlichen Stellen bekannt ist oder bekannt werden kann und dass sie ggf. auf Grund eines von ihnen nicht vorhersehbaren Datenverarbeitungsprozesses weiteren Maßnahmen der Sicherheitsbehörden unterworfen werden, die mit erheblichen Beschwernissen einhergehen können.

c) Eingriff ist nicht gerechtfertigt

Der Eingriff in die genannten Grundrechte ist nicht gerechtfertigt, weil er die Grenzen des Erforderlichen überschreitet.

Die PNR-Richtlinie verfolgt legitime Ziele, nämlich die Verhütung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (vgl. Art. 1 Abs. 2 PNR-Richtlinie). Ob die Erhebung, Speicherung und Verarbeitung von PNR-Daten zur Erreichung dieses Ziels allerdings tatsächlich geeignet sind, darf zwar bezweifelt werden. Denn die PNR-Richtlinie erläutert nicht, wie genau der Abgleich mit im Voraus festgelegten Kriterien zu neuen Verdächtigen führen soll, welche Daten also mit welchen weiteren Daten in Bezug gesetzt werden sollen und mit welchem Ergebnis.

Der Eingriff ist allerdings zur Erreichung des Ziels nicht erforderlich bzw. nicht angemessen. Die PNR-Richtlinie ist teilweise bereits zu unbestimmt (dazu unter aa)). Die vorgesehene anlasslose Speicherung und Verarbeitung von PNR-Daten ist ungeachtet dessen insgesamt unzulässig, weil ihr sachlicher und persönlicher Anwendungsbereich zu weit gefasst sind (dazu unter bb)) und die Dauer der Speicherung keinen nachvollziehbaren Grenzen unterliegt (dazu unter cc)). Schließlich sind die Verfahrensrechte der Betroffenen nicht gewahrt (dazu unter dd)) und es besteht kein ausreichender Schutz der Betroffenen bei der Übermittlung von PNR-Daten in Drittstaaten (dazu unter ee)).

aa) PNR-Richtlinie teilweise zu unbestimmt

Nach den Maßstäben des EuGH ist die PNR-Richtlinie nicht hinreichend bestimmt, soweit sie in ihrem Anhang I vorsieht, dass auch der „Vielflieger-Eintrag“ (Nr. 8) sowie „Allgemeine Hinweise (einschließlich aller verfügbaren Angaben zu …)“ (Nr. 12) zu den PNR-Daten gehören und damit zu erheben, zu speichern und zu verarbeiten sind.

Bei den allgemeinen Hinweisen nach Nr. 12 des Anhangs I handelt es sich um ein Freitextfeld. Wie Rubrik 17 des EU-Kanada-Abkommens enthalten die Vorgaben für die Befüllung dieses Feldes keine abschließenden Angaben über Art und Umfang der zu übermittelnden Informationen, wie aus der Verwendung des Wortes „einschließlich“ hervorgeht, und können selbst Informationen umfassen, die keinerlei Bezug zum Zweck der Übermittlung der PNR-Daten haben.

> So zum EU-Kanada-Abkommen das Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 160; s. oben a)cc).

Hinsichtlich des Vielfliegereintrags ergibt sich die Unbestimmtheit daraus, dass unklar ist, ob mit ihm Informationen allein über die Teilnahme der Fluggäste an Bonusprogrammen gemeint sind oder aber sämtliche Informationen über die Flüge und Buchungen, die im Rahmen solcher Programme durchgeführt werden.

So zum EU-Kanada-Abkommen das Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 157; s. oben a)cc).

bb) Zu weiter sachlicher und persönlicher Anwendungsbereich

Der Anwendungsbereich der PNR-Richtlinie ist zu weit und überschreitet die Grenzen des Erforderlichen.

Die PNR-Richtlinie enthält keine sachlichen Einschränkungen: Alle internationalen Flüge aller Fluglinien werden erfasst, unabhängig vom Herkunfts- und Zielland oder einer konkreten oder auch nur erhöhten Bedrohungslage in dem einen oder anderen Land. Zudem werden – im Falle einer Erstreckung auf EU-Flüge, vgl. Art. 2 PNR-Richtlinie – auch PNR-Daten zu Flügen zwischen EU-Nachbarstaaten erhoben und gespeichert, obwohl die EU-Mitgliedstaaten im Vergleich zu vielen anderen Regionen auf der Welt als sicher gelten können. Weiter werden alle an die PNR-Zentralstelle übermittelten Daten gespeichert und einem automatisierten Abgleich mit Datenbanken und Mustern unterworfen.

Eine mildere Maßnahme gleicher Wirkung wäre ohne Weiteres denkbar: So könnten etwa die im Voraus festgelegten Kriterien (Art. 6 Abs. 2 lit. b PNR-Richtlinie) statt auf die erhobenen und von der PNR-Zentralstelle gespeicherten PNR-Daten auf die Auswahl der Flüge angewendet werden, zu denen die Fluglinien überhaupt PNR-Daten an die PNR-Zentralstelle „pushen“ müssen.

Die PNR-Richtlinie enthält auch keine Einschränkungen des persönlichen Anwendungsbereichs: Alle Fluggäste werden erfasst, unabhängig von ihrer persönlichen Vorgeschichte – und auch ohne eine Ausnahme für Berufsgeheimnisträger, die an der Geheimhaltung bestimmter Reisen ein Interesse haben können. Laut Schätzung der Bundesregierung werden 99,9 % der in Deutschland erhobenen PNR-Datensätze keine Treffer auswerfen, das heißt von vornherein unnötigerweise gespeichert und verarbeitet (vgl. dazu bereits oben B.III.2.c)).

Das entspricht nicht der Maßgabe des EuGH, wonach die Speicherung von Daten stets objektiven Kriterien genügen muss, die einen Zusammenhang zwischen den zu speichernden personenbezogenen Daten und dem verfolgten Ziel herstellen.

Vgl. insbes. Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 191, sowie die weiteren Nachweise oben a)aa).

Denn es besteht gerade kein Zusammenhang zwischen der Speicherung der PNR-Daten von objektiv ungefährlichen und unverdächtigen Personen sowie der Terrorismusbekämpfung.

Daran ändert auch nichts, dass sich ein geringer Prozentsatz der gespeicherten PNR-Daten auf unerkannt gefährliche Personen bezieht und die Massenspeicherung gerade (auch) ihrer Identifizierung dient; denn dieser Umstand kann den Zusammenhang nur der PNR-Daten dieser Personen zum verfolgten Ziel herstellen. Der Zusammenhang entsteht auch nicht dadurch, dass etwa die ungefährlichen und unverdächtigen Personen sich wissentlich in einem bestimmten Verdachtskreis bewegen, so etwa durch die Reise in ein Krisengebiet; denn die PNR-Richtlinie betrifft ausnahmslos alle internationalen Flüge.

Die Erfassung von Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte, sowie insbesondere die Erfassung von Berufsgeheimnisträgern sind auch nach dem Maßstab der EuGH-Rechtsprechung zur Vorratsdatenspeicherung mit Art. 7 und 8 GRCh nicht vereinbar.

> Vgl. EuGH, Urt. v. 8. April 2014, Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 58.

Selbst wenn aber die Erhebung und Speicherung für noch erforderlich gehalten werden sollte, entspricht die PNR-Richtlinie jedenfalls nicht der Maßgabe des EuGH, wonach für die Verwendung der Daten materiell-rechtliche Voraussetzungen festgelegt sein müssen.

