Universität Augsburg
Juristische Fakultät

Prof. Dr. F. Wollenschläger - Juristische Fakultät - Universität Augsburg - 86135 Augsburg

Herrn Vorsitzenden
des Innenausschusses
des Deutschen Bundestages
Ansgar Heveling, MdB
Platz der Republik 1
11011 Berlin
Per Email: innenausschuss@bundestag.de

Prof. Dr. Ferdinand Wollenschläger
Lehrstuhl für Öffentliches Recht, Europarecht
und Öffentliches Wirtschaftsrecht

Universitätsstr. 24
86159 Augsburg

Tel +49 (0) 821 598-4550
Fax +49 (0) 821 598-4552

ferdinand.wollenschlaeger@jura.uni-augsburg.de
www.jura.uni-augsburg.de/wollenschlaeger

Augsburg, den 21.4.2017

Öffentliche Anhörung des Innenausschusses am 24.4.2017

Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG)“ (BT-Drs. 18/11501)

Sehr geehrter Herr Vorsitzender,

für die Einladung zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 24.4.2017 zum Entwurf des Fluggastdatengesetzes danke ich. In der Anlage überreiche ich vorab die erbetene schriftliche Stellungnahme.

Mit freundlichen Grüßen

Gez. Prof. Dr. Ferdinand Wollenschläger

Prof. Dr. Ferdinand Wollenschläger

Schriftliche Stellungnahme

Öffentliche Anhörung

des Innenausschusses

des Deutschen Bundestages

zum „Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG)“ (BT-Drs. 18/11501)

am 24. April 2017

Inhaltsübersicht

I. Zusammenfassung

In Umsetzung der EU-Richtlinie 2016/681 führt der vorliegende Gesetzentwurf die Fluggastdatenverarbeitung ein. Diese umfasst ein **Bündel informationeller Maßnahmen**, um terroristische Straftaten und schwere Kriminalität zu verhüten respektive zu verfolgen. Im Kern verpflichtet der Gesetzentwurf Luftfahrtunternehmen, bestimmte Passagierdaten [Passenger Name Record (PNR)-Daten] an das Bundeskriminalamt zu übermitteln. Dieses nimmt vor der Ankunft des Flugzeugs einen automatisierten Abgleich der Daten mit Fahndungsdatenbanken und Mustern vor, die verdachtsbegründende und verdachtsentlastende Prüfungsmerkmale enthalten und damit eine Identifikation von Personen ermöglichen, die für die Verhütung oder Verfolgung terroristischer Straftaten oder schwerer Kriminalität bedeutsame Prüfungsmerkmale erfüllen. Treffer leitet das Bundeskriminalamt nach individueller Überprüfung an bestimmte für die Verhütung und Verfolgung entsprechender Straftaten zuständige Behörden (BKA, LKAs, Zollverwaltung, Bundespolizei; Verfassungsschutzbehörden, MAD, BND) weiter. Darüber hinaus können diese Behörden – vergleichbar mit der Telekommunikations-Verkehrsdatenspeicherung – das Bundeskriminalamt um einen Abgleich der für fünf Jahre zu speichernden, freilich nach sechs Monaten (reversibel) zu depersonalisierenden PNR-Daten ersuchen.

Diese informationellen Maßnahmen stellen angesichts Anlasslosigkeit, Streubreite und Aussagekraft der Daten einen **erheblichen Grundrechtseingriff** dar. **Nicht minder gewichtig** sind freilich die verfolgten **Ziele**, nämlich terroristische Straftaten und schwere Kriminalität zu verhüten respektive zu verfolgen. Auch hierbei handelt es sich um **Anliegen von hohem Verfassungsrang**: So obliegt dem Staat nach ständiger Rechtsprechung des Bundesverfassungsgerichts sowie auch des EuGH die grundrechtlich und rechtsstaatlich fundierte Pflicht, eine effektive Strafverfolgung sicherzustellen und Individualrechtsgüter vor Beeinträchtigungen durch Dritte zu schützen.

Hinsichtlich grundrechtlicher Einwände gegen die Fluggastdatenverarbeitung (namentlich Anlasslosigkeit, Datenkategorien, Speicherdauer, Abgleich mit Mustern, fehlende Benachrichtigung) ist zunächst zu berücksichtigen, dass die **Grundrechtseingriffe im Wesentlichen auf zwingenden Vorgaben der EU-Fluggastdatenrichtlinie** beruhen, die bis zum 25.5.2018 in das deutsche Recht umzusetzen ist. Der Umsetzungspflicht entgegenhalten lassen sich nach der EuGH-Rechtsprechung nur schwere und offensichtliche Rechtsverstöße (dazu III.), deren Vorliegen mangels unmittelbar einschlägiger EuGH-Rechtsprechung und auf der Basis der Stellungnahmen der Generalanwälte zu den PNR-Abkommen mit Drittstaaten sowie der sonstigen Rechtsprechung des EuGH nicht angenommen werden kann; insbesondere lässt sich die EuGH-

Rechtsprechung zur Telekommunikations-Verkehrsdatenspeicherung wegen der deutlich höheren Eingriffsintensität jener Maßnahme nicht unbesehen übertragen. Auch jenseits der Frage der Umsetzungspflicht erscheint die **Fluggastdatenverarbeitung** vor diesem Hintergrund **mit Unionsgrundrechten prinzipiell vereinbar**.

Eine autonom **vom deutschen Gesetzgeber zu verantwortende Entscheidung** stellt die von der EU-Fluggastdatenrichtlinie ermöglichte **Einbeziehung aller Flüge innerhalb der EU** dar, die neben die zwingend vorgegebene Anwendung auf Drittstaatsflüge tritt. Auch insoweit lässt sich der Rechtsprechung des EuGH und des Bundesverfassungsgerichts **kein prinzipielles Verbot der Fluggastdatenverarbeitung** entnehmen.

Unbeschadet dessen seien **folgende (punktuelle) Änderungen am Gesetzentwurf empfohlen**:

- Zur Erhöhung der Bestimmtheit empfiehlt sich, statt des Verweises auf Unionsrecht (§ 4 Abs. 1 Nr. 5 und 6 FlugDaG-E) einen Straftatenkatalog zu formulieren (V.4.b);
- Der in Bezug genommene Betrugstatbestand ist auf hinreichend schwere Begehungsformen zu beschränken (§ 4 Abs. 1 Nr. 6 FlugDaG-E) und auch im Übrigen (§ 4 Abs. 1 FlugDaG-E) eine Erheblichkeitsschwelle im Einzelfall für die Datenübermittlung an Behörden und den Datenabruf zu prüfen (V.4.a);
- Die zu weite Befugnis zur Zweckänderung durch Strafverfolgungsbehörden in § 6 Abs. 4 FlugDaG-E ist in Einklang mit der Intention des Gesetzgebers umzuformulieren: „Die in Absatz 1 Satz 1 genannten Behörden können, soweit sie Aufgaben der Strafverfolgung wahrnehmen, die übermittelten Daten zu anderen Zwecken verarbeiten, wenn 1. mindestens vergleichbar schwer wiegende Straftaten verfolgt und 2. sich im Einzelfall konkrete Ermittlungsansätze zur Verfolgung solcher Straftaten ergeben“ (V.9.);
- § 11 FlugDaG-E ist um das Erfordernis einer regelmäßigen Kontrolle durch die/den BfDI und Berichtspflichten – wie im Kontext des § 4 Abs. 3 S. 8 und 9 FlugDaG-E – zu ergänzen [V.1.j.bb.(2); V.13.].
- Mit Blick auf das Gebot einer transparenten Richtlinienumsetzung sei eine ausdrückliche Inbezugnahme der in der Fluggastdaten-Richtlinie enthaltenen Datenschutzbestimmungen empfohlen, namentlich
    - in § 11 FlugDaG-E auf die Kontrollaufgaben und -befugnisse der/des BfDI gemäß §§ 14 ff. BDSG-E [V.1.j.bb.(2)];
    - in § 11 FlugDaG-E auf die Kontrollaufgaben und -befugnisse des Datenschutzbeauftragten der Fluggastdatenzentralstelle (§ 7 BDSG-E, § 71 f. BKAG-E);

- ferner auf § 57 BDSG-E (Auskunftsrecht), § 58 BDSG-E (Recht auf Berichtigung, Löschung oder Sperrung), § 64 BDSG-E (Anforderungen an die Sicherheit der Datenverarbeitung), §§ 65 f. BDSG-E (Benachrichtigungspflichten bei Rechtsverletzung), §§ 83 BDSG-E, 86 BKAG-E (Recht auf Schadenersatz) (V.5. und V.6.) und §§ 60 f. BDSG-E (Rechtsbehelfe);
- das Gebot einer Datenspeicherung im Hoheitsgebiet der Mitgliedstaaten (Art. 6 Abs. 8 FluggastdatenRL) ist in den FlugDaG-E aufzunehmen (V.8.);

Schließlich sei darauf hingewiesen,

- dass sich aufgrund des Verweises in das allgemeine Datenschutzrecht dort bestehende Streitfragen hinsichtlich der korrekten Umsetzung auch hier stellen [siehe §§ 16, 66 BDSG-E und dazu V.1.j.bb.(2); V.11.];
- dass § 4 Abs. 5 FlugDaG-E aus kompetentiellen Gründen kein Ersuchen der Landeskriminalämter im präventiven Bereich deckt (V.15.).

II. Hintergrund*

Der vorliegende Gesetzentwurf dient der Umsetzung der Richtlinie (EU) 2016/681 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (im Folgenden: FluggastdatenRL)[1]. Die Umsetzung der Richtlinie in nationales Recht hat bis zum 25.5.2018 zu erfolgen. Die Richtlinie verpflichtet Luftfahrtunternehmen, bestimmte Fluggastdaten [Passenger Name Record (PNR)-Daten] an eine nationale Behörde (PNR-Zentralstelle) zu übermitteln, um dieser namentlich einen Abgleich der Daten mit Fahndungsdatenbanken und auf Risikoprofile hin zu ermöglichen. Etwaige Treffer übermittelt die PNR-Zentralstelle nach individueller Überprüfung den für die Bekämpfung terroristischer Straftaten und schwerer Kriminalität zuständigen Behörden. Überdies ist ein Abgleich der (für fünf Jahre zu speichernden, gleichwohl nach sechs Monaten zu depersonalisierenden) Daten auf Ersuchen dieser Behörden möglich.

III. Umsetzung durch den deutschen Gesetzgeber

1. Umsetzungspflicht

Gemäß Art. 288 UAbs. 3 AEUV ist der deutsche Gesetzgeber verpflichtet, die Richtlinie in nationales Recht umzusetzen. Diese Umsetzungspflicht besteht auch dann, wenn Zweifel an der Unionsrechtsmäßigkeit der umzusetzenden Richtlinie bestehen. Bei Nicht- respektive nicht fristgerechter Umsetzung kann die Europäische Kommission ein Vertragsverletzungsverfahren gemäß Art. 258 AEUV einleiten. In diesem kann die Verletzung der Umsetzungspflicht grundsätzlich nicht durch Zweifel an der Unionsrechtskonformität der Richtlinie gerechtfertigt werden.[2] Anderes gilt nur, „wenn der fragliche Rechtsakt mit besonders schweren und offensichtlichen Fehlern behaftet wäre, so daß er als inexistenter Rechtsakt qualifiziert werden könnte."[3]

---

* An der Erstellung der Stellungnahme hat meine wiss. Mitarbeiterin, Frau *Cornelia Kibler, LL.M. (UNC)*, mitgewirkt.

Verweise auf den BDSG-E beziehen sich auf das BDSG i.d.F. des Gesetzentwurfs der Bundesregierung – Entwurf eines Gesetzes zur Anpassung des Datenschutzrehts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), BT-Drs. 18/11325.

Verweise auf den BKAG-E beziehen sich auf das BKAG i.d.F. des Gesetzentwurfs der Fraktionen der CDU/CSU und SPD – Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes, BT-Drs. 18/11163.

1 ABl. 2016 L 119, 132.

2 St. Rspr. EuGH, Rs. C-196/07, Slg. 2008, I-41, Rn. 34 – Kommission/Spanien; Rs. C-177/06, Slg. 2007, I-7689, Rn. 30 – Kommission/Spanien; Rs. C-53/05, Slg. 2006, I-6215, Rn. 30 – Kommission/Portugal; Rs. C-261/99, Slg. 2001, I-2537, Rn. 18 – Kommission/Frankreich; Rs. C-404/00, Slg. 2003, I-6695, Rn. 40 – Kommission/Spanien; Rs. C-74/91, Slg. 1992, I-5437, Rn. 10 – Kommission/Deutschland; Rs. 226/87, Slg. 1988, 3611, Rn. 14 – Kommission/Griechenland. Siehe auch *U. Karpenstein*, in: E. Grabitz/M. Hilf/M. Nettesheim, Das Recht der Europäischen Union, 60. EL 2016, Art. 258 AEUV Rn. 74; *J. Schwarze*, in: ders. (Hrsg.), EU-Kommentar, 3. Aufl. 2012, Art. 258 Rn. 30. Kritisch bei zweifelhafter Grundrechtskonformität *N. Wunderlich/B. Hickl*, EuR 2013, 107, 113 ff.

3 EuGH, Rs. C-74/91, Slg. 1992, I-5437, Rn. 10 – Kommission/Deutschland.

Trotz teils geäußerter Kritik an der Grundrechtskonformität der Fluggastdatenverarbeitung[4] lassen sich auf Basis der EuGH-Rechtsprechung und der Stellungnahmen der Generalanwälte zu den PNR-Abkommen keine derart schweren und offensichtlichen Rechtsverstöße annehmen, die der Umsetzungspflicht entgegengehalten werden könnten (siehe auch unten, IV. und V.).

2. Anwendbares Grundrechtsregime: nationale oder EU-Grundrechte

Das zweistufige Rechtserzeugungsverfahren (Erlass der Richtlinie auf EU-Ebene und Umsetzung der Richtlinie auf nationaler Ebene) zieht eine vielschichtige Grundrechtsbindung nach sich.[5] An den EU-Grundrechten ist nicht nur die Richtlinie selbst als Unionshandeln zu messen, sondern auch die Umsetzung durch den deutschen Gesetzgeber als Akt der „Durchführung des Rechts der Union" (Art. 51 Abs. 1 S. 1 GRC). Dabei nimmt der EuGH eine Grundrechtsbindung der Mitgliedstaaten nicht nur dann an, wenn diese zwingende Vorgaben des Unionsrechts umsetzen, sondern auch dann, wenn die Richtlinie den Mitgliedstaaten Ermessen einräumt.[6] Das Bundesverfassungsgericht verzichtet auf eine Kontrolle von Unionsrechtsakten und der Umsetzung zwingender unionsrechtlicher Vorgaben in das nationale Recht am Maßstab der deutschen Grundrechte, solange ein adäquater Grundrechtsschutz auf EU-Ebene gewährleistet ist (Solange-Vorbehalt, siehe auch Art. 23 Abs. 1 S. 1 GG).[7] Die Inanspruchnahme von Umsetzungsspielräumen durch den deutschen Gesetzgeber unterwirft das Bundesverfassungsgericht indes einer vollumfänglichen Kontrolle an den nationalen Grundrechten.[8] Letzteres, mithin die Parallelanwendung nationaler Grundrechte, erachtet der EuGH für zulässig, „sofern … weder das Schutzniveau der Charta … noch der Vorrang, die Einheit und die Wirksamkeit des Unionsrechts beeinträchtigt werden".[9]

---

4 Siehe etwa *T. Fiedler*, Die Einführung eines europäischen Fluggastdatensystems, 2016, S. 117 ff. Die Grundrechtskonformität demgegenüber **bejahend**: *D. Lowe*, ICLRev. 17 (2017), S. 78.

5 Umfassend dazu nur *F. Wollenschläger*, A. Hatje/P.-C. Müller-Graff (Hrsg.), Enzyklopädie Europarecht, Bd. 1, 1. Aufl. 2013, § 8, Rn. 18 ff.

6 EuGH, Rs. C-540/03, Slg. 2006, I-5769, Rn. 104 f. – Parlament/Rat; ferner verb. Rs. C-411/10 u. C-493/10, Slg. 2011, I-13905, Rn. 64 ff. – N.S. et al.; Rs. C-418/11, EU:C:2013:588, Rn. 70 ff. – Texdata. Näher *F. Wollenschläger*, in: A. Hatje/P.-C. Müller-Graff (Hrsg.), Enzyklopädie Europarecht, Bd. 1, 1. Aufl. 2013, § 8, Rn. 19. Kritisch hinsichtlich der Bindung bei Ermessensspielräumen etwa *T. Kingreen*, in: C. Calliess/M. Ruffert (Hrsg.), EUV/AEUV, 5. Aufl. 2016, Art. 51 GRC Rn. 14 f.

7 Siehe nur BVerfGE 73, 339, 376; ferner NJW 1990, 974, 974; NVwZ 1993, 883, 883; BVerfGE 89, 155, 174 f.; E 118, 79, 95 ff.; E 129, 186, 207 f. Zu jüngst aktivierten Grenzen vor dem Hintergrund der Verfassungsidentität E 140, 317, 334 ff.

8 Siehe nur BVerfGE 125, 260, 308 f.; E 129, 78, 104 f.; E 130, 151, 186 ff.

9 Vgl. EuGH, Rs. C-399/11, EU:C:2013:107, Rn. 60 – Melloni; ferner Rs. C-617/10, EU:C:2013:105, Rn. 29 – Fransson; Gutachten 2/13, EU:C:2014:2454, Rn. 187 f. (Beitritt zur EMRK); Rs. C-168/13, EU:C:2013:358, Rn. 53 – Jeremy F.

Vor diesem Hintergrund ist der Gesetzentwurf, soweit er zwingende Richtlinienvorgaben umsetzt, an den EU-Grundrechten zu messen;[10] soweit der deutsche Gesetzgeber von Umsetzungsspielräumen Gebrauch macht, ist der Gesetzentwurf sowohl an den EU- als auch an den nationalen Grundrechten zu messen.

3. Weitgehende 1:1-Umsetzung des deutschen Gesetzgebers

Wie auch die Gesetzesbegründung betont,[11] stellt der Gesetzentwurf im Wesentlichen eine 1:1-Umsetzung zwingender Richtlinienvorgaben dar. Dies gilt namentlich für die besonders grundrechtssensiblen Aspekte der Pflicht zur anlasslosen Datenübermittlung durch die Fluggesellschaften (Art. 8 FluggastdatenRL/§ 2 FlugDaG-E), der zu übermittelnden Datenkategorien (Art. 3 Nr. 5 i.V.m. Anhang I FluggastdatenRL/§ 2 FlugDaG-E), des Abgleichs mit Mustern (Art. 6 Abs. 3 ff./§ 4 Abs. 2 ff. FluDaG-E), der Speicherdauer (Art. 12 FluggastdatenRL/§ 13 FlugDaG-E) und des behördlichen Datenaustausches (Art. 9 ff. FluggastdatenRL/§§ 6 ff. FlugDaG-E).

Den hinsichtlich seiner Grundrechtsrelevanz bedeutendsten Umsetzungsspielraum nimmt der Gesetzentwurf dadurch in Anspruch, dass er, ebenso wie im Übrigen alle anderen Mitgliedstaaten, von der in Art. 2 FluggastdatenRL eröffneten Möglichkeit Gebrauch macht, auch innereuropäische Flüge (und nicht nur Flüge nach/aus Drittstaaten) in die Fluggastdatenverarbeitung einzubeziehen (siehe § 2 Abs. 3 FlugDaG-E).[12] Ebenfalls eine autonome Entscheidung des Gesetzentwurfs stellt die von der Richtlinie ermöglichte (siehe Erwägungsgrund 33 FluggastdatenRL) Einbeziehung anderer Unternehmen als Luftfahrtunternehmen in die Übermittlungspflicht dar (siehe § 3 FlugDaG-E).

---

10 Die Problematik des Unterschreitens des verfassungsrechtlich geforderten Mindestgrundrechtsstandards (Art. 23 Abs. 1 S. 1 GG) kann hier ausgeklammert bleiben. Zu einer weitergehenden Inanspruchnahme der Kontrollbefugnis: BVerfGE 125, 260, 306 f.: „Die Beschwerdeführer können sich auf die Grundrechte des Grundgesetzes jedoch insoweit berufen, als der Gesetzgeber bei der Umsetzung von Unionsrecht Gestaltungsfreiheit hat, das heißt durch das Unionsrecht nicht determiniert ist … Darüber hinaus sind die Verfassungsbeschwerden vorliegend aber auch insoweit zulässig, als die angegriffenen Vorschriften auf Richtlinienbestimmungen beruhen, die einen zwingenden Inhalt haben. Die Beschwerdeführer machen geltend, dass es der Richtlinie 2006/24/EG an einer gemeinschaftsrechtlichen Kompetenzgrundlage fehle und sie gegen europäische Grundrechtsverbürgungen verstoße. Sie erstreben deshalb unter anderem, ohne dass sie dies angesichts ihrer unmittelbar gegen das Umsetzungsgesetz gerichteten Verfassungsbeschwerden vor den Fachgerichten geltend machen konnten, eine Vorlage durch das Bundesverfassungsgericht an den Europäischen Gerichtshof, damit dieser im Wege der Vorabentscheidung nach Art. 267 AEUV (vormals Art. 234 EGV) die Richtlinie für nichtig erkläre und so den Weg frei mache für eine Überprüfung der angegriffenen Vorschriften am Maßstab der deutschen Grundrechte. Jedenfalls ist auf diesem Weg eine Prüfung der angegriffenen Vorschriften am Maßstab der Grundrechte des Grundgesetzes nach dem Begehren der Beschwerdeführer nicht von vornherein ausgeschlossen."

11 Siehe ausdrücklich BT-Drs. 18/11501, S. 2.

12 So auch ausdrücklich BT-Drs. 18/11501, S. 19.

IV. Grundrechtliche Bewertung der Pflicht zur Speicherung von Fluggastdaten

Die Pflicht der Luftfahrtunternehmen zur Übermittlung von Fluggastdaten an staatliche Stellen und die Verarbeitung dieser Daten durch staatliche Stellen ist in erster Linie an den EU-Grundrechten auf Achtung des Privatlebens (Art. 7 GRC) und auf Schutz der personenbezogenen Daten (Art. 8 GRC) zu messen; die den Luftfahrtunternehmen auferlegten Pflichten sind überdies an der unternehmerischen Freiheit (Art. 16 GRC) zu messen.

Es existiert keine unmittelbar einschlägige Rechtsprechung des EuGH zur Frage, ob und inwieweit die Verarbeitung von Fluggastdaten unionsgrundrechtskonform ist, wohl aber bieten die beiden Urteile des EuGH zur Telekommunikations-Verkehrsdatenspeicherung vom 8.4.2014 bzw. vom 21.12.2016 sowie die Schlussanträge der Generalanwälte *Léger und Mengozzi* vom 22.11.2005 bzw. vom 8.9.2016 zu den Fluggastdatenabkommen mit Drittstaaten Anhaltspunkte (1.). Auf dieser Basis ist festzuhalten, dass kein unionsgrundrechtliches Verbot einer anlasslosen Fluggastdatenverarbeitung besteht (2.), eine Verletzung des Wesensgehalts der Art. 7 f. GRC ausscheidet (3.) und die Fluggastdatenverarbeitung zur Erreichung der mit ihr verfolgten legitimen Ziele (4.) als geeignet (5.) sowie erforderlich (6.) angesehen werden kann. Auch die Angemessenheit, namentlich mit Blick auf Verwendungszwecke, Speicherdauer und erfasste Datenkategorien, lässt sich grundsätzlich bejahen (7.), ebenso wie die Wahrung der materiell- und verfahrensrechtlichen Anforderungen für den Zugang zu den Datenbeständen (8.) sowie die Wahrung der Datensicherheit (9.). Ferner begegnen die Weitergaberegeln keinen durchgreifenden Bedenken (10.). Spezifische Regeln zum Schutz von Berufsgeheimnisträgern erscheinen entbehrlich (11.). Schließlich bestehen mit Blick auf eine Verletzung der unternehmerischen Freiheit relativ weitgehende Möglichkeiten der Inpflichtnahme von Unternehmen zur Datenspeicherung und Übermittlung (12.).

1. Anhaltspunkte in der Rechtsprechung

Es existiert keine unmittelbar einschlägige Rechtsprechung des EuGH zur Frage, ob und inwieweit die Verarbeitung von Fluggastdaten unionsgrundrechtskonform ist.

Indes hat der EuGH in seinem Urteil vom 30.5.2006 das bis dahin bestehende Fluggastdatenabkommen mit den USA für nichtig erklärt.[13] Er hat seine Entscheidung dabei im Wesentlichen auf die Kompetenzwidrigkeit des Abkommens gestützt, die Grundrechtswidrigkeit aber nicht

---

13 EuGH, verb. Rs. C-317/04 u. C-318/04, Slg. 2006, I-4721 – Parlament/Rat und Kommission.

thematisiert.[14] Letztere erörterte GA *Léger* in seinen Schlussanträgen, der einen gerechtfertigten Eingriff in das Grundrecht auf Schutz des Privatlebens annimmt.[15]

Auch ein weiteres, aktuell anhängiges, aber noch nicht entschiedenes Gutachtenverfahren vor dem EuGH[16] betrifft die Zulässigkeit von Fluggastdatenabkommen. Am 8.9.2016 hat GA *Mengozzi* seine Schlussanträge[17] vorgelegt, in denen er neben den – hier nicht relevanten – Kompetenzfragen auch die Unionsgrundrechtskonformität der Flugastdatenspeicherung erörtert.

Zunächst hält er fest, dass die Fluggastdatenverarbeitung einen schweren Eingriff in Art. 7 und Art. 8 GRC darstellt:[18]

> Ohne dass die 19 Kategorien von PNR-Daten, die im Anhang des geplanten Abkommens aufgezählt werden, individuell und abschließend geprüft werden müssen, steht fest, dass sie insbesondere die Identität, die Staatsangehörigkeit und die Anschrift der Fluggäste, sämtliche verfügbaren Kontaktangaben (Wohnadresse, E-Mail-Adresse, Telefon) des Fluggasts, der die Buchung durchgeführt hat, die Informationen über das verwendete Zahlungsmittel, gegebenenfalls einschließlich der Nummer der zur Buchung des Fluges verwendeten Kreditkarte, die Informationen über Gepäck und Reisegewohnheiten der Fluggäste sowie die Informationen über die von diesen aufgrund etwaiger gesundheitlicher Probleme, einschließlich Mobilitätsproblemen, oder besonderer Essenswünsche verlangten zusätzlichen Leistungen betreffen, die u.a. Hinweise auf den Gesundheitszustand eines oder mehrerer Reisenden, auf ihre ethnische Herkunft oder ihre religiösen Überzeugungen geben können.
>
> Diese Daten berühren in ihrer Gesamtheit den Bereich des Privatlebens, ja sogar des Intimlebens, und betreffen unbestreitbar eine oder mehrere „bestimmte oder bestimmbare natürliche Person(en)". Es besteht daher in Anbetracht der Rechtsprechung des Gerichtshofs kein Zweifel daran, dass die systematische Übermittlung der PNR-Daten an die kanadischen Behörden, der Zugang zu diesen Daten, die Nutzung und die Speicherung dieser Daten für eine Dauer von fünf Jahren durch diese Behörden sowie gegebenenfalls ihre Weiterübermittlung an andere Behörden einschließlich solcher anderer Drittländer nach den Bestimmungen des geplanten Abkommens Vorgänge sind, die in den Anwendungsbereich des von Art. 7 der Charta garantierten Grundrechts der Achtung des Privat- und Familienlebens sowie des damit „in engem Zusammenhang [stehenden]", aber dennoch eigenständigen, von Art. 8 Abs. 1 der Charta garantierten Grundrechts auf Schutz personenbezogener Daten fallen und einen Eingriff in diese Grundrechte darstellen.
>
> Der Gerichtshof hat nämlich bereits zu Art. 8 EMRK, auf den sich die Art. 7 und 8 der Charta stützen, entschieden, dass die Weitergabe von personenbezogenen Daten an einen Dritten – in diesem Fall an eine Behörde – ein Eingriff im Sinne dieses Artikels ist und dass die Pflicht der staatlichen Stellen zur Speicherung der Daten sowie der spätere Zugang der zuständigen nationalen Behörden zu den Daten über das Privatleben auch für sich genommen einen Eingriff in die von Art. 7 der Charta garantierten Rechte darstellen. Ebenso greift ein Unionsrechtsakt, der jegliche Form der Verarbeitung personenbezogener Daten vorsieht, in das Grundrecht auf Schutz solcher Daten nach Art. 8 der Charta ein … Die Rechtmäßigkeit eines solchen Rechtsakts ist nämlich von der Achtung der in der Unionsrechtsordnung geschützten Grundrechte abhängig, insbesondere der durch die Art. 7 und 8 der Charta garantierten.
>
> Auf den … Umstand, dass die vom geplanten Abkommen betroffenen Personen oder zumindest der überwiegende Teil von ihnen durch den Eingriff keine Nachteile erlitten, kommt es für die Feststellung des Vorliegens eines solchen Eingriffs nicht an.