> Vgl. Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 192, sowie die weiteren Nachweise oben a)aa).

Denn die Verwendung unterliegt gerade keinen weiteren Voraussetzungen: Alle PNR-Daten werden mit bestehenden Datenbanken und mit „im Voraus festgelegte[n] Kriterien“ abgeglichen (Art. 6 Abs. 3 PNR-Richtlinie).

Damit geht die PNR-Richtlinie sogar über die Verwendung von auf Vorrat gespeicherten Telekommunikations-Verbindungsdaten hinaus; denn diese musste stets in Zusammenhang mit einem konkreten Fall stehen – also einem konkreten Tatverdacht –, während die PNR-Datenverarbeitung keinen Anlass braucht, sondern eben ohne weitere Voraussetzungen automatisch erfolgt.

Während der Abgleich der PNR-Daten mit Datenbanken, die – das sei hier unterstellt – einer Straftat verdächtige oder für gefährlich befundene Personen enthalten, noch einen zumindest abstrakten sachlichen Zusammenhang zu dem Ziel der PNR-Richtlinie aufweisen mag, ist das für den Abgleich mit im Voraus festgelegten Mustern nicht gewährleistet. Denn der heutige Stand der Technik bietet keine Gewähr dafür, dass wie auch immer definierte Muster 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 hält diese Fehlerquote sogar für „erheblich“.

> Vgl. dazu das Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 169 f.

Solange aber eine „gewisse“ bis „erhebliche“ Fehlerquote besteht, ist die gleichmäßige Überprüfung aller Flugpassagiere anhand dieser Muster nicht erforderlich, weil klassische Ermittlungsmethoden ebenso viel Erfolg versprechen dürften. Sie ist aber auch unangemessen, weil eine „gewisse“ bis „erhebliche“ Fehlerquote zu einer hohen Zahl an unschuldig Betroffenen führt, die mit nicht gerechtfertigten Folgemaßnahmen rechnen müssen.

Entsprechend hat der EuGH festgestellt, dass für eine automatisierte Verarbeitung mithilfe von Modellen und Kriterien zu gewährleisten ist, dass diese spezifisch und zuverlässig sowie nicht diskriminierend sind, indem bei ihrer Erstellung und Überprüfung statistische Daten und die Ergebnisse internationaler Forschung berücksichtigt werden.

> Vgl. dazu das Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 174.

Derlei Vorkehrungen trifft die PNR-Richtlinie nicht. Zwar gibt Art. 6 Abs. 4 Satz 3 PNR-Richtlinie vor, dass die Kriterien „zielgerichtet, verhältnismäßig und bestimmt sein“ müssten, nicht aber, wie das zu erreichen ist. Zudem ist unklar, wie gewährleistet werden soll, dass als Grundlage der Muster entsprechend der Maßgabe des Art. 6 Abs. 4 Satz 4 PNR-Richtlinie, der vor Diskriminierung (vgl. Art. 21 Abs. 1 GRCh) schützen soll, nicht die rassische oder ethnische Herkunft dienen dürfen. Denn es scheint wahrscheinlich, dass bestimmte internationale Flugrouten für sensibler als andere gehalten werden und dass in erhöhtem Maße Menschen einer bestimmten rassischen oder ethnischen Herkunft diese Flugrouten nutzen. So ist zum Beispiel der Anteil türkischer oder türkischstämmiger Menschen in Flügen von Deutschland in die Türkei sehr hoch und es ist zu erwarten, dass ein Kriterium, das Flüge aus Deutschland in die Türkei für sicherheitsrelevant hält, systematisch türkische oder türkischstämmige Menschen treffen wird und dadurch mittelbar diskriminierend wirkt.

cc) Unzureichende zeitliche Grenzen für die Speicherung und Verwendung der PNR-Daten

Gemessen an den vom EuGH aufgestellten zeitlichen Grenzen für die Speicherung von PNR-Daten überschreitet die PNR-Richtlinie auch insoweit die Grenzen des Erforderlichen.

Nach der Richtlinie ist es zulässig, die PNR-Daten sämtlicher Fluggäste fünf Jahre lang zu speichern und während der gesamten Dauer ihrer Speicherung zu den in Art. 6 Abs. 2 PNR-Richtlinie genannten Zwecken zu verwenden (nach sechs Monaten allerdings nur unter den weiteren Voraussetzungen des Art. 6 Abs. 3 PNR-Richtlinie). Insbesondere hat es auf diese Verwendungsmöglichkeit keinen Einfluss, wenn die Betroffenen das Zielland wieder verlassen haben.

Dies entspricht nicht den Anforderungen der Art. 7 und 8 GRCh, wie sie der EuGH entwickelt hat. Zum EU-Kanada-Abkommen hat der Gerichtshof festgestellt, dass von Fluggästen, die bei ihrer Ein- und Ausreise kontrolliert wurden, für Kanada grundsätzlich keine Gefahr im Bereich des Terrorismus oder grenzübergreifender schwerer Kriminalität ausgehe, wenn weder diese Kontrollen und Überprüfungen noch irgendein anderer Umstand objektive Anhaltspunkte hierfür geliefert hätten. In diesen Fällen bestehe nach ihrer Ausreise kein Zusammenhang mehr zwischen den PNR-Daten und der öffentlichen Sicherheit und die fortwährende Speicherung der Daten sämtlicher Fluggäste sei nicht mehr notwendig. Anderes könne nur gelten, wenn es in konkreten Fällen objektive Anhaltspunkte dafür gäbe, dass von bestimmten Fluggästen auch nach ihrer Ausreise eine Gefahr im Zusammenhang mit Terrorismus oder grenzübergreifender schwerer Kriminalität ausgehen könnte.

> Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 204 ff.; vgl. auch EuGH, Urt. v. 8. April 2014, EU:C:2014:238, Rn. 63 f.; EuGH, Urt. v. 21. Dezember 2016, EU:C:2016:970, Rn. 119.

Übertragen auf die PNR-Richtlinie bedeutet dies, dass eine Speicherung von – besonders qualifizierten, vgl. oben bb) – PNR-Daten von vornherein nur für die Dauer des Aufenthalts im Zielland für erforderlich gehalten werden kann. Die PNR-Daten von Personen, die weder im Vorfeld der Reise noch während der Reise selbst für sicherheitsrelevant befunden wurden, sind sofort zu löschen. Es mag zwar theoretisch möglich sein, dass die Daten irgendwann wieder relevant werden könnten; aber auf diese Eventualität hin Daten über die Reise hinaus zu speichern, steht nach den Wertungen des EuGH in keinem Verhältnis zu dem tiefgreifenden, massenhaften Eingriff in die Grundrechte der Betroffenen.