---

14 EuGH, verb. Rs. C-317/04 u. C-318/04, Slg. 2006, I-4721, Rn. 69 f. – Parlament/Rat und Kommission.

15 GA Léger, in: EuGH, verb. Rs. C-317/04 u. C-318/04, Slg. 2006, I-4721, Rn. 238 f. – Parlament/Rat und Kommission.

16 EuGH, Gutachten 1/15.

17 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656.

18 So auch die die Ausarbeitung der Wissenschaftlichen Dienste des Bundestags zur Vereinbarkeit des Richtlinienentwurfs über die Verwendung von Fluggastdaten mit der Europäischen Grundrechtecharta vom 10. März 2011, WD 11 – 3000 – 26/11, S. 7.

Desgleichen ist es nicht relevant, dass die Möglichkeit besteht, dass die übermittelten Informationen oder zumindest die Mehrheit von ihnen keinen sensiblen Charakter haben.

Im Übrigen weise ich darauf hin, dass sich die Vertragsparteien über den Eingriff, den die Übermittlung, die Nutzung, die Speicherung und die Weiterübermittlung der PNR-Daten nach dem geplanten Abkommen bedeuten, völlig im Klaren sind, weil das Abkommen, wie aus seiner Präambel ausdrücklich hervorgeht, gerade aufgrund dieses Eingriffs die Erfordernisse der öffentlichen Sicherheit und die der Achtung der Grundrechte auf Schutz der Privatsphäre und auf Datenschutz miteinander in Einklang zu bringen versucht.

Zwar kann das Bemühen der Vertragsparteien um einen solchen Ausgleich die Intensität oder die Schwere des mit dem geplanten Abkommen verbundenen Eingriffs in die durch die Art. 7 und 8 der Charta garantierten Grundrechte verringern.

Der … Eingriff ist jedoch von einem gewissen Ausmaß und einer nicht zu vernachlässigenden Schwere. Zum einen betrifft er nämlich systematisch alle Fluggäste, die von den Flugverbindungen zwischen Kanada und der Europäischen Union Gebrauch machen, d.h. mehrere Dutzend Millionen Menschen pro Jahr. Zum anderen ist, wie die meisten Beteiligten bestätigt haben, ganz offensichtlich, dass die Übermittlung großer Mengen personenbezogener Daten der Fluggäste, darunter auch sensibler Daten, die zwangsläufig einer automatisierten Verarbeitung unterzogen werden müssen, sowie die Speicherung dieser Daten für einen Zeitraum von fünf Jahren, es ermöglichen sollen, diese Daten – gegebenenfalls retrospektiv – mit im Voraus festgelegten Mustern von „risikobehaftetem“ oder „besorgniserregendem“ Verhalten im Zusammenhang mit terroristischen Handlungen und/oder grenzübergreifender schwerer Kriminalität zu vergleichen, um Personen zu identifizieren, die der Polizei bis dahin unbekannt waren oder von ihr nicht verdächtigt wurden. Diese Merkmale, die offensichtlich in der Natur der … PNR-Regelung begründet liegen, können jedoch den fatalen Eindruck vermitteln, dass alle betroffenen Reisenden zu möglichen Verdächtigen gemacht werden …

[D]as geplante Abkommen [ist] … mit einem schweren Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte verbunden. Um zulässig zu sein, muss dieser Eingriff gerechtfertigt sein.[19]

Die Fluggastdatenverarbeitung kann dennoch mit Art. 16 AEUV sowie Art. 7, Art. 8 und Art. 52 Abs. 1 der GRC vereinbar sein, wenn bestimmte Voraussetzungen erfüllt sind:

Weder das Recht auf Achtung des Privat- und Familienlebens noch das auf Schutz personenbezogener Daten sind absolute Rechte.

So lässt Art. 52 Abs. 1 der Charta Einschränkungen der Ausübung der Rechte wie derjenigen zu, die in ihren Art. 7 und 8 Abs. 1 verankert sind, sofern diese Einschränkungen gesetzlich vorgesehen sind, den Wesensgehalt dieser Rechte achten und unter Wahrung des Grundsatzes der Verhältnismäßigkeit notwendig sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.[20]

Im Einzelnen hat GA *Mengozzi* folgende Voraussetzungen formuliert:[21]

– Die Kategorien von Fluggastdatensätzen (PNR) der Fluggäste im Anhang des geplanten Abkommens werden klar und präzise formuliert und die sensiblen Daten im Sinne des geplanten Abkommens vom Anwendungsbereich des Abkommens ausgeschlossen;

– die Straftaten, die unter die Definition der grenzübergreifenden schweren Kriminalität nach Art. 3 Abs. 3 des geplanten Abkommens fallen, werden in diesem oder einem Anhang zum Abkommen abschließend aufgezählt;

– das geplante Abkommen bestimmt die für die Verarbeitung von Fluggastdatensätzen zuständige Behörde hinreichend klar und präzise, um den Schutz und die Sicherheit dieser Daten zu gewährleisten;

– das geplante Abkommen bestimmt ausdrücklich die Grundsätze und Vorschriften, die auf die im Voraus festgesetzten Szenarien oder Beurteilungskriterien sowie die Datenbanken, mit denen die Fluggastdatensätze mittels automatisierter Verarbeitung dieser Daten abgeglichen werden, anwendbar sind, so dass die Anzahl der als „Ziel“ erfassten Personen weitgehend und nicht diskriminierend auf diejenigen beschränkt

---

19 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 169 ff.

20 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 181 f.

21 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 328.

werden kann, denen gegenüber ein begründeter Verdacht der Beteiligung an einer terroristischen Straftat oder grenzübergreifender schwerer Kriminalität besteht;

– das geplante Abkommen legt fest, dass nur die Bediensteten der zuständigen kanadischen Behörde zum Zugang zu den Fluggastdatensätzen befugt sind, und sieht objektive Kriterien vor, die es ermöglichen, die Anzahl dieser Bediensteten konkret zu bestimmen;

– das geplante Abkommen gibt substantiiert die objektiven Gründe an, aus denen die Speicherung aller Fluggastdatensätze der Fluggäste für einen Zeitraum von höchstens fünf Jahren erforderlich ist;

– für den Fall, dass die Dauer der Speicherung der Fluggastdatensätze von höchstens fünf Jahren als erforderlich angesehen wird, stellt das geplante Abkommen eine „Anonymisierung" durch Unkenntlichmachung aller PNR-Daten sicher, anhand deren ein Fluggast unmittelbar identifiziert werden kann;

– das geplante Abkommen macht die Prüfung der zuständigen kanadischen Behörde betreffend das von anderen kanadischen Staatsbehörden oder Staatsbehörden von Drittländern gewährleistete Schutzniveau sowie die etwaige Entscheidung über die Weitergabe der Fluggastdatensätze an diese Behörden im Einzelfall von einer Vorabkontrolle durch eine unabhängige Behörde oder ein Gericht abhängig;

– die Absicht, Fluggastdatensätze eines Staatsangehörigen eines Mitgliedstaats der Union an eine andere kanadische Staatsbehörde oder eine Staatsbehörde eines Drittlands zu übermitteln, ist vor jeder tatsächlichen Übermittlung der zuständigen Behörde des fraglichen Mitgliedstaats und/oder der Kommission im Voraus mitzuteilen;

– das geplante Abkommen garantiert durch eine klare und präzise Regel planmäßig eine Überwachung der Achtung des Privatlebens und des Schutzes personenbezogener Daten der Fluggäste, deren Fluggastdatensätze verarbeitet werden, durch eine unabhängige Stelle im Sinne von Art. 8 Abs. 3 der Charta der Grundrechte der Europäischen Union und

– das geplante Abkommen bestimmt klar, dass die Anträge auf Zugang, auf Berichtigung und auf Anbringung eines Bestreitungsvermerks von Fluggästen, die sich nicht im kanadischen Hoheitsgebiet aufhalten, entweder unmittelbar oder im Wege eines verwaltungsrechtlichen Rechtsbehelfs vor eine unabhängige Behörde gebracht werden können.

Eine Unionsgrundrechtswidrigkeit des PNR-Abkommens mit Kanada nimmt GA *Mengozzi* an, soweit

– Art. 3 Abs. 5 des geplanten Abkommens über das, was unbedingt erforderlich ist, hinaus gestattet, die Möglichkeiten der Verarbeitung von Fluggastdatensätzen unabhängig von dem in Art. 3 dieses Abkommens genannten Zweck der Verhinderung und Aufdeckung von terroristischen Straftaten und grenzübergreifender schwerer Kriminalität zu erweitern;

– Art. 8 des geplanten Abkommens die Verarbeitung, die Nutzung und die Speicherung von Fluggastdatensätzen, die sensible Daten enthalten, durch Kanada vorsieht;

– Art. 12 Abs. 3 des geplanten Abkommens Kanada über das, was unbedingt erforderlich ist, hinaus das Recht gewährt, jede Information offenzulegen, sofern es angemessene rechtliche Anforderungen und Beschränkungen einhält;

– Art. 16 Abs. 5 des geplanten Abkommens Kanada gestattet, die Fluggastdatensätze für einen Zeitraum von höchstens fünf Jahren insbesondere für eine besondere Maßnahme, Überprüfung, Untersuchung oder ein Gerichtsverfahren zu speichern, ohne dass ein Zusammenhang mit dem in Art. 3 dieses Abkommens genannten Zweck der Verhinderung und Aufdeckung von terroristischen Straftaten und grenzübergreifender schwerer Kriminalität erforderlich ist, und

– Art. 19 des geplanten Abkommens die Übermittlung von Fluggastdatensätzen an eine Staatsbehörde eines Drittlands erlaubt, ohne dass die zuständige kanadische Behörde von einer unabhängigen Stelle überwacht wird und sich zuvor vergewissert hat, dass die Staatsbehörde des fraglichen Drittlands diese Daten nicht selbst an eine andere Einheit, gegebenenfalls in einem anderen Drittland, weiter übermitteln kann.

Inwieweit der EuGH sind dem anschließt, bleibt freilich abzuwarten. Überdies ist zu berücksichtigen, dass das Gutachtenverfahren die Datenübermittlung an einen Drittstaat (Kanada) betrifft, nicht aber an mitgliedstaatliche Behörden.

(Strenge) Anforderungen für die anlasslose Datenverarbeitung hat der EuGH in seinen beiden Urteilen zur Telekommunikations-Verkehrsdatenspeicherung formuliert, nämlich im Urteil vom 8.4.2014 (*Digital Rights Ireland u.a.*),[22] das die Gültigkeit der Vorratsdatenspeicherungs-Richtlinie 2006/24/EG betraf,[23] sowie im Urteil vom 21.12.2016 (*Tele2 Sverige u.a.*),[24] das die Vereinbarkeit nationaler Vorgaben zur Verkehrsdatenspeicherung mit europäischem Recht thematisierte.

Dass diese Urteile ohne Weiteres auf die anlasslose Verarbeitung von Fluggastdaten übertragbar sind, ist aufgrund der unterschiedlichen Eingriffsintensität der jeweiligen Maßnahmen abzulehnen.[25] So ist zu berücksichtigen, dass die (anlasslose) Verarbeitung von PNR-Daten einen weniger intensiven Eingriff in das Privatleben darstellt als diejenige von TK-Verkehrsdaten, da die Streubreite des Eingriffs und die Aussagekraft der Daten geringer ist. So werden Flugbuchungen in der Regel seltener vorgenommen. Zudem sind die jeweiligen Eingriffe in das Privatleben auf eine isolierte Tätigkeit – das Fliegen – und eine isolierte Personengruppe – Fluggäste – beschränkt, so dass kein Gefühl erzeugt wird, „dass [das] Privatleben Gegenstand einer ständigen Überwachung ist."[26] Auch GA *Mengozzi* hat betont, dass der mit der Fluggastdatenverarbeitung „verbundene Eingriff weniger weitreichend als der von der Richtlinie 2006/24 vorgesehene [TK-Verkehrsdatenspeicherung]" ist „und … sich auch weniger stark auf das tägliche Leben jedes Einzelnen aus[wirkt]".[27]

2. Kein unionsgrundrechtliches Verbot einer anlasslosen Fluggastdatenverarbeitung

Die Regelungen zur Fluggastdatenverarbeitung sehen eine anlasslose Pflicht zur Datenübermittlung an staatliche Stellen vor, die jeden Passagier unabhängig von einer spezifischen Verbindung zu terroristischen Straftaten und schwerer Kriminalität erfasst. Dies begründet eine

---

22 EuGH, verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238 – Digital Rights Ireland u.a.

23 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15.3.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. 2006 L 105, 54.

24 EuGH, verb. Rs. C-203/15 u. C-698/15, EU:C:2016:970 – Tele2 Sverige u.a.

25 Vgl. für eine grundsätzliche Übertragbarkeit: Rechtsausschuss des Deutschen Bundesrates in seiner Empfehlung zum Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG) vom 20.03.2017, BR-Drs. 161/1/17. Ebenso: Gutachten des Juristischen Dienstes des Europäischen Parlaments vom 22. Dezember 2014 („LIBE – Questions relating to the judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and others – Directive 2006/24/EC on data retention – Consequences of the judgment"), abrufbar unter: http://www.statewatch.org/news/2015/apr/ep-ls-opinion-digital-rights-judgment.pdf (6.4.2017), Rn. 63. Differenzierend: *M. Haller*, SIAK-Journal 2016, 86, 95 f.

26 EuGH, verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238, Rn. 37 – Digital Rights Ireland u.a. So auch *M. Haller*, SIAK-Journal 2016, 86, 96.

27 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 240.

erhebliche Streubreite der Datenverarbeitung. In seinen Urteilen zur TK-Verkehrsdatenspeicherung hat der EuGH diese Anlasslosigkeit der Datenverarbeitung problematisiert, wobei sich das Urteil in der Rs. *Tele2 Sverige u.a.* besonders streng liest:

Zudem kann zwar die Wirksamkeit der Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen; eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht, für die Kriminalitätsbekämpfung nicht rechtfertigen …

Eine solche Regelung hat zum einen in Anbetracht ihrer in Rn. 97 des vorliegenden Urteils beschriebenen charakteristischen Merkmale zur Folge, dass die Vorratsspeicherung der Verkehrs- und Standortdaten die Regel ist, obwohl nach dem mit der Richtlinie 2002/58 geschaffenen System die Vorratsspeicherung von Daten die Ausnahme zu sein hat.

Zum anderen sieht eine nationale Regelung wie die im Ausgangsverfahren, die sich allgemein auf alle Teilnehmer und registrierten Nutzer erstreckt und alle elektronischen Kommunikationsmittel sowie sämtliche Verkehrsdaten erfasst, keine Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel vor. Sie betrifft pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich diese Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Zudem sieht sie keine Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen …

Eine solche Regelung verlangt keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit. Insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung von Straftaten beitragen könnten …

Eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende überschreitet somit die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta verlangt.

Hingegen untersagt Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta einem Mitgliedstaat nicht, eine Regelung zu erlassen, die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist.

Um den in der vorstehenden Randnummer des vorliegenden Urteils genannten Erfordernissen zu genügen, muss die betreffende nationale Regelung erstens klare und präzise Regeln über die Tragweite und die Anwendung einer solchen Maßnahme der Vorratsdatenspeicherung vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf, um so zu gewährleisten, dass eine derartige Maßnahme auf das absolut Notwendige beschränkt wird …

Zweitens können sich die materiellen Voraussetzungen, die eine nationale Regelung, die im Rahmen der Bekämpfung von Straftaten vorbeugend die Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, erfüllen muss, um zu gewährleisten, dass sie auf das absolut Notwendige beschränkt wird, zwar je nach den zur Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten getroffenen Maßnahmen unterscheiden, doch muss die Vorratsspeicherung der Daten stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Voraussetzungen müssen insbesondere in der Praxis geeignet sein, den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen.

Bei der Begrenzung einer solchen Maßnahme im Hinblick auf die potenziell betroffenen Personenkreise und Situationen muss sich die nationale Regelung auf objektive Anknüpfungspunkte stützen, die es ermöglichen, Perso-

nenkreise zu erfassen, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern. Eine solche Begrenzung lässt sich durch ein geografisches Kriterium gewährleisten, wenn die zuständigen nationalen Behörden aufgrund objektiver Anhaltspunkte annehmen, dass in einem oder mehreren geografischen Gebieten ein erhöhtes Risiko besteht, dass solche Taten vorbereitet oder begangen werden.

In Anbetracht all dessen ist auf die erste Frage in der Rechtssache C-203/15 zu antworten, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht.[28]

Ob demnach eine anlasslose TK-Verkehrsdatenspeicherung per se unionsgrundrechtswidrig ist,[29] bedarf hier keiner abschließenden Beurteilung. Denn die strengen Standards aus dem Kontext der TK-Verkehrsdatenspeicherung, die aus deren besonderer Eingriffsintensität (Streubreite und Aussagekraft der Daten) resultieren, lassen sich nicht unbesehen auf die Fluggastdatenverarbeitung übertragen. GA *Mengozzi* hat dies nicht nur in seinen Schlussanträgen zum PNR-Abkommen betont (siehe soeben IV.1.), sondern auch keine (anlassbezogene) Beschränkung des persönlichen Anwendungsbereichs für erforderlich erachtet:

Wie ich allerdings bereits … dargelegt habe, liegt die Bedeutung der PNR-Regelungen gerade in der Garantie der massenhaften Übermittlung von Daten, die den zuständigen Behörden erlaubt, mit Hilfe von Instrumenten zur automatisierten Verarbeitung und im Voraus festgelegter Szenarien oder Kriterien Personen zu identifizieren, die den Strafverfolgungsbehörden bis dahin unbekannt waren, aber für die öffentliche Sicherheit von „Interesse" sein oder eine Gefahr darstellen könnten, und daher später eingehenderen individuellen Kontrollen unterzogen werden können. Diese Kontrollen müssen auch während eines bestimmten Zeitraums, nachdem die fraglichen Fluggäste gereist sind, erfolgen können.

Außerdem machen, anders als die Personen, deren Daten Gegenstand der von der Richtlinie 2006/24 vorgesehenen Verarbeitung waren, alle Personen, die unter das geplante Abkommen fallen, freiwillig von einem internationalen Transportmittel für die Reise in ein oder aus einem Drittland Gebrauch, wobei dieses Transportmittel selbst leider immer wieder Mittel oder Ziel terroristischer Handlungen oder grenzübergreifender schwerer Kriminalität ist, was den Erlass von Maßnahmen erfordert, die ein hohes Sicherheitsniveau für sämtliche Fluggäste gewährleisten.

Zwar ist eine Regelung der Übermittlung und Verarbeitung von PNR-Daten vorstellbar, die die Fluggäste z. B. nach geografischen Herkunftsgebieten (im Fall der Zwischenlandung in der Union) oder nach ihrem Alter unterscheidet, wobei z. B. Minderjährige von vornherein ein geringeres Risiko für die öffentliche Sicherheit darstellen könnten. Sofern in ihnen keine verbotene Diskriminierung gesehen werden kann, bestände bei solchen Maßnahmen, sobald sie bekannt wären, jedoch die Gefahr, dass die Bestimmungen des geplanten Abkommens umgangen würden, was jedenfalls die wirksame Erreichung eines seiner Ziele beeinträchtigte.

Wie ich bereits ausgeführt habe, ist es nicht hinreichend, abstrakt Alternativmaßnahmen zu ersinnen, die die Grundrechte weniger stark einschränken. Diese Maßnahmen müssen meiner Ansicht nach auch Garantien aufweisen, dass sie ebenso wirksam sind wie die Maßnahmen, die zur Bekämpfung terroristischer Straftaten und grenzübergreifender schwerer Kriminalität eingeführt werden sollen. Dem Gerichtshof ist im Rahmen des vorliegenden

---

[28] EuGH, verb. Rs. C-203/15 u. C-698/15, EU:C:2016:970, Rn. 103 ff. – Tele2 Sverige u.a. Das Urteil in der Rs. Digital Rights Ireland u.a. vom 8.4.2014, verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238, ist demgegenüber offener formuliert, siehe dazu *F. Wollenschläger*, Stellungnahme zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (BT-Drs. 18/5088, 18/5171 und 18/4971) im Rahmen der Expertenanhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages am 21.9.2015, S. 30 ff., abrufbar unter https://www.bundestag.de/blob/388296/77e18af13306be0d15e1b9fe9c002d33/wollenschlaeger-data.pdf (21.4.2017).

[29] So etwa *R. Priebe*, EuZW 2017, 136, 138; *A. Roßnagel*, NJW 2017, 696, 697 f.; mit Bedenken hinsichtlich der Praktikabilität *A. Sandhu*, EuR 2017, 420 i.E. A.A. *W. Bär*, NZWiSt 2017, 81, 86; *L. Woods*, Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber), abrufbar unter: http://eulawanalysis.blogspot.de/2016/12/data-retention-and-national-law-ecj.html (13.4.2017).

Verfahrens keine andere Maßnahme mitgeteilt worden, die die Anzahl der Personen beschränkt, deren PNR-Daten durch die zuständige kanadische Behörde einer automatisierten Verarbeitung unterzogen werden, gleichzeitig aber ebenso wirksam das von den Vertragsparteien verfolgte Ziel der öffentlichen Sicherheit erreichen könnte.

Alles in allem kann daher nach meiner Ansicht allgemein der persönliche Anwendungsbereich des geplanten Abkommens nicht weiter eingegrenzt werden, ohne den Zweck der PNR-Regelungen selbst zu beeinträchtigen.[30]

Schließlich ist festzuhalten, dass die Richtlinie die anlasslose Fluggastdatenverarbeitung zwingend vorgibt, so dass insoweit eine Umsetzungspflicht besteht (vgl. dazu III.1.).

3. Wahrung des Wesensgehalts (Art. 52 Abs. 1 S. 1 GRC)

Der Gerichtshof der Europäischen Union stellte in seiner Entscheidung zur Vorratsdatenspeicherungsrichtlinie zunächst fest, dass die anlasslose vorsorgliche Speicherung von Verkehrsdaten keinen Eingriff in den unantastbaren Wesensgehalt der Art. 7 f. GRC darstellt:

Zum Wesensgehalt des Grundrechts auf Achtung des Privatlebens und der übrigen in Art. 7 der Charta verankerten Rechte ist festzustellen, dass die nach der Richtlinie 2006/24 vorgeschriebene Vorratsspeicherung von Daten zwar einen besonders schwerwiegenden Eingriff in diese Rechte darstellt, doch nicht geeignet ist, ihren Wesensgehalt anzutasten, da die Richtlinie, wie sich aus ihrem Art. 1 Abs. 2 ergibt, die Kenntnisnahme des Inhalts elektronischer Kommunikation als solchen nicht gestattet.

Die Vorratsspeicherung von Daten ist auch nicht geeignet, den Wesensgehalt des in Art. 8 der Charta verankerten Grundrechts auf den Schutz personenbezogener Daten anzutasten, weil die Richtlinie 2006/24 in ihrem Art. 7 eine Vorschrift zum Datenschutz und zur Datensicherheit enthält, nach der Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten bzw. Betreiber eines öffentlichen Kommunikationsnetzes, unbeschadet der zur Umsetzung der Richtlinien 95/46 und 2002/58 erlassenen Vorschriften, bestimmte Grundsätze des Datenschutzes und der Datensicherheit einhalten müssen. Nach diesen Grundsätzen stellen die Mitgliedstaaten sicher, dass geeignete technische und organisatorische Maßnahmen getroffen werden, um die Daten gegen zufällige oder unrechtmäßige Zerstörung sowie zufälligen Verlust oder zufällige Änderung zu schützen.[31]

Einen Eingriff in den unantastbaren Wesensgehalt der Art. 7 f. GRC hat auch GA *Mengozzi* für die Fluggastdatenverarbeitung verneint:

Sodann wurde vor dem Gerichtshof nicht geltend gemacht und kann es meines Erachtens auch nicht, dass der im geplanten Abkommen enthaltene Eingriff den „Wesensgehalt" im Sinne von Art. 52 Abs. 1 der Charta der in deren Art. 7 und Art. 8 Abs. 1 verankerten Grundrechte beeinträchtigen

Zum einen erlaubt nämlich die Art der PNR-Daten, die Gegenstand des geplanten Abkommens sind, keine genauen Schlüsse auf den Wesensgehalt des Privatlebens der betroffenen Personen. Sie beziehen sich lediglich auf die Flugreisegewohnheiten …. Überdies sieht das geplante Abkommen in seinen Art. 8, 16, 18 und 19 eine Reihe von Garantien betreffend die Unkenntlichmachung und die schrittweise Anonymisierung der PNR-Daten vor, … was im Wesentlichen den Schutz des Privatlebens sicherstellen soll.

Zum anderen ist, was den Wesensgehalt des Schutzes personenbezogener Daten betrifft, darauf hinzuweisen, dass nach Art. 9 des geplanten Abkommens Kanada u. a. „für den Schutz, die Sicherheit, die Vertraulichkeit und die Integrität der Daten [sorgen]" sowie „regulatorische, verfahrensrechtliche oder technische Maßnahmen [ergreifen muss], um PNR-Daten vor Verarbeitung oder Verlust zu schützen und den Zugriff darauf zu verhindern, wenn dies versehentlich, unrechtmäßig oder ohne Befugnis geschieht". Weiter müssen bei jedem Verstoß gegen die Datensicherheit wirksame und abschreckende Korrekturmaßnahmen ergriffen werden können, zu denen auch Strafen gehören können.[32]

---

30 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 241 ff.

31 EuGH, verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238, Rn. 39 f. – Digital Rights Ireland u.a.

32 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 185 ff.

4. Legitimer Zweck

Sowohl die Bekämpfung des Terrorismus als auch der schweren Kriminalität stellen, wie auch GA *Mengozzi* betont hat, legitime Ziele dar, die eine Einschränkung des Datenschutzgrundrechts rechtfertigen können.[33]

5. Eignung

Der Gerichtshof hat keine Zweifel an der Eignung der anlasslosen TK-Verkehrsdatenspeicherung, schwere Kriminalität zu bekämpfen und somit zur Wahrung der öffentlichen Sicherheit beizutragen, angemeldet:

> Zu der Frage, ob die Vorratsspeicherung der Daten zur Erreichung des mit der Richtlinie 2006/24 verfolgten Ziels geeignet ist, ist festzustellen, dass angesichts der wachsenden Bedeutung elektronischer Kommunikationsmittel die nach dieser Richtlinie auf Vorrat zu speichernden Daten den für die Strafverfolgung zuständigen nationalen Behörden zusätzliche Möglichkeiten zur Aufklärung schwerer Straftaten bieten und insoweit daher ein nützliches Mittel für strafrechtliche Ermittlungen darstellen. Die Vorratsspeicherung solcher Daten kann somit als zur Erreichung des mit der Richtlinie verfolgten Ziels geeignet angesehen werden.
>
> Diese Beurteilung kann nicht durch den … Umstand in Frage gestellt werden, dass es mehrere elektronische Kommunikationsweisen gebe, die nicht in den Anwendungsbereich der Richtlinie 2006/24 fielen oder die eine anonyme Kommunikation ermöglichten. Dieser Umstand vermag zwar die Eignung der in der Vorratsspeicherung der Daten bestehenden Maßnahme zur Erreichung des verfolgten Ziels zu begrenzen, führt aber, wie der Generalanwalt in Nr. 137 seiner Schlussanträge ausgeführt hat, nicht zur Ungeeignetheit dieser Maßnahme.[34]

Ebenso hat GA *Mengozzi* die Eignung der Passagierdatenverarbeitung zur Föderung des legitimen Interesses, Terrorismus und schwere Kriminalität zu bekämpfen, angemeldet:

> [Ich] denke …, dass nichts wirklich dagegen spricht, anzuerkennen, dass der mit dem geplanten Abkommen verbundene Eingriff zur Erreichung des von ihm verfolgten Ziels der öffentlichen Sicherheit, insbesondere der Bekämpfung des Terrorismus und der grenzübergreifenden schweren Kriminalität, geeignet ist. Wie nämlich insbesondere die Regierung des Vereinigten Königreichs und die Kommission geltend gemacht haben, bietet die Übermittlung von PNR-Daten zum Zweck einer Analyse und Speicherung … zusätzliche Möglichkeiten zur Erkennung von bis dahin unbekannten und nicht verdächtigten Fluggästen, die Verbindungen zu anderen, in ein Terroristennetz einbezogenen oder an grenzübergreifender schwerer Kriminalität beteiligten Personen und/oder Fluggästen haben könnten. Diese Daten stellen, wie die von der Regierung des Vereinigten Königreichs und der Kommission übermittelten Statistiken über die frühere Praxis der kanadischen Behörden veranschaulichen, nützliche Mittel für strafrechtliche Ermittlungen dar, die insbesondere im Hinblick auf die vom geplanten Abkommen geschaffene polizeiliche Zusammenarbeit auch zur Verhinderung und Aufdeckung einer terroristischen Straftat oder grenzübergreifender schwerer Kriminalität innerhalb der Union beitragen können.[35]

---

33 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 194. Siehe zum hohen Gewicht der Terrorismusbekämpfung auch BVerfGE 133, 277, 333 f.: „das große Gewicht einer effektiven Bekämpfung des Terrorismus für die demokratische und freiheitliche Ordnung zu berücksichtigen. Straftaten mit dem Gepräge des Terrorismus, wie sie das Antiterrordateigesetz zum Bezugspunkt hat (siehe oben D. III. 1.), zielen auf eine Destabilisierung des Gemeinwesens und umfassen hierbei in rücksichtsloser Instrumentalisierung anderer Menschen Angriffe auf Leib und Leben beliebiger Dritter. Sie richten sich gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes. Es ist Gebot unserer verfassungsrechtlichen Ordnung, solche Angriffe nicht als Krieg oder als Ausnahmezustand aufzufassen, die von der Beachtung rechtsstaatlicher Anforderungen dispensieren, sondern sie als Straftaten mit den Mitteln des Rechtsstaats zu bekämpfen. Dem entspricht umgekehrt, dass der Terrorismusbekämpfung im rechtsstaatlichen Rahmen der Verhältnismäßigkeitsabwägung ein erhebliches Gewicht beizumessen ist“. Siehe ferner BVerfG, NJW 2016, 1781, 1783, Rn. 96.