An dieser Einschätzung ändert auch nichts, dass die PNR-Daten gemäß Art. 12 Abs. 2 PNR-Richtlinie nach sechs Monaten ab ihrer Übermittlung zu depersonalisieren sind. Es kann hier dahinstehen, ob eine solche (umkehrbare) Depersonalisierung (unter Aufrechterhaltung des Vollzugriffs eines qualifizierten Personenkreises, vgl. Gesetzesbegründung, BT-Drs. 18/11501, S. 30) aus grundrechtlicher Sicht überhaupt einen Mehrwert hat – zumal die Daten in der Zwischenzeit bereits bei anderen Behörden liegen können und dort deren eigenen Regeln unterliegen. Denn jedenfalls ändert die Depersonalisierung nichts daran, dass der EuGH eine Fortdauer der Speicherung von PNR-Daten über die Reisedauer hinaus nur bei objektiven Anhaltspunkten dafür zulässt, dass von konkreten Personen auch nach ihrer Ausreise eine Gefahr im Zusammenhang mit Terrorismus oder grenzübergreifender schwerer Kriminalität ausgehen könnte.

dd) Unzureichende Verfahrensgarantien

Weiter bietet die PNR-Richtlinie keinen ausreichenden verfahrensrechtlichen Schutz.

Die PNR-Richtlinie enthält keine Vorgaben, wonach die Speicherung und Verwendung der PNR-Daten einer unabhängigen Kontrolle unterliegen. Lediglich die Aufhebung der Depersonalisierung bedarf der Genehmigung einer „Justizbehörde“ oder einer anderen qualifizierten nationalen Behörde, Art. 12 Abs. 3 PNR-Richtlinie.

Dies entspricht nicht den Anforderungen der Art. 7 und 8 GRCh, wie sie der EuGH entwickelt hat. Zum EU-Kanada-Abkommen hat der EuGH festgestellt, dass eine Verwendung der gespeicherten PNR-Daten nach Einreise in das Zielland (dort: Kanada) nur zulässig ist, wenn sie grundsätzlich – d.h. außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und dessen/deren Entscheidung im Anschluss an einen mit Gründen versehenen Antrag ergeht, der von den zuständigen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Aufdeckung oder Verfolgung von Straftaten gestellt wird.

Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 202 m.w.N.

Diese Vorgaben hält die PNR-Richtlinie nicht ein. Daran ändert auch die Prüfung der Aufhebung der Depersonalisierung durch eine Justizbehörde nichts. Denn erstens ist bereits fraglich, ob sämtliche „Justizbehörden“ der Mitgliedstaaten unabhängig im Sinne des EuGH-Gutachtens sind; und zweitens ist die Prüfung durch eine Justizbehörde nicht für den Fall vorgesehen, dass ein Datensatz nach erfolgreicher Einreise auf Grund neuer konkreter Hinweise weiter verwendet werden soll (dazu bereits oben cc)).

Der EuGH hat in seinem Gutachten zudem die Erforderlichkeit einer Pflicht zur Benachrichtigung von Betroffenen betont. Dazu hat er festgestellt, dass eine – nachträgliche – individuelle Information der Fluggäste erforderlich sei, wenn objektive Anhaltspunkte vorliegen, die eine Verwendung der PNR-Daten über die systematischen/automatisierten Prüfungen hinaus rechtfertigen – und dass im Übrigen eine vorherige Genehmigung durch ein Gericht oder eine unabhängige Verwaltungsstelle erforderlich sei. Dasselbe gelte für Fälle, in denen die PNR-Daten an andere Behörden oder an Einzelpersonen weitergegeben würden. Eine solche Mitteilung dürfe aber erst erfolgen, wenn sie die Ermittlungen der Behörden nicht mehr beeinträchtigen könne.

Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 223 f.

Die PNR-Richtlinie enthält keine solche Benachrichtigungspflicht. Sie verstößt folglich auch aus diesem Grund gegen Art. 7 und 8 GRCh.

ee) Keine ausreichenden Sicherungen bei Übermittlung von PNR-Daten in Drittstaaten

Schließlich enthält die PNR-Richtlinie auch keine ausreichenden Schutzvorkehrungen bei der Übermittlung von PNR-Daten an Drittstaaten.

Der EuGH hat festgestellt, dass eine Weitergabe personenbezogener Daten in Drittländer erfordere, dass ein Beschluss der Kommission gemäß Art. 25 Abs. 6 der Richtlinie 95/46 (jetzt: Art. 36 Datenschutz-Richtlinie) gefasst worden ist, wonach das Drittland ein angemessenes Schutzniveau für die Daten gewährleistet.

Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 214.

Wie oben dargestellt (vgl. B.III.3), können PNR-Daten jedoch auch unter anderen Bedingungen an Drittstaaten weitergeleitet werden, namentlich auf Grundlage von Garantien (Art. 37 Datenschutz-Richtlinie) oder vager Ausnahmebestimmungen (Art. 38 Datenschutz-Richtlinie). Ein angemessenes Datenschutzniveau ist dann gerade nicht gewährleistet.

ff) Gesamtabwägung

Auch einer Gesamtabwägung im Rahmen der Verhältnismäßigkeitsprüfung nach Art. 52 Abs. 1 Satz 2 GRCh hält die PNR-Richtlinie nicht stand.

Sie verfolgt das Ziel, terroristische oder andere schwere Straftaten zu verhindern und zu verfolgen, indem außerhalb konkret erhöhter Bedrohungslagen PNR-Daten sämtlicher

internationaler Fluggäste erhoben, gespeichert und verarbeitet werden, um die Flugbewegungen von in Datenbanken erfassten Personen zu registrieren und mittels im Voraus festgelegter Kriterien neue Verdächtige und Verdachtsmomente zu gewinnen, wobei letztere Kriterien eine „gewisse“ bis „erhebliche“ Fehlerquote haben und zudem der Mehrwert einer erfolgreichen Verdachtsermittlung für die öffentliche Sicherheit unklar ist.

Dem gegenüber stehen

- die staatliche, massenweise, auf Vorrat erfolgende und vor allem automatisierte Speicherung und Verarbeitung der PNR-Daten von Personen, die durch ihr Vorverhalten keinen Anlass zu ihrer Überwachung gegeben haben;
- die überaus lange Speicherung der PNR-Daten (fünf Jahre);
- die an Sicherheit grenzende Wahrscheinlichkeit ungerechtfertigter Folgemaßnahmen gegenüber fälschlich Verdächtigten, wie etwa weitere staatliche Ermittlungsmaßnahmen oder die Verweigerung der Einreise;
- die Gefahr einer einschüchternden Wirkung der heimlichen Massenüberwachung auf die Ausübung anderer Grundrechte wie etwa des Grundrechts auf Bewegungsfreiheit; sowie
- die Gefahr der stigmatisierenden Wirkung gegenüber bestimmten Bevölkerungsgruppen, die auf Grund ihrer Herkunft überproportional von den im Voraus festgelegten Kriterien erfasst werden könnten.

3. Rechtsfolge: Vorlage zum EuGH

Sollte dieses Gericht dem hiesigen Vortrag folgen und Bedenken an der Vereinbarkeit der PNR-Richtlinie – und damit des FlugDaG – mit der EU-Grundrechtecharta haben, so hat es dem EuGH die Frage nach der Gültigkeit der PNR-Richtlinie gemäß Art. 267 Abs. 2 AEUV vorzulegen. Denn hält ein nationales Gericht Sekundärrecht für unvereinbar mit höherrangigem europäischem Recht, so muss es die Sache dem EuGH vorlegen, selbst wenn gegen seine Entscheidung noch Rechtsmittel zulässig wären; der nach Art. 267 Abs. 2 AEUV eingeräumte Ermessensspielraum ist dann auf null reduziert, weil die mitgliedstaatlichen Gerichte nicht befugt sind, selbst die Ungültigkeit von Handlungen der Unionsinstitutionen festzustellen.

> Grundlegend EuGH, Urt. v. 22. Oktober 1987, Foto-Frost, C-314/85, EU:C:1987:452, Rn. 11 ff.; ausdrücklich bestätigt in Urt. v. 6. Dezember 2005, Gaston Schul, C-461/03, EU:C:2005:742, Rn. 17 ff.

Als Vorlagefragen schlagen wir vor:

1. *Ist die Richtlinie 2016/681 mit dem in Art. 7 GRCh verankerten Recht auf Privatleben vereinbar?*
2. *Ist die Richtlinie 2016/681 mit dem in Art. 8 GRCh verankerten Recht auf Schutz personenbezogener Daten vereinbar?*

III. FlugDaG verstößt gegen Art. 7 und 8 GRCh

Die Mitgliedstaaten sind nach Art. 51 Abs. 1 Satz 1 Hs. 2 GRCh bei der Umsetzung von Richtlinien an die EU-Grundrechtecharta gebunden.

> EuGH, Urt. v. 12. Dezember 1996, X, C-74/95, EU:C:1996:491, Rn. 25 f. (zu Art. 7 EMRK); Urt. v. 29. Januar 2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 68.

Soweit das FlugDaG die PNR-Richtlinie eins zu eins umsetzt, ist es an Art. 7 und 8 i.V.m. Art. 51 Abs. 1 Satz 2 GRCh zu messen, danach ebenfalls unwirksam (vgl. oben II.) und seine Anwendung zu unterlassen.

IV. FlugDaG verstößt gegen das Grundgesetz, soweit der deutsche Gesetzgeber Spielräume der PNR-Richtlinie nutzt

Indem § 2 Abs. 3 FlugDaG die Pflicht zur Datenübertragung auch auf innereuropäische Flüge erstreckt, schöpft das Gesetz einen von der PNR-Richtlinie eingeräumten Spielraum aus, der den Prüfmaßstab des Grundgesetzes aktiviert (dazu unter 1.). An diesem Maßstab scheitert das Gesetz, denn es verletzt den Kläger in seinem Grundrecht auf informationelle Selbstbestimmung (dazu unter 2.).

1. Am Grundgesetz zu messender Teil des FlugDaG

Soweit ein nationales Umsetzungsgesetz die Vorgaben einer EU-Richtlinie umsetzt, ist es vorrangig am europäischen Recht zu messen; diese Vorgaben verletzt das FlugDaG im selben Umfang wie die PNR-Richtlinie (vgl. dazu oben II. und III.).

Nur soweit die Ausgestaltung des nationalen Umsetzungsgesetzes nicht EU-rechtlich vorgegeben ist, bleibt das nationale Verfassungsrecht anwendbar.

So speziell zu EU-Richtlinien BVerfGE 118, 79 <95> m.w.N.

Das ist für folgende Regelungen des FlugDaG (im Folgenden die „**angegriffenen FlugDaG-Regelungen**“) der Fall:

- die Erstreckung der PNR-Datenspeicherung und -verarbeitung auf Intra-EU-Flüge nach § 2 Abs. 3 FlugDaG, die nach Art. 2 PNR-Richtlinie nicht zwingend vorgesehen ist;
- die Möglichkeit der Zweckänderung der Datennutzung nach § 6 Abs. 4 FlugDaG;
- die Entscheidung in § 4 Abs. 1 Nr. 5 und 6 FlugDaG, auf europäische Regelungen zu verweisen, anstatt die Straftatbestände aus dem deutschen StGB aufzuzählen.

Insbesondere der erstgenannte Punkt eröffnet eine umfassende Pflicht zur Prüfung, ob die Speicherung und Verarbeitung von PNR-Daten der Intra-EU-Flüge mit dem Grundgesetz vereinbar sind. Denn die damit verbundene Erweiterung des sachlichen Anwendungsbereichs der PNR-Datenspeicherung und -verarbeitung wirkt wie eine eigenständige, nationale PNR-Gesetzgebung, die sich vor dem Maßstab des Grundgesetzes bewähren muss.

2. Verstoß gegen Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Die angegriffenen FlugDaG-Regelungen verletzen den Kläger in seinem Grundrecht auf informationelle Selbstbestimmung.

a) Maßstab

Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verbürgt ein Grundrecht auf informationelle Selbstbestimmung. Dieses Recht gewährleistet die aus dem Grundsatz der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.

> Vgl. BVerfGE 65, 1 <43>; 84, 192 <194>; 96, 171 <181>; 103, 21 <32 f.>; 113, 29 <46>; 115, 320 <341>.

Es sichert seinen Trägern insbesondere Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe der auf sie bezogenen, individualisierten oder individualisierbaren Daten.

> Vgl. BVerfGE 65, 1 <43>; 67, 100 <143>; 84, 239 <279>; 103, 21 <33>; 115, 320 <341>.

Denn wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.

> Vgl. BVerfGE 65, 1 <42 f.>; 115, 320 <341 f.>.

Die beobachtende oder observierende Tätigkeit der Polizei kann den grundrechtlichen Schutzbereich berühren und die rechtliche Qualität von Grundrechtseingriffen gewinnen.

> Vgl. BVerfGE 110, 33 <56>; 115, 320 <342>.

Das gilt namentlich, wenn personenbezogene Informationen zum Zwecke der elektronischen Datenverarbeitung erhoben und gespeichert werden. In der Folge sind diese Daten nicht nur jederzeit und ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar, sie können darüber hinaus – vor allem beim Aufbau integrierter Informationssysteme – mit anderen

Datensammlungen zusammengefügt werden, wodurch vielfältige Nutzungs- und Verknüpfungsmöglichkeiten entstehen.

Vgl. BVerfGE 65, 1 <42>; 115, 320 <342>.

Das Grundrecht auf informationelle Selbstbestimmung ist allerdings nicht schrankenlos gewährleistet. Der Einzelne muss vielmehr solche Beschränkungen seines Rechts hinnehmen, die durch überwiegende Allgemeininteressen gerechtfertigt sind.

Vgl. BVerfGE 65, 1 <43 f.>; 115, 320 <344 f.>.

Diese Beschränkungen bedürfen jedoch einer verfassungsmäßigen gesetzlichen Grundlage, die insbesondere dem Grundsatz der Verhältnismäßigkeit und dem Gebot der Normenklarheit entsprechen muss.

Vgl. BVerfGE 65, 1 <43 f.>; 115, 320 <345>.

Für die rechtliche Beurteilung der Art des durch die Ermächtigung ermöglichten Eingriffs ist unter anderem bedeutsam, wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben.

Vgl. BVerfGE 100, 313 <376>; 109, 279 <353>; 115, 320 <347>.

Für das Gewicht der individuellen Beeinträchtigung ist erheblich, ob die Betroffenen als Personen anonym bleiben, welche persönlichkeitsbezogenen Informationen erfasst werden und welche Nachteile den Grundrechtsträgern aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden.

Vgl. BVerfGE 100, 313 <376>; 109, 279 <353>; 115, 320 <347>.