34 EuGH, verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238, Rn. 41 f. – Digital Rights Ireland u.a.

35 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 205.

Hinzuweisen ist schließlich darauf, dass Art. 19 FluggastdatenRL eine Evaluationspflicht statuiert.

6. Erforderlichkeit

Das Gebot der Erforderlichkeit eines Grundrechtseingriffs verlangt, bei Vorhandensein gleich geeigneter Handlungsoptionen das mildeste Mittel zu wählen.[36] Wie im Kontext der TK-Verkehrsdatenspeicherung ist die einzelfallbezogene Speicherung von Passagierdaten bei Vorliegen eines konkreten Anlasses zwar eine mildere, aber keine ebenso effektive Maßnahme, wie auch GA *Mengozzi* in seinem Schlussantrag vom 8.9.2016 ausgeführt hat: So

> ist es nicht hinreichend, abstrakt Alternativmaßnahmen zu ersinnen, die die Grundrechte weniger stark einschränken. Diese Maßnahmen müssen meiner Ansicht nach auch Garantien aufweisen, dass sie ebenso wirksam sind wie die Maßnahmen, die zur Bekämpfung terroristischer Straftaten und grenzübergreifender schwerer Kriminalität eingeführt werden sollen. Dem Gerichtshof ist im Rahmen des vorliegenden Verfahrens keine andere Maßnahme mitgeteilt worden, die die Anzahl der Personen beschränkt, deren PNR-Daten durch die zuständige kanadische Behörde einer automatisierten Verarbeitung unterzogen werden, gleichzeitig aber ebenso wirksam das von den Vertragsparteien verfolgte Ziel der öffentlichen Sicherheit erreichen könnte.
>
> Alles in allem kann daher nach meiner Ansicht allgemein der persönliche Anwendungsbereich des geplanten Abkommens nicht weiter eingegrenzt werden, ohne den Zweck der PNR-Regelungen selbst zu beeinträchtigen.[37]

Hinzuweisen ist schließlich darauf, dass Art. 19 FluggastdatenRL eine Evaluationspflicht statuiert.

7. Angemessenheit

a) Verwendungszwecke

In seinen Urteilen zur Vorratsdatenspeicherung hat der EuGH eine Beschränkung der Verwendungszwecke auf die „Bekämpfung schwerer Straftaten" verlangt.[38] Die FluggastdatenRL gestattet eine Datenverarbeitung nur zur Bekämpfung von „terroristischen Straftaten" und „schwerer Kriminalität" (vgl. Art. 1 Abs. 2 und Art. 6 Abs. 2).

Art. 3 Nr. 8 und Nr. 9 der FluggastdatenRL definieren, was unter „terroristischen Straftaten" und „schwerer Kriminalität" iSd Richtlinie zu verstehen ist:

> 8. „terroristische Straftaten" die nach nationalem Recht strafbaren Handlungen im Sinne der Artikel 1 bis 4 des Rahmenbeschlusses 2002/475/JI;
>
> 9. „schwere Kriminalität" die in Anhang II aufgeführten strafbaren Handlungen, die nach dem nationalen Recht eines Mitgliedstaats mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind;

---

[36] EuGH, Rs. 265/87, Slg. 1989, 2237, Rn. 21 – Schräder u.a.; verb. Rs. C-184/02 u. C-223/02, Slg. 2004, I-7789, Rn. 57 – Spanien und Finnland/Parlament und Rat; *F. Wollenschläger*, in: A. Hatje/P.-C. Müller-Graff (Hrsg.), Enzyklopädie Europarecht, Bd. 1, 1. Aufl. 2013, § 8, Rn. 73.

[37] GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 244 f.

[38] Siehe nur EuGH, verb. Rs. C-203/15 u. C-698/15, EU:C:2016:970, Rn. 115 – Tele2 Sverige u.a.

In Anhang II der Richtlinie ist eine abschließende Liste dieser strafbaren Handlungen zu finden.[39]

Die notwendige Eingriffsschwelle ist vorliegend prinzipiell gewahrt. Bei der Alternative schwere Kriminalität stellt die Kombination aus Mindesthöchstmaß und Listung gewichtiger strafbarer Handlungen einen entsprechenden Schweregrad sicher; allein die Einbeziehung aller Betrugstaten erscheint sehr weitgehend, ebenso das Fehlen einer Erheblichkeitsschwelle im Einzelfall (zur Korrekturmöglichkeit im Umsetzungskontext unten, V.4.a; siehe ferner zur Aufgabe der Beschränkung für Strafverfolgungsbehörden V.9.).

Zudem muss der Unionsrechtsakt objektive Kriterien vorsehen, um eine entsprechende Beschränkung des Zugriffs auf Fälle schwerer Straftaten zu ermöglichen; nicht genügt hat der bloße Verweis in Art. 1 Abs. 1 RL 2006/24/EG auf die Verfolgung „schwere[r] Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden".[40] Auch diese Voraussetzung ist erfüllt, da die FluggastdatenRL, im Gegensatz zur beanstandeten Richtlinie 2006/24/EG, objektive Kriterien zur Bestimmung dieser Straftaten aufstellt.

Dass dies den unionsrechtlichen Anforderungen genügt, hat GA *Mengozzi* zunächst betont:

> Zunächst bin ich der Meinung, dass anders als im Fall des in der Rechtssache Digital Rights Ireland u. a. … in Rede stehenden Rechtsakts Art. 3 des geplanten Abkommens objektive Kriterien vorsieht, die die Natur und den Schweregrad der Straftaten betreffen, die den kanadischen Behörden die Verarbeitung der PNR-Daten gestatten. So ist die terroristische Straftat unmittelbar in Art. 3 Abs. 2 des geplanten Abkommens definiert und verweist auch auf Handlungen, die in den internationalen Übereinkünften und den Protokollen zur Terrorismusbekämpfung als solche definiert sind. Die Natur und die Schwere einer als „grenzübergreifende schwere Kriminalität" eingestuften Straftat ergibt sich ebenso durchaus aus Art. 3 Abs. 3 des geplanten Abkommens, da es sich um eine Straftat handelt, die in mehr als einem Land verübt wird und die in Kanada mit einer Freiheitsstrafe im Höchstmaß von mindestens vier Jahren geahndet wird. Es handelt sich eindeutig nicht um minder schwere Straftaten oder Straftaten, deren Schwere, wie es bei dem dem Urteil vom 8. April 2014, Digital Rights Ireland u. a. …, zugrunde liegenden Rechtsakt der Fall war, nach dem innerstaatlichen Recht in mehreren Staaten variieren kann und es damit unmöglich macht, den Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte als auf das unbedingt Erforderliche beschränkt anzusehen.[41]

---

[39] Die in Anlage II genannten strafbaren Handlungen umfassen: Beteiligung an einer kriminellen Vereinigung, Menschenhandel, Sexuelle Ausbeutung von Kindern und Kinderpornografie, Illegaler Handel mit Drogen und psychotropen Stoffen, Illegaler Handel mit Waffen, Munition und Sprengstoffen, Korruption, Betrugsdelikte, einschließlich Betrug zum Nachteil der finanziellen Interessen der Union, Wäsche von Erträgen aus Straftaten und Geldfälschung, einschließlich Euro-Fälschung, Computerstraftaten/Cyberkriminalität, Umweltkriminalität, einschließlich des illegalen Handels mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten, Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt, Vorsätzliche Tötung, schwere Körperverletzung, Illegaler Handel mit menschlichen Organen und menschlichem Gewebe, Entführung, Freiheitsberaubung und Geiselnahme, Diebstahl in organisierter Form oder mit Waffen, Illegaler Handel mit Kulturgütern, einschließlich Antiquitäten und Kunstgegenständen, Betrügerische Nachahmung und Produktpiraterie, Fälschung von amtlichen Dokumenten und Handel damit, Illegaler Handel mit Hormonen und anderen Wachstumsförderern, Illegaler Handel mit nuklearen und radioaktiven Substanzen, Vergewaltigung, Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen, Flugzeug- und Schiffsentführung, Sabotage, Handel mit gestohlenen Kraftfahrzeugen und Wirtschaftsspionage.

[40] EuGH, verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238, Rn. 60 – Digital Rights Ireland u.a.

[41] GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 231.

Indes hat er darüber hinaus eine Auflistung der erfassten Straftaten in einem Anhang zum Abkommen verlangt.[42] Dies erscheint jedoch angesichts der zuvor erwähnten Präzisierungen die Bestimmtheitsanforderungen zu überspannen.[43]

b) Automatisierter Abgleich mit Mustern

Die besondere Bedeutung der Fluggastdatenverarbeitung liegt im dadurch ermöglichten automatisierten Abgleich mit Mustern, wie GA *Mengozzi* betont: „der wichtigste Mehrwert der Verarbeitung der PNR-Daten [ist] die Abgleichung der gesammelten Daten mit im Voraus festgelegten Risikoszenarien oder Kriterien für die Risikobeurteilung oder mit Datenbanken, wodurch mittels der automatisierten Verarbeitung ‚Ziele' identifiziert werden können, die später eingehenderen Kontrollen unterzogen werden können".[44]

Die grundsätzliche Angemessenheit des Abgleichs stellt GA *Mengozzi* nicht infrage; hinsichtlich der materiellen und prozeduralen Kriterien für den automatisierten Abgleich fordert er:

> Meiner Meinung nach müsste das geplante Abkommen allerdings zumindest ausdrücklich bestimmen, dass sich weder die im Voraus festgelegten Szenarien und Beurteilungskriterien noch die verwendeten Datenbanken auf die rassische oder ethnische Herkunft einer Person, ihre politischen Meinungen, ihre Religion oder ihre weltanschaulichen Überzeugungen, ihre Gewerkschaftszugehörigkeit, ihren Gesundheitszustand oder ihre sexuelle Ausrichtung stützen dürfen. Außerdem müssten die Kriterien, Szenarien und Datenbanken ausdrücklich auf die von Art. 3 des geplanten Abkommens vorgesehenen Zwecke und Straftaten eingegrenzt werden.
>
> Darüber hinaus müsste das geplante Abkommen meines Erachtens klarer festlegen, als es derzeit sein Art. 15 tut, dass in dem Fall, dass die Abgleichung der PNR-Daten mit den im Voraus festgelegten Kriterien und Szenarien zu einem positiven Ergebnis führt, dieses Ergebnis mit Mitteln eines nicht automatisierten Verfahrens geprüft werden muss. Durch diese Garantie könnte die Zahl der Personen verringert werden, die für eine spätere eingehendere physische Kontrolle in Betracht kommen können.
>
> Zur Beschränkung auf das, was unbedingt erforderlich ist, müssten zudem diese relevanten Kriterien, Szenarien und Datenbanken sowie ihre Überprüfung meiner Ansicht nach der Kontrolle der im geplanten Abkommen genannten unabhängigen Behörde, nämlich des kanadischen Datenschutzbeauftragten (Privacy Commissioner) unterliegen und Gegenstand eines Berichts über ihre Anwendung sein, der an die zuständigen Organe und Einrichtungen der Union im Kontext von Art. 26 des geplanten Abkommens, der die gemeinsame Überprüfung und Evaluierung der Durchführung des Abkommens regelt, übermittelt wird.[45]

Dem genügt die FluggastdatenRL, vgl. Art. 6 Abs. 2 zur Beschränkung der Verarbeitungszwecke, Art. 6 Abs. 3 lit. b zur Vorabfestlegung, Art. 6 Abs. 4 zur Kriterienbestimmung einschließlich des Ausschlusses sensibler Kriterien, Art. 6 Abs. 5 f. zum Erfordernis einer individuellen Überprüfung, Art. 6 Abs. 7 zur Kontrolle. Der FlugDaG-E grenzt den Abgleich mit Mustern weiter ein (siehe unten, V.13.).

---

42 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 232 ff.

43 Vgl. auch *D. Lowe*, ICLRev. 17 (2017), 78, 99.

44 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 252.

45 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 258 ff.

c) Speicherdauer

In der Rs. *Digital Rights Ireland u.a.* hat der EuGH eine klare Bestimmung der Speicherfrist verlangt.[46] Überdies müsse diese auf das absolut Notwendige beschränkt sein, ohne dass sich allerdings konkrete Angaben hinsichtlich der maximalen Speicherdauer finden.[47]

Zweifelsohne ist eine Speicherdauer von fünf Jahren (Art. 12 Abs. 1 FluggastdatenRL) erheblich. Angesichts der geringeren Eingriffsintensität der Fluggastdaten- im Vergleich zur TK-Verkehrsdatenspeicherung (dazu bereits oben, IV.1.) ist der Rahmen des absolut Notwendigen vorliegend weiter. Zu berücksichtigen ist überdies, dass bereits sechs Monate nach Übermittlung der Daten alle eine Identitätsfestellung ermöglichenden PNR-Daten zu depersonalisieren sind (Art. 12 Abs. 2 FluggastdatenRL) und dann nur noch eingeschränkte Zugriffsmöglichkeiten bestehen (Art. 12 Abs. 3 FluggastdatenRL).

GA *Mengozzi* fordert demgegenüber eine objektive Begründung der Notwendigkeit einer fünfjährigen Speicherung[48] und meldet Zweifel an der Notwendigkeit einer Speicherung aller Datenkategorien für fünf Jahre an[49]. Dies ist polizei-fachlich weiter zu prüfen. Die Anonymisierung müsse schließlich alle zur Identifikation geeigneten Daten erfassen,[50] was vorliegend gesichert ist (vgl. Art. 12 Abs. 2 FluggastdatenRL).

d) Kategorien von Fluggastdatensätzen

Gemäß Art. 8 Abs. 1 i.V.m. Anhang I der FluggastdatenRL erstreckt sich die Übermittlungspflicht auf folgende Daten:

1. PNR-Buchungscode (Record Locator)
2. Datum der Buchung/Flugscheinausstellung
3. Planmäßiges Abflugdatum bzw. planmäßige Abflugdaten
4. Name(n)
5. Anschrift und Kontaktangaben (Telefonnummer, E-Mail-Adresse)
6. Alle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift
7. Gesamter Reiseverlauf für bestimmte PNR-Daten
8. Vielflieger-Eintrag
9. Reisebüro/Sachbearbeiter

---

46 EuGH, verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238, Rn. 63 ff. – Digital Rights Ireland u.a.

47 EuGH, verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238, Rn. 64 f. – Digital Rights Ireland u.a.

48 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 279 ff.