Das Bundesverfassungsgericht hat diese Kriterien für die Bemessung der Eingriffsintensität informationsbezogener Grundrechtseingriffe vor allem in Entscheidungen zum Fernmeldegeheimnis aus Art. 10 Abs. 1 GG und zum Grundrecht der Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG entwickelt. Da diese Grundrechte spezielle Ausprägungen des Grundrechts auf informationelle Selbstbestimmung darstellen,

vgl. BVerfGE 51, 97 <105>; 100, 313 <358>; 109, 279 <325 f.>,

sind diese Maßstäbe auch auf das allgemeinere Grundrecht anwendbar, soweit sie nicht durch die für die speziellen Gewährleistungen geltenden Besonderheiten geprägt sind.

Vgl. BVerfGE 115, 320 <347>.

Das Gewicht informationsbezogener Grundrechtseingriffe richtet sich auch danach, welche Nachteile den Betroffenen aufgrund der Eingriffe drohen oder von ihnen nicht ohne Grund befürchtet werden.

Vgl. BVerfGE 100, 313 <376>; 115, 320 <351>.

So kann die Übermittlung und Verwendung von Daten für die davon Betroffenen das Risiko begründen, Gegenstand staatlicher Ermittlungsmaßnahmen zu werden, was über das allgemeine Risiko hinausgeht, einem unberechtigten Verdacht ausgesetzt zu werden.

Vgl. BVerfGE 115, 320 <351>.

Auch können informationsbezogene Ermittlungsmaßnahmen im Falle ihres Bekanntwerdens eine stigmatisierende Wirkung für die Betroffenen haben und so mittelbar das Risiko erhöhen, im Alltag oder im Berufsleben diskriminiert zu werden.

Vgl. BVerfGE 115, 320 <351>.

Grundrechtseingriffe, die sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind – bei denen also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben – , weisen grundsätzlich eine hohe Eingriffsintensität auf.

Vgl. BVerfGE 100, 313 <376, 392>; 109, 279 <353>; 113, 29 <53>; 113, 348 <383>; 115, 320 <354>.

Denn der Einzelne ist in seiner grundrechtlichen Freiheit umso intensiver betroffen, je weniger er selbst für einen staatlichen Eingriff Anlass gegeben hat. Von solchen Eingriffen können ferner Einschüchterungseffekte ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können.

Vgl. BVerfGE 65, 1 <41 f.>; 113, 29 <46>; 115, 320 <354>.

Ein von der Grundrechtsausübung abschreckender Effekt muss nicht nur zum Schutze der subjektiven Rechte der betroffenen Einzelnen vermieden werden. Auch das Gemeinwohl wird dadurch beeinträchtigt, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist.

Vgl. BVerfGE 113, 29 <46>; 115, 320 <354 f.>.

Es gefährdet die Unbefangenheit des Verhaltens, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen.

Vgl. BVerfGE 115, 320 <355>.

Der Grundsatz der Verhältnismäßigkeit führt zudem dazu, dass der Gesetzgeber intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorsehen darf.

Vgl. BVerfGE 100, 313 <383 f.>; 109, 279 <350 ff.>; 115, 320 <361>.

Ob ein Grundrechtseingriff zur Abwehr künftig drohender Rechtsgutbeeinträchtigungen auch im Vorfeld konkreter Gefahren verhältnismäßig sein kann, hängt nicht nur davon ab, ob eine hinreichende Aussicht darauf besteht, dass der Eingriff Erfolg verspricht,

zum Erfordernis der Erfolgseignung BVerfGE 42, 212 <220>; 96, 44 <51>; 115, 320 <361>,

sondern auch davon, welche Anforderungen die Eingriffsnorm hinsichtlich der Nähe der betroffenen Personen zur fraglichen Rechtsgutbedrohung vorsieht.

Vgl. BVerfGE 100, 313 <395>; 110, 33 <60 f.>; 113, 348 <385 ff., 389>; 115, 320 <361 f.>.

Verzichtet der Gesetzgeber auf begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe der Betroffenen zur abzuwehrenden Bedrohung und sieht er gleichwohl eine Befugnis zu Eingriffen von erheblichem Gewicht vor, genügt dies dem Verfassungsrecht nicht.

Vgl. BVerfGE 115, 320 <362>.

Nach diesen Maßstäben stellte das Bundesverfassungsgericht etwa zur Rasterfahndung fest, sie dürfe nicht schon im Vorfeld einer konkreten Gefahr ermöglicht werden, denn sie würde zu vollständig verdachtslos und mit hoher Streubreite erfolgenden Grundrechtseingriffen führen, die Informationen mit intensivem Persönlichkeitsbezug erfassen können.

Vgl. BVerfGE 115, 320 <362>.

b) Grundrechtsverletzung durch PNR-Datenspeicherung und -verarbeitung

Nach diesen Maßstäben verletzen die angegriffenen FlugDaG-Regelungen das Grundrecht auf informationelle Selbstbestimmung.

aa) Anwendung des FlugDaG auf Intra-EU-Flüge

Die PNR-Datenspeicherung und -verarbeitung greift in das Recht auf informationelle Selbstbestimmung ein, denn es werden personenbezogene Informationen zum Zwecke der elektronischen Datenverarbeitung erhoben, gespeichert und weiterverarbeitet.

> Vgl. BVerfGE 115, 320 <342>; 120, 378 <397 f.>; vgl. auch bereits oben II.2.b) zu den strukturell gleichartigen Art. 7, 8 GRCh.

Ein solcher Eingriff muss, um gerechtfertigt zu sein, den Verhältnismäßigkeitsgrundsatz einhalten, also ein legitimes Ziel verfolgen sowie zur Erreichung dieses Ziels geeignet, erforderlich und angemessen sein.

Wie auch die PNR-Richtlinie selbst verfolgt das FlugDaG mit der Verhütung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (§ 1 Abs. 2 FlugDaG) legitime Ziele.

Es ist allerdings fraglich, ob die Maßnahme zur Erreichung dieser Ziele tatsächlich geeignet ist, mehr noch als im Fall der Verarbeitung von PNR-Daten zu Flügen aus dem und in das Nicht-EU-Ausland. Denn dazu müssten Erkenntnisse vorliegen, dass auf Intra-EU-Flüge angewandte Muster sowie der Abgleich mit Datenbanken zur Verhütung und Verfolgung besagter Straftaten beitragen können. Der Gesetzgeber liefert hierfür keine Begründung.

> Dazu krit. *Arzt,* DÖV 2017, 1013 (1026).

Jedenfalls ist aber die Maßnahme zur Zielerreichung nicht erforderlich. Insoweit lassen sich die obigen Ausführungen zur Unverhältnismäßigkeit der PNR-Richtlinie im Lichte der Art. 7, 8 GRCh auf das FlugDaG übertragen: Der sachliche und persönliche Anwendungsbereich des FlugDaG ist zu weit, weil es nicht differenziert, zum Beispiel nach bestimmten Reiserouten oder dem Verdächtigenstatus (dazu oben II.2.c)bb)); auch sind die zeitlichen Grenzen für die Speicherung und Verarbeitung unzureichend, weil nach erfolgreicher Ein- bzw. Ausreise der Betroffenen der Anlass für den Grundrechtseingriff weggefallen ist und das Gesetz hierauf nicht reagiert (dazu oben II.2.c)cc)).

Zudem ist der mit der PNR-Datenspeicherung und -verarbeitung verbundene Grundrechtseingriff nach den Maßstäben der Rechtsprechung des Bundesverfassungsgerichts unangemessen.