49 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 284.

50 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 285 ff.

10. Reisestatus des Fluggasts mit Angaben über Reisebestätigungen, Eincheckstatus, nicht angetretene Flüge (No show) und Fluggäste mit Flugschein, aber ohne Reservierung (Go show)
11. Angaben über gesplittete/geteilte PNR-Daten
12. Allgemeine Hinweise (einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen unter 18 Jahren, wie beispielsweise Name und Geschlecht des Minderjährigen, Alter, Sprache(n), Name und Kontaktdaten der Begleitperson beim Abflug und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, Name und Kontaktdaten der abholenden Person und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, begleitender Flughafenmitarbeiter bei Abflug und Ankunft)
13. Flugscheindaten einschließlich Flugscheinnummer, Ausstellungsdatum, einfacher Flug (One-way), automatische Tarifanzeige (Automated Ticket Fare Quote fields)
14. Sitzplatznummer und sonstige Sitzplatzinformationen
15. Code-Sharing
16. Vollständige Gepäckangaben
17. Zahl und Namen von Mitreisenden im Rahmen der PNR-Daten
18. Etwaige erhobene erweiterte Fluggastdaten (API-Daten) (einschließlich Art, Nummer, Ausstellungsland und Ablaufdatum von Identitätsdokumenten, Staatsangehörigkeit, Familienname, Vorname, Geschlecht, Geburtsdatum, Fluggesellschaft, Flugnummer, Tag des Abflugs, Tag der Ankunft, Flughafen des Abflugs, Flughafen der Ankunft, Uhrzeit des Abflugs und Uhrzeit der Ankunft)
19. Alle vormaligen Änderungen der unter den Nummern 1 bis 18 aufgeführten PNR-Daten.

GA *Mengozzi* verfolgt in seinem Schlussantrag eine strenge Linie und hat zunächst Zweifel an der **Bestimmtheit** einiger Kategorien geäußert [siehe Rn. 217 ff.; genannt werden „‘Verfügbare Vielflieger- und Bonus-Daten (d. h. Gratisflugscheine, Upgrades usw.)‘, … ‚Sämtliche verfügbaren Kontaktangaben, einschließlich Informationen zur Identifizierung des Dateneingebers‘ …. ‚Allgemeine Eintragungen‘“].[51] Hier ist freilich zu berücksichtigen, dass die FluggastdatenRL die Kategorie „Allgemeine Eintragungen“ präzisiert durch einen Klammerzusatz.

Ebenfalls für nicht erforderlich erachtet hat GA *Mengozzi* die **Einbeziehung sensibler PNR-Daten**,

die konkret Hinweise auf den Gesundheitszustand geben können oder aus denen die ethnische Herkunft oder die religiösen Überzeugungen des betreffenden Fluggasts und/oder derjenigen, die ihn begleiten, hervorgehen können.[52]

Die **Garantien zum Schutz dieser sensiblen Daten** im Abkommen genügten nicht:

Trotz der in Art. 8 Abs. 1 bis 4 des geplanten Abkommens vorgesehenen Maßnahmen gestattet nämlich Abs. 5 a. E. dieses Artikels „Kanada“ (und nicht nur der zuständigen kanadischen Behörde), die sensiblen Daten gemäß Art. 16 Abs. 5 des geplanten Abkommens zu speichern. Aus dieser Bestimmung geht u. a. hervor, dass diese Daten höchstens fünf Jahre lang gespeichert werden dürfen, wenn diese Daten „bis zum Abschluss einer besonderen Maßnahme, Überprüfung, Untersuchung, Vollzugsmaßnahme, eines Gerichtsverfahrens, einer strafrechtlichen

---

51 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 217 ff.

52 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 221 f.

Verfolgung oder der Vollstreckung von Strafen erforderlich sind". Art. 16 Abs. 5 des geplanten Abkommens verweist außerdem, im Gegensatz zu dem ihm unmittelbar vorangehenden Absatz, nicht auf die in Art. 3 des Abkommens genannten Zwecke. Folglich könnten die sensiblen Daten eines Unionsbürgers, der mit dem Flugzeug nach Kanada reist, für eine „besondere Maßnahme", „Überprüfung" oder ein „Gerichtsverfahren", die in keinem Zusammenhang mit dem vom geplanten Abkommen verfolgten Ziel stehen – z. B., wie das Parlament geltend gemacht hat, im Fall eines das Vertragsrecht oder das Familienrecht betreffenden Verfahrens –, fünf Jahre lang von jeder kanadischen Behörde gespeichert (und in diesem Zeitraum gegebenenfalls die Unkenntlichmachung aufgehoben und die Daten analysiert) werden. Die Möglichkeit eines solchen Falles legt den Schluss nahe, dass die Vertragsparteien die vom geplanten Abkommen verfolgten Ziele in diesem Punkt nicht ausgewogen gewichtet haben.[53]

Mit Blick auf die FluggastdatenRL ist freilich zu berücksichtigen, dass diese einen Abgleich anhand sensibler Daten verbietet (Art. 6 Abs. 4 S. 4; siehe ferner Art. 7 Abs. 6 für das Verbot einer nachteiligen Entscheidung zulasten des Betroffenen aufgrund dieser Kriterien):

Die rassische oder ethnische Herkunft, die politischen Meinungen, die religiösen oder weltanschaulichen Überzeugungen, die Mitgliedschaft in einer Gewerkschaft, der Gesundheitszustand, das Sexualleben oder die sexuelle Orientierung einer Person dürfen unter keinen Umständen als Grundlage für diese Kriterien dienen.

Schließlich enthält Art. 13 Abs. 4 FluggastdatenRL ein Verarbeitungsverbot (siehe auch die Löschungspflicht in § 13 Abs. 3 FlugDaG-E):

Die Mitgliedstaaten untersagen die Verarbeitung von PNR-Daten, die die rassische oder ethnische Herkunft einer Person, ihre politischen Meinungen, ihre religiösen oder weltanschaulichen Überzeugungen, ihre Mitgliedschaft in einer Gewerkschaft, ihren Gesundheitszustand oder ihr Sexualleben oder ihre sexuelle Orientierung erkennen lassen. Bei der PNR-Zentralstelle eingehende PNR-Daten, aus denen derartige Informationen hervorgehen, werden umgehend gelöscht.

Mit Blick auf die soeben skizzierten Einwände ist schließlich zu berücksichtigen, dass GA *Léger* in seinen Schlussanträgen zum Verfahren über das Fluggastdatenabkommen mit den USA von einem größeren Spielraum ausgeht:

Meines Erachtens hat die Kommission mit der Entscheidung über die Liste mit 34 personenbezogenen Daten … keine Maßnahme angenommen, die zur Erreichung des Zieles der Terrorismusbekämpfung und anderer schwerer Straftaten offensichtlich ungeeignet ist. Zum einen nämlich ist die Bedeutung hervorzuheben, die die Aufklärung im Kampf gegen den Terrorismus hat, weil die Sicherheitsdienste eines Staates durch die Beschaffung geeigneter Informationen eventuelle Terroranschläge verhüten können. So gesehen kann die Notwendigkeit, die Profile potenzieller Terroristen zu erstellen, den Zugang zu einer größeren Anzahl von Daten voraussetzen. Zum anderen reicht der Umstand, dass andere innerhalb der Europäischen Union erlassene Vorschriften über den Informationsaustausch die Weitergabe einer geringeren Anzahl von Daten vorsehen, nicht als Beweis dafür aus, dass die Anzahl von Daten, die in der spezifischen Terrorbekämpfungsnorm der PNR-Regelung verlangt wird, überhöht ist ...

Ferner ist zwar richtig, … dass drei der insgesamt verlangten Datenelemente sensible Daten enthalten können …, doch ist zum einen der Zugriff des CBP auf diese drei Datenelemente nach Absatz 5 der Verpflichtungserklärung eng begrenzt, zum anderen ist es nach den Absätzen 9 bis 11 der Verpflichtungserklärung ausgeschlossen, dass das CBP sensible Daten verwenden kann, und schließlich wurde vom CBP gemäß der von ihm übernommenen Verpflichtung ein Filtersystem für die genannten Daten in Betrieb genommen.[54]

---

53 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 217 ff.

54 GA Léger, in: EuGH, verb. Rs. C-317/04 u. C-318/04, Slg. 2006, I-4721, Rn. 238 f. – Parlament/Rat und Kommission.

8. Materiell- und verfahrensrechtliche Anforderungen für den Zugang zu Datenbeständen

a) Vorabkontrolle

In seinem Urteil in der Rs. *Tele2 Sverige u.a.* verlangt der EuGH eine dem Zugriff auf die gespeicherten Daten vorausgehende Vorabkontrolle durch ein Gericht oder eine unabhängige Behörde:

> Damit in der Praxis die vollständige Einhaltung dieser Voraussetzungen gewährleistet ist, ist es unabdingbar, dass der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten grundsätzlich – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und deren Entscheidung auf einen mit Gründen versehenen Antrag ergeht, der von den zuständigen nationalen Behörden u. a. im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellt wird.[55]

Dieses Erfordernis der Vorabkontrolle kann allenfalls für den Zugang, nicht aber schon für den automatisierten Abgleich gelten (zu den dortigen Kautelen oben, IV.7.b).[56] Bei Bestehen adäquater Rechtsschutzmöglichkeiten erachtet GA *Mengozzi* indes auch eine derartige Vorabkontrolle für entbehrlich:

> Die angemessene Abwägung zwischen der wirksamen Bekämpfung des Terrorismus und der grenzübergreifenden schweren Kriminalität einerseits und der Wahrung eines hohen Niveaus des Schutzes der personenbezogenen Daten der betreffenden Fluggäste andererseits verlangt allerdings nicht zwangsläufig, dass eine vorherige Kontrolle des Zugangs zu den PNR-Daten vorgesehen wird.
>
> Ohne dass geprüft werden müsste, ob eine solche vorherige Kontrolle, insbesondere im Hinblick auf die Menge zu prüfender Daten und die Mittel, über die die unabhängigen Kontrollbehörden verfügen, in der Praxis denkbar und hinreichend wirksam wäre, möchte ich darauf hinweisen, dass der EGMR im Zusammenhang mit der Beachtung von Art. 8 EMRK durch die Behörden, die Maßnahmen zur Erfassung und Überwachung der privaten Kommunikation getroffen haben, anerkannt hat, dass vorbehaltlich besonderer Umstände, die insbesondere die Vertraulichkeit der Informationsquellen der Journalisten oder die Kommunikation zwischen Anwälten und ihren Mandanten betreffen, eine Vorabkontrolle dieser Maßnahmen durch eine unabhängige Behörde oder einen Richter kein absolutes Erfordernis darstellt, sofern eine nachträgliche umfassende gerichtliche Kontrolle dieser Maßnahmen garantiert ist.
>
> Insoweit ist unabhängig von den Zweifeln, die die Verteilung der Zuständigkeiten für die Aufsicht und Kontrolle der CBSA zwischen der „unabhängigen Behörde“ und der „durch administrative Mittel eingerichteten Stelle, die ihre Aufgaben unparteiisch wahrnimmt und nachweislich unabhängig Entscheidungen trifft“, aufwirft …, zu beachten, dass nach Art. 14 Abs. 2 des geplanten Abkommens Kanada dafür zu sorgen hat, dass jede Person, die der Auffassung ist, dass ihre Rechte durch eine Entscheidung oder Maßnahme in Bezug auf ihre PNR-Daten verletzt wurden, Anspruch auf einen wirksamen gerichtlichen Rechtsbehelf nach kanadischem Recht u. a. im Hinblick auf eine gerichtliche Überprüfung hat. Angesichts des Wortlauts von Art. 14 Abs. 1 des geplanten Abkommens und der Ausführungen der Beteiligten steht außer Frage, dass dieser Rechtsbehelf gegen jede Entscheidung über den Zugang zu den PNR-Daten der betreffenden Personen gegeben ist, unabhängig von ihrer Staatsangehörigkeit, ihrem Wohnsitz oder ihrem Aufenthalt im kanadischen Hoheitsgebiet. Im Rahmen des vorliegenden Verfahrens zur präventiven Prüfung der Vereinbarkeit der Bestimmungen des geplanten Abkommens mit den Art. 7 und 8 der Charta erfüllt die Garantie eines solchen Rechtsbehelfs, dessen Wirksamkeit von keinem Beteiligten angezweifelt wurde, meines Erachtens die nach diesen Bestimmungen erforderlichen Voraussetzungen im Licht der Auslegung von Art. 8 EMRK durch den EGMR.
>
> Folglich ist der Umstand, dass das geplante Abkommen den Zugang der hierzu befugten Bediensteten der CBSA zu den PNR-Daten nicht einer vorherigen Kontrolle durch eine unabhängige Verwaltungsbehörde oder ein Gericht

---

55 EuGH, verb. Rs. C-203/15 u. C-698/15, EU:C:2016:970, Rn. 120 – Tele2 Sverige u.a. Siehe bereits verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238, Rn. 62 – Digital Rights Ireland u.a.

56 Vgl. auch GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 262 f., 268.

unterwirft, meiner Meinung nach nicht mit Art. 7, Art. 8 und Art. 52 Abs. 1 der Charta unvereinbar, soweit das geplante Abkommen Kanada verpflichtet – was der Fall ist –, jedem Betroffenen das Recht zu garantieren, die Entscheidungen oder Maßnahmen, die den Zugang zu seinen PNR-Daten betreffen, einer effektiven nachträglichen gerichtlichen Kontrolle zu unterziehen.[57]

Art. 6 Abs. 7 FluggastdatenRL sieht lediglich eine allgemeine (unabhängige) Datenschutzkontrolle, aber keine Vorabkontrolle für die Übermittlung vor; verlangt wird freilich eine Übermittlung nur im Einzelfall und eine individuelle Kontrolle der automatisiert verarbeiteten Daten (Art. 6 Abs. 5 f. FluggastdatenRL). Überdies verpflichtet Art. 13 Abs. 1 FluggastdatenRL die Mitgliedstaaten, dafür Sorge zu tragen, dass „die Rechte jedes Fluggasts in Bezug auf Schutz personenbezogener Daten, Zugang, Berichtigung, Löschung und Einschränkung der Verarbeitung sowie Schadenersatz und Rechtsbehelfe den Rechten entsprechen, die nach Unionsrecht und nationalem Recht sowie zur Umsetzung der Artikel 17, 18, 19 und 20 des Rahmenbeschlusses 2008/977/JI festgelegt sind. Diesbezüglich gelten daher jene Artikel." Ferner verlangt Art. 13 Abs. 8 FluggastdatenRL eine Benachrichtigung bei Rechtsverletzungen (zur Frage Rechtsschutz ermöglichender Benachrichtigungspflichten sogleich, IV.8.c). Weitergehende Benachrichtigungspflichten hat das von GA *Mengozzi* insoweit gebilligte Abkommen nicht enthalten.