Zwar dient das FlugDaG dem Schutz hochrangiger Verfassungsgüter, nämlich dem Schutz der von Terror und schweren Straftaten bedrohten Rechtsgüter. Allerdings genügt diese abstrakte Zwecksetzung nicht. Vielmehr ist der konkrete Beitrag der Einbeziehung von Intra-EU-Flügen in die PNR-Datenspeicherung und -verarbeitung zum Schutz dieser Rechtsgüter abzuschätzen und mit dem in Rede stehenden Grundrechtseingriff abzuwägen. Dabei ist zu berücksichtigen, dass der Gesetzgeber in nur 0,1 % der Fälle positive Treffer aus dem Abgleich mit Datenbanken und Mustern erwartet (dazu oben B.III.2.c)), wobei unklar ist, ob die Trefferquote für die Gruppe der Intra-EU-Flüge hiervon abweicht. Ungeachtet dessen bedeuten positive Treffer noch nicht, dass die neuen Verdachtsmomente begründet (oder Festnahmen von Verdächtigen zurecht erfolgt) sind; herauszurechnen ist vielmehr eine „gewisse“ bis „erhebliche“ Fehlerquote (dazu oben II.2.c)bb)). Selbst unter Abzug dieser Quote ist im Gefahrabwehrbereich nur ein neuer Verdacht gewonnen; dieser kann sich wieder verflüchtigen. Schließlich ist auch im Falle seiner Erhärtung unklar, in wie vielen Fällen eine Verdachtsgewinnung tatsächlich dazu führt, dass eine Straftat verhindert wird.

> Vgl. dazu auch die Erläuterungen des Bundesverfassungsgerichts zur Erfolglosigkeit der Rasterfahndung nach sog. terroristischen Schläfern, für die Datensätze von 5,2 Mio. Menschen verarbeitet wurden, was zu einer Schläferdatei mit 32.000 Menschen führte, deren Durchforstung wiederum für sich genommen zu keinem konkreten Störerverdacht führte, BVerfGE 115, 320 <356>.

Dem gegenüber steht die kontinuierliche, staatliche, langwierige, massenweise und vor allem anlasslose Speicherung und Verarbeitung der PNR-Daten von Personen. Die damit verbundenen Eingriffe haben erhebliches Gewicht, wie sich insbesondere aus der Rechtsprechung des Bundesverfassungsgerichts zur Rasterfahndung und zur Vorratsspeicherung von Telekommunikationsdaten ergibt.

> Zur Bedeutung der BVerfG-Rspr. zur Rasterfahndung für die Beurteilung des FlugDaG vgl. auch *Arzt*, DÖV 2017, 1023 ff.

Zwar definiert das FlugDaG immerhin – anders als die seinerzeit im Streit stehende Regelung des nordrhein-westfälischen Polizeirechts zur Rasterfahndung – die von Speicherung und Verarbeitung betroffenen Daten (vgl. § 2 Abs. 2 FlugDaG). Aber die PNR-Daten enthalten bereits für sich genommen zahlreiche bedeutsame Informationen, neben Namen, Anschrift, Staatsangehörigkeit und Geburtsdatum nämlich auch die Telefonnummer, E-Mail-Adresse

und Zahlungsinformationen sowie Angaben zu Begleitpersonen, zum Gepäck und zum Vielfliegereintrag (dazu vieles weitere). Zudem ist unklar, welche weiteren „allgemeine[n] Hinweise“ die Fluglinien noch durch das Freitextfeld (§ 2 Abs. 2 Nr. 16 FlugDaG) übermitteln werden. Auch sind keine Ausnahmen für Berufsgeheimnisträger vorgesehen.

Problematisch ist auch, dass die PNR-Daten – anders als bei der Vorratsspeicherung der Telekommunikationsdaten – sogleich zentral beim Staat zusammengeführt werden, eben ohne Anlass.

> Für das BVerfG war die dezentrale Speicherung bei Privaten ein wesentliches Kriterium für die Verfassungskonformität einer Vorratsspeicherung von Telekommunikationsdaten, BVerfGE 125, 260 <321 f.>.

All diese Daten sollen nun mit weiteren Datenbanken und „Mustern“ abgeglichen werden, woraus sich – wie bei der Rasterfahndung,

> dazu BVerfGE 115, 320 <349> –

vielfältige neue Informationen gewinnen lassen. Das ist bereits für sich genommen ein tiefer Eingriff in das Grundrecht auf informationelle Selbstbestimmung.

Auf die Intensität dieses Eingriffs wirken sich weiter etwaige aus dem Abgleich resultierende Folgen für die Betroffenen aus:

- Der Abgleich begründet für die Betroffenen ein erhöhtes Risiko, Ziel weiterer behördlicher Ermittlungsmaßnahmen zu werden und unter Erklärungsdruck zu geraten.

  > Zu diesem Aspekt im Zusammenhang mit der Vorratsspeicherung von Telekommunikationsdaten BVerfGE 125, 260 <320>.

  Folgemaßnahmen können auch eine stigmatisierende Wirkung haben, so bereits im Fall der Verweigerung einer Einreise bei der Passkontrolle im Flughafen.
- Die von positiven Treffern Betroffenen werden nicht benachrichtigt – auch nicht nach Abschluss der einem Treffer folgenden Ermittlungen (vgl. zur Unanwendbarkeit des § 56 BDSG oben III.).
- Die Daten bleiben auch nach dem Abgleich bei Ein- bzw. Ausreise ausnahmslos – d.h. auch, wenn sich kein Verdacht ergeben hat – fünf Jahre lang gespeichert und werden für weitere Abgleiche bereitgehalten (nach sechs Monaten allerdings nur noch unter weiteren Voraussetzungen). Diese zeitliche Grenze übertrifft bei weitem jene sechs

Monate, die das Bundesverfassungsgericht im Zusammenhang mit der Vorratsspeicherung von Telekommunikationsdaten „an der Obergrenze dessen“ sah, „was unter Verhältnismäßigkeitserwägungen rechtfertigungsfähig ist“.

BVerfGE 125, 260 <322>.

Anders als bei der Vorratsspeicherung von Telekommunikationsdaten kann sich der Betroffene auch nicht „darauf verlassen, dass seine Daten [nach Ablauf der Frist] gelöscht werden und für niemanden mehr rekonstruierbar sind“,

BVerfGE 125, 260 <322>,

weil vielfältige Übermittlungsmöglichkeiten bestehen, die Daten sich also bereits selbstständig gemacht haben könnten (vgl. oben B.III.3).

- Schließlich ist auch zu berücksichtigen, dass ein Diebstahl der erhobenen Daten nie sicher ausgeschlossen werden kann, was insbesondere im Falle eines Missbrauchs von Zahlungsinformationen weitreichende Folgen für die Betroffenen haben kann.

Hinzu kommt die bereits angesprochene hohe Streubreite der Maßnahme, denn es werden alle ein- oder ausreisenden Fluggäste erfasst, darunter systematisch unverdächtige Personen; außerdem erfolgt der Abgleich nicht im Kontext konkreter Bedrohungslagen, sondern kontinuierlich.

> Vgl. zur automatisierten Kennzeichenerfassung BVerfGE 120, 378 <430>: „Eine automatisierte Kennzeichenerfassung, die unterschiedslos jeden nur deshalb trifft, weil er mit einem Fahrzeug eine ohne besonderen Anlass oder gar dauerhaft eingerichtete Stelle zur automatisierten Erfassung von Kraftfahrzeugkennzeichen passiert, vermittelt im Übrigen den Eindruck ständiger Kontrolle. Das sich einstellende Gefühl des Überwachtwerdens kann [...] zu Einschüchterungseffekten und in der Folge zu Beeinträchtigungen bei der Ausübung von Grundrechten führen.“

Verzichtet aber der Gesetzgeber auf begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe der Betroffenen zur abzuwehrenden Bedrohung und sieht er gleichwohl eine Befugnis zu Eingriffen von erheblichem Gewicht vor, genügt dies dem Verfassungsrecht nicht.

Vgl. BVerfGE 115, 320 <362>.

So intensive Grundrechtseingriffe wie hier sind nur bei einer konkreten Gefahr angemessen.

Vgl. entsprechend zur Rasterfahndung ausführlich BVerfGE 115, 320 <357 ff.>; ähnlich auch (Vorratsdatenspeicherung) BVerfGE 125, 260 <330>: „Die gesetzliche Ermächtigungsgrundlage muss diesbezüglich zumindest tatsächliche Anhaltspunkte einer konkreten Gefahr für die zu schützenden Rechtsgüter verlangen. Dieses Erfordernis führt dazu, dass Vermutungen oder allgemeine Erfahrungssätze nicht ausreichen, um den Zugriff auf die Daten zu rechtfertigen."

Dafür kommt zwar auch eine Dauergefahr in Betracht; eine allgemeine Bedrohungslage, wie sie angeblich spätestens nach dem 11. September 2001 praktisch ununterbrochen bestanden hat, reicht dafür aber nicht aus. Der durch die PNR-Datenspeicherung und -verarbeitung bewirkte Eingriff in das Recht auf informationelle Selbstbestimmung setzt vielmehr das Vorliegen weiterer Tatsachen voraus, aus denen sich eine konkrete Gefahr ergibt, etwa weil tatsächliche Anhaltspunkte für die Vorbereitung terroristischer Anschläge oder dafür bestehen, dass sich in Deutschland Personen für Terroranschläge bereithalten, die in absehbarer Zeit in Deutschland selbst oder andernorts verübt werden sollen.

So ebenfalls zur Rasterfahndung BVerfGE 115, 320 <364 f.>.

bb) Möglichkeit der Zweckänderung der PNR-Daten und Verarbeitungsergebnisse

§ 6 FlugDaG regelt die Übermittlung von Daten, die aus einem Abgleich nach § 4 Abs. 2 oder 5 FlugDaG resultieren, sowie der Ergebnisse der Verarbeitung dieser Daten an verschiedene inländische Behörden. Nach § 6 Abs. 3 FlugDaG dürfen diese Behörden die übermittelten Daten nur zu den Zwecken nach § 4 Abs. 1 FlugDaG verarbeiten. § 6 Abs. 4 FlugDaG schränkt diese Zweckbindung zu Gunsten der Strafverfolgung ein, wenn Erkenntnisse „den Verdacht einer bestimmten anderen Straftat begründen".

Diese Möglichkeit einer Zweckänderung verletzt die Betroffenen in ihrem Recht auf informationelle Selbstbestimmung.

Nach der Rechtsprechung des Bundesverfassungsgerichts sind Zweckänderungen jeweils an den Grundrechten zu messen, die für die Datenerhebung maßgeblich waren. Das gilt für jede Art der Verwendung von Daten zu einem anderen Zweck als dem Erhebungszweck, unabhängig davon, ob es sich um die Verwendung als Beweismittel oder als Ermittlungsansatz handelt.

Vgl. BVerfGE 109, 279 <377>; 141, 220 <327>.

Zwar kann der Gesetzgeber eine weitere Nutzung der Daten auch zu anderen Zwecken als denen der ursprünglichen Datenerhebung erlauben. Er hat dann allerdings sicherzustellen, dass dem Eingriffsgewicht der Datenerhebung auch hinsichtlich der neuen Nutzung Rechnung getragen wird.

> Vgl. BVerfGE 100, 313 <389 f.>; 109, 279 <375 f.>; 120, 378 <408>; 130, 1 <33 f.>; 133, 277 <372 f.>; 141, 220 <326 f.>.

Voraussetzung für eine Zweckänderung ist danach, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten.

> Vgl. BVerfGE 100, 313 <360 ff.>; 109, 279 <377>; 110, 33 <73>; 120, 378 <408>; 130, 1 <34>; 141, 220 <328>.

Das ist in der gegenwärtigen Regelung nicht gewährleistet, denn sie spricht lediglich vom Einsatz der Daten zur Verfolgung des Verdachts einer „bestimmten anderen Straftat“. Diese Formulierung genügt nicht den Anforderungen des Bundesverfassungsgerichts, weil das vergleichbare Gewicht der Straftaten nicht gewährleistet ist.

> So auch *Wollenschläger*, Stellungnahme zum Entwurf des FlugDaG vom 24. April 2017, S. 53 f.

cc) Straftatenkatalog erfüllt nicht die verfassungsrechtlichen Vorgaben

§ 4 Abs. 1 Nr. 1 bis 4 FlugDaG nehmen Bezug auf konkrete Straftatbestände, während § 4 Abs. 1 Nr. 5 und 6 FlugDaG auf EU-Normen verweisen, die lediglich bestimmte strafbare Handlungen – aber keine deutschen Straftatbestände – aufzählen. Außerdem enthält der in Bezug genommene Anhang II der PNR-Richtlinie eine Reihe strafbarer Handlungen, die gegenüber der Schwere der übrigen Handlungen abfallen und häufig in minder schwerer Form begangen werden, wie etwa Korruption (Nr. 6), Betrug (Nr. 7), Geldwäsche (Nr. 8 Var. 1), Computerstraftaten (Nr. 9), Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt (Nr. 11), illegaler Handel mit Kulturgütern (Nr. 16) oder betrügerische Nachahmung und Produktpiraterie (Nr. 17).

Auch das verletzt die Betroffenen in ihrem Grundrecht auf informationelle Selbstbestimmung.

§ 4 Abs. 1 Nr. 5 und 6 FlugDaG sind zunächst nicht hinreichend bestimmt. Nach der Rechtsprechung des Bundesverfassungsgerichts müssen die Voraussetzungen für die

Datenverwendung und deren Umfang in den betreffenden Rechtsgrundlagen umso enger begrenzt werden, je schwerer der in der Speicherung liegende Eingriff wiegt. Anlass, Zweck und Umfang des jeweiligen Eingriffs sowie die entsprechenden Eingriffsschwellen sind dabei durch den Gesetzgeber bereichsspezifisch, präzise und normenklar zu regeln.

Vgl. BVerfGE 100, 313 <359 f.>; 110, 33 <53>; 113, 29 <51>; 113, 348 <375>; 115, 320 <365>; 118, 168 <186 f.>; 125, 260 <328>.

Für die Strafverfolgung folgt hieraus, dass ein Abruf der Daten zumindest den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzt. Welche Straftatbestände hiervon umfasst sein sollen, hat der Gesetzgeber abschließend mit der Verpflichtung zur Datenspeicherung festzulegen. Ihm kommt hierbei ein Beurteilungsspielraum zu. Er kann dabei entweder auf bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen, etwa um Straftaten, für die die Telekommunikationsverkehrsdaten besondere Bedeutung haben, zu erfassen. Die Qualifizierung einer Straftat als schwer muss aber in der Strafnorm – insbesondere etwa durch deren Strafrahmen – einen objektivierten Ausdruck finden. Eine Generalklausel oder lediglich die Verweisung auf Straftaten von erheblicher Bedeutung reichen hingegen nicht aus.