Eine Vorabkontrolle hinsichtlich des Zugangs fordert Art. 12 Abs. 3 lit. b FluggastdatenRL schließlich für den Zugang nach Ablauf der Sechs-Monatsfrist:

Nach Ablauf der in Absatz 2 genannten Frist von sechs Monaten ist die Offenlegung der vollständigen PNR-Daten nur zulässig, wenn

a) berechtigter Grund zu der Annahme besteht, dass dies für die Zwecke des Artikels 6 Absatz 2 Buchstabe b erforderlich ist und

b) dies genehmigt wird durch

i) eine Justizbehörde oder

ii) eine andere nationale Behörde, die nach nationalem Recht dafür zuständig ist zu überprüfen, ob die Bedingungen für die Offenlegung erfüllt sind, vorbehaltlich der Unterrichtung des Datenschutzbeauftragten der PNR-Zentralstelle und einer Ex-Post-Überprüfung durch diesen Datenschutzbeauftragten.

b) Beschränkung des Zugangs

In seinem Urteil in der Rs. *Digital Ireland Ltd.* hat der EuGH eine klare Begrenzung der Zugansberechtigten verlangt und beanstandet, dass die „Richtlinie 2006/24 kein objektives Kriterium vor[sieht], das es erlaubt, die Zahl der Personen, die zum Zugang zu den auf Vorrat gespeicherten Daten und zu deren späterer Nutzung befugt sind, auf das angesichts des verfolgten Ziels absolut Notwendige zu beschränken."[58] Auch GA *Mengozzi* fordert die Festlegung

---

57 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 269 ff.

58 EuGH, verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238, Rn. 62 – Digital Rights Ireland u.a.

objektiver Kriterien, die „die Zahl der Personen, die zum Zugang zu den in Rede stehenden personenbezogenen Daten befugt waren", beschränken.[59]

Eine strikte objektiv-individuelle Zugangsbeschränkung findet sich nicht in der FluggastdatenRL. Indes sieht die FluggastdatenRL entsprechende Begrenzungen auf Behördenebene vor und enthält Regelungen, die insoweit Transparenz herstellen.

Zunächst verlangt Art. 4 Abs. 1 FluggastdatenRL, „*eine* für die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten und schwerer Kriminalität zuständige Behörde oder eine Abteilung einer solchen Behörde, die als seine PNR-Zentralstelle handelt", zu errichten oder benennen (Hervorhebung nicht im Original). Erwägungsgrund 13 betont das Konzentrations- und Transparenzanliegen dieser Regelung: „Um Klarheit zu gewährleisten und die Kosten für die Fluggesellschaften gering zu halten, sollten die PNR-Daten an eine einzige, genau bezeichnete Stelle … des jeweiligen Mitgliedstaats übermittelt werden. Die PNR-Zentralstelle kann über verschiedene Zweigstellen in einem Mitgliedstaat verfügen, und Mitgliedstaaten können auch eine PNR-Zentralstelle gemeinsam einrichten." Art. 4 Abs. 5 FluggastdatenRL stellt schließlich Transparenz hinsichtlich der Zuständigkeit sicher: „Innerhalb eines Monats nach der Errichtung seiner PNR-Zentralstelle teilt jeder Mitgliedstaat dies der Kommission mit und kann seine Mitteilung jederzeit ändern. Die Kommission veröffentlicht die Mitteilung sowie alle nachfolgenden Änderungen im Amtsblatt der Europäischen Union."

Vergleichbare Regelungen finden sich in Art. 9 FluggastdatenRL hinsichtlich der zur Anforderung oder Entgegennahme von PNR-Daten berechtigten Personen:

(1) Jeder Mitgliedstaat erstellt eine Liste der zuständigen Behörden, die berechtigt sind, zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität PNR-Daten oder die Ergebnisse der Verarbeitung dieser Daten von den PNR-Zentralstellen anzufordern oder entgegenzunehmen, um sie einer weiteren Prüfung zu unterziehen oder um geeignete Maßnahmen zu veranlassen.

(2) Die in Absatz 1 genannten Behörden sind diejenigen Behörden, die für die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten oder schwerer Kriminalität zuständig sind.

(3) Für die Zwecke des Artikels 9 Absatz 3 übermittelt jeder Mitgliedstaat der Kommission bis zum 25. Mai 2017 die Liste seiner zuständigen Behörden und kann seine Mitteilung jederzeit ändern. Die Kommission veröffentlicht die Mitteilung und eventuelle Änderungen derselben im Amtsblatt der Europäischen Union.

---

59 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 263.

Überdies statuiert Art. 13 Abs. 5 FluggastdatenRL Dokumentationspflichten und impliziert eine (entsprechend selektive) Beauftragung:

Die Mitgliedstaaten sorgen dafür, dass die PNR-Zentralstellen alle ihrer Zuständigkeit unterliegenden Verarbeitungssysteme und -verfahren dokumentieren. Diese Dokumentation muss zumindest folgende Unterlagen enthalten: a) den Namen und die Kontaktinformationen der Organisation und des Personals der PNR-Zentralstelle, die mit der Verarbeitung der PNR-Daten beauftragt sind, und die verschiedenen Ebenen der Zugangsberechtigungen; …

Schließlich ist zu berücksichtigen, dass auch die Anforderung der Datensicherheit einen Zugangsschutz verlangt (vgl. Art. 13 Abs. 2 FluggastdatenRL i.V.m. Art. 22 Rahmenbeschluss 2008/977/JI[60] bzw. Art. 59, 29 Datenschutz-RL 2016/680/EU[61]). GA *Mengozzi* fordert überdies eine **hinreichend bestimmte Festlegung der zuständigen Behörde(n)**.[62] Dem genügt, wie soeben aufgezeigt, Art. 4 und 9 FluggastdatenRL.

Schließlich bedarf es einen **Missbrauchsschutzes**.[63] Dem dienen die Anforderungen an die Datensicherheit (s. unten, IV.9.).

c) Benachrichtigungspflichten

Nachdem es sich um einen „heimlichen" Grundrechtseingriff handelt, verlangt der EuGH in der Rs. *Tele2 Sverige u.a.* eine Rechtsschutz ermöglichende Benachrichtigung:

Außerdem ist es wichtig, dass die zuständigen nationalen Behörden, denen Zugang zu den auf Vorrat gespeicherten Daten gewährt worden ist, die betroffenen Personen im Rahmen der einschlägigen nationalen Verfahren davon in Kenntnis setzen, sobald die Mitteilung die behördlichen Ermittlungen nicht mehr beeinträchtigen kann. Diese Information ist nämlich der Sache nach erforderlich, damit die betroffenen Personen u. a. das Recht auf Einlegung eines Rechtsbehelfs ausüben können, das in Art. 15 Abs. 2 der Richtlinie 2002/58 in Verbindung mit Art. 22 der Richtlinie 95/46 für den Fall einer Verletzung ihrer Rechte ausdrücklich vorgesehen ist.[64]

Art. 13 Abs. 1 FluggastdatenRL schließt eine Benachrichtigung Betroffener von der Datenerhebung aus, da Art. 16 des Rahmenbeschlusses 2008/977/JI (Information der betroffenen Person), künftig Art. 13 (i.V.m. Art. 59) Datenschutz-RL 2016/680/EU (Der betroffenen Person zur Verfügung zu stellende oder zu erteilende Informationen), für nicht anwendbar erklärt wer-

---

60 Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. 2008 L 350, 60.

61 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl.2016 L 119, 89.

62 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 246 ff.

63 EuGH, verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238, Rn. 66 – Digital Rights Ireland u.a.; GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 263.

64 EuGH, verb. Rs. C-203/15 u. C-698/15, EU:C:2016:970, Rn. 121 – Tele2 Sverige u.a.

den, obgleich diese Ausnahmemöglichkeiten vorsehen (siehe namentlich Art. 13 Abs. 3 Datenschutz-RL 2016/680/EU). Immerhin enthält Art. 13 Abs. 8 FluggastdatenRL eine Benachrichtigungspflicht bei Rechtsverletzungen:

> Die Mitgliedstaaten sorgen dafür, dass die PNR-Zentralstelle die betroffene Person und die nationale Kontrollstelle unverzüglich von einer Verletzung des Schutzes personenbezogener Daten benachrichtigt, wenn diese Verletzung voraussichtlich ein hohes Risiko für den Schutz der personenbezogenen Daten oder eine Verletzung der Privatsphäre der betroffenen Person zur Folge hat.

Hinzu kommt, dass eine Benachrichtigung im Rahmen weiterer, auf der Grundlage der übermittelten Information ergriffener Maßnahmen möglich ist.

Schließlich besteht das Auskunftsrecht gemäß Art. 13 Abs. 1 FluggastdatenRL i.V.m. Art. 17 des Rahmenbeschlusses 2008/977/JI (Recht auf Auskunft), künftig Art. 14 f. (i.V.m. Art. 59) Datenschutz-RL 2016/680/EU.

Daher können die Transparenzregeln gerade auch angesichts der geringeren Grundrechtsintensität des Eingriffs für ausreichend erachtet werden. Erwägenswert erscheint freilich, ob nicht durch die Statuierung einer Benachrichtigungspflicht unter Gebrauchmachen von Ausnahmemöglichkeiten die Betroffenenrechte gestärkt werden könnten bei gleichzeitiger hinreichender Sicherung von öffentlichen Geheimhaltungsinteressen.

d) Überwachung durch unabhängige Stelle

Darüber hinaus ist eine Überwachung durch eine unabhängige Stelle i.S.d. Art. 8 Abs. 3 GRC zu sichern.[65] Art. 5 FluggastdatenRL verpflichtet zur Einrichtung eines Datenschutzbeauftragten der PNR-Zentralstelle, der eine unabhängige und wirksame Kontrolle ausübt. Art. 15 FluggastdatenRL sieht ferner die Überwachung durch eine nationale Kontrollstelle vor. Überdies sieht Art. 13 Abs. 5 f. FluggastdatenRL Dokumentationspflichten zur Ermöglichung der Überwachung vor.

9. Datensicherheit

In der Rs. *Tele2 Sverige u.a.* hat der EuGH auch einen hohen Datensicherheitsstandard gefordert. Er verlangt,

> durch geeignete technische und organisatorische Maßnahmen ein besonders hohes Schutz- und Sicherheitsniveau gewährleisten. Die nationale Regelung muss insbesondere vorsehen, dass die Daten im Unionsgebiet zu speichern und nach Ablauf ihrer Speicherungsfrist unwiderruflich zu vernichten sind.[66]

---

65 EuGH, verb. Rs. C-203/15 u. C-698/15, EU:C:2016:970, Rn. 123 – Tele2 Sverige u.a. Siehe bereits verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238, Rn. 68 – Digital Rights Ireland u.a.

66 EuGH, verb. Rs. C-203/15 u. C-698/15, EU:C:2016:970, Rn. 122 – Tele2 Sverige u.a. Siehe bereits verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238, Rn. 66 ff. – Digital Rights Ireland u.a.

Entsprechende Sicherungen sind zunächst durch Art. 6 Abs. 8 FluggastdatenRL vorgegeben:

Die Speicherung, Verarbeitung und Auswertung von PNR-Daten durch die PNR-Zentralstelle erfolgt ausschließlich an einem gesicherten Ort bzw. gesicherten Orten im Hoheitsgebiet der Mitgliedstaaten.

Ferner bestimmt Art. 13 Abs. 2 f., 7 FluggastdatenRL:

(2) Jeder Mitgliedstaat sorgt dafür, dass die nach nationalem Recht erlassenen Bestimmungen zur Umsetzung der Artikel 21 und 22 des Rahmenbeschlusses 2008/977/JI betreffend die Vertraulichkeit der Verarbeitung und die Datensicherheit ebenfalls auf jede Verarbeitung personenbezogener Daten nach dieser Richtlinie Anwendung finden.

(3) Diese Richtlinie berührt nicht die Anwendbarkeit der Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates auf die Verarbeitung personenbezogener Daten durch Fluggesellschaften, insbesondere deren Pflichten, geeignete technische und organisatorische Maßnahmen zum Schutz der Sicherheit und Vertraulichkeit der personenbezogenen Daten zu treffen.

(7) Die Mitgliedstaaten sorgen dafür, dass ihre PNR-Zentralstelle technische und organisatorische Maßnahmen und Verfahren umsetzt, um ein hohes Sicherheitsniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden PNR-Daten angemessen ist.

Art. 12 Abs. 4 FluggastdatenRL sieht die geforderte Löschungspflicht vor.

10. Weiterleitung an Drittstaaten

Der EuGH hat in der Rs. *Schrems* das Erfordernis eines angemessenen Datenschutzniveaus für die Übermittlung an Drittstaaten betont.[67]

Zur Möglichkeit der Weitergabe der Daten an andere innerstaatliche oder ausländische Stellen hat GA *Léger* in seinen Schlussanträgen zum Verfahren über das Fluggastdatenabkommen mit den USA ausgeführt, dass eine solche Weitergabe unter Wahrung bestimmter Garantien zulässig ist:

Das Parlament ist schließlich der Ansicht, die PNR-Regelung gehe über das hinaus, was für die Bekämpfung des Terrorismus und anderer schwerer Straftaten erforderlich sei, da sie die Übermittlung der Fluggästedaten an andere staatliche Stellen erlaube. Das CBP verfüge bei der Übermittlung der PNR-Daten an andere staatliche Behörden, und zwar auch an ausländische Regierungsbehörden, über ein Ermessen, was mit Artikel 8 Absatz 2 EMRK unvereinbar sei.

Ich teile diese Auffassung nicht. Auch hier sprechen nämlich die für die Übermittlung von PNR-Daten an andere Regierungsbehörden geltenden Garantien dafür, dass der Eingriff in das Privatleben der Fluggäste gemessen an dem von der PNR-Regelung verfolgten Ziel verhältnismäßig ist …

So erfolgt … die Übermittlung von PNR-Daten an andere Regierungsbehörden, „die Terrorismusbekämpfungs- oder Strafverfolgungsaufgaben wahrnehmen", „auch solche in Drittländern", „nur von Fall zu Fall" und grundsätzlich nur „zum Zwecke der Verhütung oder Bekämpfung der unter Absatz 3 aufgeführten Straftaten". Das CBP hat gemäß Absatz 30 der Verpflichtungserklärung zu prüfen, ob die Offenlegung der Daten gegenüber einer anderen Behörde diesem Zweck dient. …

Abgesehen ... davon… enthält die Verpflichtungserklärung eine Reihe von Garantien. So bestimmt z. B. Absatz 31 der Verpflichtungserklärung, dass „[b]ei der etwaigen Weitergabe von PNR-Daten an andere designierte Behörden ... das CBP als ‚Eigentümer' der Daten [gilt]. Den designierten Stellen obliegen aufgrund der ausdrücklichen Offenlegungsbestimmungen" eine Reihe von Pflichten. Zu diesen Pflichten der Empfängerbehörden zählen insbesondere die Pflicht „[sicherzustellen], dass die bereitgestellten PNR-Informationen ordnungsgemäß und im Einklang mit den Datenspeicherverfahren der designierten Stelle vernichtet werden", sowie die Pflicht, „für die Weiterverbreitung die ausdrückliche Genehmigung des CBP [einzuholen]".