Vgl. BVerfGE 125, 260 <328 f.>.

Nach diesen Maßstäben genügt ein bloßer Verweis in einen EU-Katalog mit strafbaren Handlungen nicht; denn für die Sicherheitsbehörden ist nicht eindeutig ersichtlich, welche deutschen Straftatbestände den in Anhang II PNR-Richtlinie genannten strafbaren Handlungen entsprechen und den Anwendungsbereich des FlugDaG eröffnen. Der Gesetzgeber hätte folglich die dort genannten strafbaren Handlungen „übersetzen“ und in § 4 Abs. 1 aufzählen müssen.

So wohl auch *Arzt*, DÖV 2017, 1023 (1025).

Es ist aber auch nicht gewährleistet, dass der Abgleich nach § 4 Abs. 2 und 5 FlugDaG hinsichtlich hinreichend schwerer Straftaten erfolgt. Das Bundesverfassungsgericht verlangt nämlich vom Gesetzgeber, über die abstrakte Festlegung eines entsprechenden Straftatenkatalogs hinaus sicherzustellen, dass ein Rückgriff auf vorsorglich gespeicherte Daten nur dann zulässig ist, wenn auch im Einzelfall die verfolgte Straftat schwer wiegt und die Verwendung der Daten verhältnismäßig ist.

Vgl. BVerfGE 125, 260 <329>.

Das ist insbesondere für die eingangs dieses Abschnitts aufgezählten strafbaren Handlungen, die auch minderschwere Begehungsformen kennen, nicht gewährleistet. Insoweit fehlt es an einer Erheblichkeitsschwelle im Einzelfall, insbesondere für die Datenübermittlung an andere Behörden (§§ 6 ff. FlugDaG).

Alldem ist auch, soweit inner-europäische Flüge betroffen sind, nicht entgegenzuhalten, die in Anhang II PNR-Richtlinie genannten strafbaren Handlungen seien europarechtlich vorgegeben. Denn der deutsche Gesetzgeber hätte hinsichtlich der inner-europäischen Flüge einen eigenen Straftatenkatalog aufstellen können und müssen.

3. Rechtsfolge: Normenkontrollantrag nach Art. 100 Abs. 1 GG

Für den Fall, dass die Kammer die PNR-Richtlinie für mit Art. 7 und 8 GRCh vereinbar halten oder der EuGH im Wege der Vorabkontrolle die Ungültigkeit der PNR-Richtlinie feststellen sollte, regen wir namens des Klägers eine Vorlage zum Bundesverfassungsgericht nach Art. 100 Abs. 1 Satz 1 GG an.

V. Antrag auf Erlass einstweiliger Anordnung

Der Antrag auf Erlass einer einstweiligen Anordnung nach § 123 Abs. 1 VwGO ist zulässig. Insbesondere besteht trotz des hier geltend gemachten vorbeugenden Rechtsschutzes ein hinreichendes Rechtsschutzinteresse. Verwaltungsgerichtlicher Rechtsschutz ist vor dem Hintergrund des verfassungsrechtlichen Grundsatzes der Gewaltenteilung und des im Ausgangspunkt reaktiv konzipierten Gebots eines effektiven Rechtsschutzes in Art. 19 Abs. 4 GG grundsätzlich nicht vorbeugend ausgestaltet. Ein Abweichen von dieser Grundentscheidung kommt nur ausnahmsweise in Betracht, wenn der nachträgliche Rechtsschutz mit unzumutbaren Nachteilen für den Betroffenen verbunden wäre, insbesondere wenn ohne die Inanspruchnahme vorbeugenden Rechtsschutzes die Gefahr bestünde, dass vollendete, nicht mehr rückgängig zu machende Tatsachen geschaffen würden oder wenn ein nicht mehr wiedergutzumachender Schaden entstünde.

> Vgl. OVG Münster, Beschl. v. 22. Juni 2017 – 13 B 238/17 –, Rn. 27 m.w.N.; OVG Münster, Beschl. v. 1. August 2013 – 4 B 608/13 (= NVwZ 2014, 92); VGH Kassel, Beschl. v. 14. Juli 1988 – 11 TG 1736/85 (= NJW 1989, 470, 472); *Schoch*, in: Schoch/Schneider/Bier, VwGO, Stand: März 2014, § 123 Rn. 46.

Das ist hier der Fall. Denn die PNR-Datenspeicherung und -verarbeitung wird spätestens 24 Stunden vor Abflug erfolgen. Auch droht eine Weiterleitung an andere, auch ausländische

Behörden. Nachgängiger Rechtsschutz könnte die Wirkung dieser Eingriffe nicht mehr beseitigen.

Der Antrag auf Erlass einer einstweiligen Anordnung ist auch begründet. Zur Darlegung des Anordnungsanspruchs verweisen wir auf oben: Die Speicherung und Verarbeitung der PNR-Daten des Klägers wäre rechtswidrig, weil die dem FlugDaG zugrundeliegende PNR-Richtlinie wegen Verstoßes gegen Art. 7 und 8 GRCh ungültig und damit die PNR-Datenspeicherung und -verarbeitung selbst gegen die GRCh verstößt (vgl. oben C.II und C.III); soweit der Bundesgesetzgeber Spielräume der PNR-Richtlinie ausschöpft (PNR-Datenspeicherung und -verarbeitung auch für inner-europäische Flüge) bzw. wegen Ungültigkeit der PNR-Richtlinie das gesamte FlugDaG am Grundgesetz zu messen ist, verstößt die PNR-Datenspeicherung und -verarbeitung auch gegen Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (vgl. oben C.IV).

Der Anordnungsgrund ergibt sich daraus, dass der Verweis des Klägers auf den rechtskräftigen Abschluss des Hauptsacheverfahrens seine zu sichernden Rechte mit Blick auf den bevorstehenden Flug jedenfalls teilweise irreversibel vereiteln würde.

VI. Zusammenfassung

Zusammenfassend ist daher Folgendes festzustellen:

1. Die Klage ist zulässig und begründet.

2. Der Antrag auf Erlass einer einstweiligen Anordnung ist ebenfalls zulässig und begründet.

Der Kläger hat einen im Wege der allgemeinen Leistungsklage (vorbeugende Unterlassungsklage) zu verfolgenden öffentlich-rechtlichen Anspruch auf Unterlassung der PNR-Datenspeicherung, -verarbeitung und -übermittlung.

Nach alledem ist das Verfahren auszusetzen und dem EuGH zur Vorabentscheidung die Frage der Gültigkeit der PNR-Richtlinie vorzulegen.

Wir bitten um unverzügliche Entscheidung über den Anordnungsantrag.

Zur Klage bitten wir höflich um eine baldige mündliche Verhandlung.

Zwei beglaubigte Abschriften anbei.

Prof. Dr. Remo Klinger
(Rechtsanwalt)

Anlagenverzeichnis

Anlage 1: Flugbuchung

Anlage 2: Aufforderungsschreiben an die Beklagte

Anlage 3: Antwortschreiben der Beklagten