---

67 EuGH, Rs. C-362/14, EU:C:2015:650, insb. Rn. 67 ff. – Schrems.

Außerdem heißt es in Absatz 32 der Verpflichtungserklärung, dass „[j]ede Offenlegung von PNR-Daten durch das CBP ... davon abhängig gemacht [wird], dass die Empfängerbehörde diese Daten als vertrauliche Geschäftsinformationen und als strafverfolgungsrelevante, vertrauliche personenbezogene Daten des Betroffenen ... behandelt, die als von der Offenlegung nach dem Freedom of Information Act ... ausgenommen behandelt werden sollten". Ferner ist in demselben Absatz bestimmt, dass „der Empfängerbehörde mitgeteilt [wird], dass eine Weiterverbreitung derartiger Informationen ohne ausdrückliche vorherige Genehmigung durch das CBP nicht zulässig ist", wobei das CBP darüber hinaus „eine Weiterübermittlung von PNR-Daten zu Zwecken, die nicht in den Absätzen 29, 34 und 35 aufgeführt sind", nicht genehmigen wird. Schließlich heißt es in Absatz 33 der Verpflichtungserklärung, dass „Mitarbeiter designierter Behörden, die ohne entsprechende Befugnis PNR-Daten offen legen, ... sich strafbar machen [können]".[68]

Bei der Verarbeitung in Drittstaaten verlangt GA *Mengozzi* hinreichende Datensicherheit und hinreichenden Datenschutz.[69] Überdies sei eine Vorabkontrolle durch Gerichte oder unabhängige Behörden erforderlich.[70]

Art. 11 Abs. 1 FluggastdatenRL i.V.m. Art. 13 Rahmenbeschluss 2008/977/JI verlangt ein angemessenes Datenschutzniveau im Drittstaat für die Übermittlung. Art. 11 Abs. 4 FluggastdatenRL sieht eine Pflicht zur Unterrichtung des Datenschutzbeauftragten der PNR-Zentralstelle vor. Eine Vorabkontrolle ist nicht vorgesehen; ob eine solche zwingend notwendig ist, erscheint fraglich.

11. Berufsgeheimnisträger

In seinem Urteil in der Rs. *Digital Rights Ireland u.a.* hat der Gerichtshof beanstandet, dass die Richtlinie Ausnahmen zum Schutz von Berufsgeheimnisträgern vermissen lasse: „Zudem sieht sie keinerlei Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen."[71] Auch die FluggastdatenRL enthält keine entsprechenden Kautelen. Deren Erforderlichkeit hängt davon ab, ob und inwieweit die Generierung von Informationen droht, die für entsprechende Vertrauensbeziehungen relevant sind; diese Gefahr erscheint im Vergleich zur TK-Verkehrsdatenspeicherung deutlich geringer.

12. Unternehmerische Freiheit

Die den Fluggesellschaften auferlegte Übermittlungspflicht stellt einen Eingriff in die unternehmerische Freiheit (Art. 16 GRC) dar.[72] Dessen Rechtfertigungsfähigkeit hängt vom Auf-

---

68 GA Léger, in: EuGH, verb. Rs. C-317/04 u. C-318/04, Slg. 2006, I-4721, Rn. 255 ff. – Parlament/Rat und Kommission.

69 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 277, 296.

70 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 300.

71 EuGH, verb. Rs. C-293/12 u. C-594/12, EU:C:2014:238, Rn. 59 – Digital Rights Ireland u.a.

72 Umfassend zu dieser *F. Wollenschläger*, in: H. von der Groeben/J. Schwarze/A. Hatje (Hrsg.), Europäisches Unionsrecht, 7. Aufl. 2015, Art. 16 GRC.

wand ab, der den Fluggesellschaften entsteht. Im Kontext seiner Urteile zur TK-Verkehrsdatenspeicherung hat der EuGH diesen Aspekt nicht erörtert; die Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung vom 2.3.2010 geht von einer relativ weitgehenden Möglichkeit der Inpflichtnahme von Unternehmen zur Datenspeicherung und Übermittlung aus:

Die Speicherungs- und Übermittlungspflichten legitimieren sich auch hinsichtlich des Eingriffs in die Berufsfreiheit aus der Zielsetzung einer Effektivierung der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Geheimdienste. Sie stützen sich damit auf vernünftige Gründe des Allgemeinwohls, für deren Förderung sie geeignet sind. Eine weniger eingreifende Regelung, die ebenso effektiv und für die öffentliche Hand kostengünstig ist, ist nicht ersichtlich …

Die Speicherungspflicht überschreitet die Grenze der Zulässigkeit nicht durch den technischen Aufwand, den sie den Diensteanbietern abverlangt. Da sich die betreffenden Diensteanbieter auf dem Telekommunikationsmarkt bewegen, müssen sie ohnehin ein hohes Maß an Technikbeherrschung im Bereich der Telekommunikationsdatenerfassung, -speicherung und -verarbeitung aufweisen. Über diese Fähigkeiten müssen auch kleine Unternehmen in diesem Sektor verfügen. Überdies wird jedenfalls ein Großteil der nach § 113a TKG zu speichernden Daten ohnehin von den betreffenden Telekommunikationsunternehmen vorübergehend für eigene Zwecke gespeichert. Anspruchsvolle organisatorische Anforderungen zur Gewährleistung von Datensicherheit entstehen nicht erst aus der Speicherungspflicht …, sondern unabhängig davon schon aus dem Gegenstand der von den betreffenden Unternehmen angebotenen Dienste. Insoweit ist die Auferlegung der spezifischen Pflichten … in technisch-organisatorischer Hinsicht nicht unverhältnismäßig.

Unverhältnismäßig ist die Speicherungspflicht auch nicht in Bezug auf die finanziellen Lasten, die den Unternehmen durch die Speicherungspflicht nach § 113a TKG und die hieran knüpfenden Folgeverpflichtungen wie die Gewährleistung von Datensicherheit erwachsen. Unzumutbar ist dieses insbesondere nicht deshalb, weil dadurch private Unternehmen unzulässig mit Staatsaufgaben betraut würden. Eine kategorische Trennung von "Staatsaufgaben" und "privaten Aufgaben" mit der Folge der grundsätzlichen Unzulässigkeit einer Indienstnahme für Gemeinwohlzwecke von Privaten auf deren Kosten lässt sich der Verfassung nicht entnehmen. Vielmehr hat der Gesetzgeber [hat] einen weiten Gestaltungsspielraum, welche Pflichten zur Sicherstellung von Gemeinwohlbelangen er Privaten im Rahmen ihrer Berufstätigkeit auferlegt (vgl. BVerfGE 109, 64 <85>). Grundsätzlich kann er Lasten und Maßnahmen zur Wahrung von Gemeinwohlbelangen, die als Folge kommerzieller Aktivitäten regelungsbedürftig sind, den entsprechenden Marktakteuren auferlegen, um die damit verbundenen Kosten auf diese Weise in den Markt und den Marktpreis zu integrieren. Dabei ist der Gesetzgeber nicht darauf beschränkt, Private nur dann in Dienst zu nehmen, wenn ihre berufliche Tätigkeit unmittelbar Gefahren auslösen kann oder sie hinsichtlich dieser Gefahren unmittelbar ein Verschulden trifft. Vielmehr reicht insoweit eine hinreichende Sach- und Verantwortungsnähe zwischen der beruflichen Tätigkeit und der auferlegten Verpflichtung (vgl. BVerfGE 95, 173 <187>). Danach bestehen gegen die den Speicherungspflichtigen erwachsenden Kostenlasten keine grundsätzlichen Bedenken. Der Gesetzgeber verlagert auf diese Weise die mit der Speicherung verbundenen Kosten entsprechend der Privatisierung des Telekommunikationssektors insgesamt in den Markt. So wie die Telekommunikationsunternehmen die neuen Chancen der Telekommunikationstechnik zur Gewinnerzielung nutzen können, müssen sie auch die Kosten für die Einhegung der neuen Sicherheitsrisiken, die mit der Telekommunikation verbunden sind, übernehmen und in ihren Preisen verarbeiten. Die den Unternehmen auferlegten Pflichten stehen in engem Zusammenhang mit den von ihnen erbrachten Dienstleistungen und können als solche nur von ihnen selbst erbracht werden. Auch werden hierbei nicht einzelnen Diensteanbietern einzelfallbezogen Sonderopfer auferlegt, sondern in allgemeiner Form die Rahmenbedingungen für die Erbringung von Telekommunikationsdiensten ausgestaltet. Es ist damit verfassungsrechtlich nicht zu beanstanden, wenn die Unternehmen hierfür dann auch die anfallenden Kosten grundsätzlich zu tragen haben. Allein die gemeinwohlbezogene Zielsetzung gebietet es nicht, hierfür einen Kostenersatz vorzusehen (vgl. BVerfGE 30, 292 [311]). Ein Gesetz, das die Berufsausübung in der Weise regelt, dass es Privaten bei der Ausübung ihres Berufs Pflichten auferlegt und dabei regelmäßig eine Vielzahl von Personen betrifft, ist nicht bereits dann unverhältnismäßig, wenn es einzelne Betroffene unzumutbar belastet, sondern erst dann, wenn es bei einer größeren Betroffenengruppe das Übermaßverbot verletzt (vgl. BVerfGE 30, 292 [316]). Dass die Kostenlasten in dieser Weise erdrosselnde Wirkungen haben, ist weder substantiiert vorgebracht noch erkennbar.

Insofern ist nicht weiter zu prüfen, ob hinsichtlich Fallgruppen (vgl. BVerfGE 30, 292 [327]) oder Sondersituationen aus dem Gesichtspunkt der Verhältnismäßigkeit Härteregelungen geboten sind. Denn jedenfalls ergibt sich hierfür aus dem Vorbringen der Beschwerdeführerin … nichts. Insbesondere hat sie auch in Bezug auf Anonymisierungsdienste eine über die bei den sonstigen Telekommunikationsunternehmen hinausgehende Belastung weder für sich noch für andere Anbieter solcher Dienste hinreichend nachvollziehbar durch konkrete Zahlen belegt. Nur

unter dieser Voraussetzung ließe sich aber eine Überschreitung des gesetzgeberischen Gestaltungsspielraums bei der Indienstnahme der Anonymisierungsdienste feststellen. Solange die Einschätzung des Gesetzgebers nur durch Vermutungen und Behauptungen in Frage gestellt wird, kann das Bundesverfassungsgericht dieser Frage nicht nachgehen (vgl. BVerfGE 114, 196 [248]).

Keinen grundsätzlichen Bedenken hinsichtlich möglicher verbleibender Kostenlasten unterliegt auch die Übermittlungspflicht gemäß § 113b Satz 1 Nr. 1 TKG in Verbindung mit § 100g StPO, für die der Gesetzgeber eine Entschädigungsregelung vorgesehen hat (vgl. § 23 Abs. 1 Justizvergütungs- und -entschädigungsgesetz). Die hier vorgesehenen Ausgleichsansprüche sind nicht Gegenstand des vorliegenden Verfahrens.[73]

V. Umsetzungsfragen

1. Einbeziehung auch innereuropäischer Flüge

Der deutsche Gesetzgeber hat, ebenso wie alle anderen Mitgliedstaaten,[74] von der in Art. 2 FluggastdatenRL eröffneten Möglichkeit Gebrauch gemacht, auch innereuropäische Flüge (und nicht nur Flüge in/aus Drittstaaten) in die Fluggastdatenverarbeitung einzubeziehen (siehe § 2 Abs. 3 FlugDaG-E).[75] Diese im Ermessen des deutschen Gesetzgebers liegende Entscheidung ist sowohl an Unions- als auch an nationalen Grundrechten zu messen und vom deutschen Gesetzgeber zu verantworten (siehe oben, III.2.).

Die Erweiterung des Anwendungsbereichs der Fluggastdatenverarbeitung verschärft zwar die mit ihr einhergehenden Grundrechtseingriffe; allerdings stellen sich keine strukturell anderen Fragen als im oben erörterten internationalen Kontext. Hinsichtlich der Unionsgrundrechtskonformität kann damit nach oben verwiesen werden (IV.).

Hinsichtlich der Vereinbarkeit mit nationalen Grundrechten ist zunächst festzuhalten, dass – ebenso wie im unionsrechtlichen Kontext – keine unmittelbar einschlägige Rechtsprechung zur Fluggastdatenverarbeitung existiert. Eine gewisse Orientierung bietet das Urteil des Bundesverfassungsgerichts zur (anlasslosen) Telekommunikations-Verkehrsdatenspeicherung vom 2.3.2010 sowie weitere Urteile zu informatiellen Eingriffen zu repressiven und präventiven Zwecken.[76] Bei einer Übertragung der im zuerst genannten Urteil entwickelten Grundsätze ist wiederum zu berücksichtigen, dass die Fluggastdatenverarbeitung angesichts der geringeren Streubreite des Eingriffs und der geringeren Aussagekraft der Daten einen weniger intensiven Grundrechtseingriff als die TK-Verkehrsdatenspeicherung darstellt (siehe bereits oben, IV.1.).

---

73 BVerfGE 125, 260, 360 ff.

74 Vgl. die Erklärung des Rates v. 18.4.2016, http://data.consilium.europa.eu/doc/document/ST-7829-2016-ADD-1/de/pdf (13.4.2017).

75 So auch ausdrücklich BT-Drs. 18/11501, S. 19.

76 BVerfGE 125, 260; ferner E 120, 274; E 130, 151; NJW 2016, 1781.

Das Bundesverfassungsgericht hat letztere für verfassungskonform erachtet, so die Ausgestaltung der gesetzlichen Regelung dem besonderen Gewicht des Eingriffs Rechnung trägt:

> Materiell verfassungsgemäß sind die Eingriffe in das Telekommunikationsgeheimnis, wenn sie legitimen Gemeinwohlzwecken dienen und im Übrigen dem Grundsatz der Verhältnismäßigkeit genügen …, das heißt zur Erreichung der Zwecke geeignet, erforderlich und angemessen sind …
>
> Eine sechsmonatige anlasslose Speicherung von Telekommunikationsverkehrsdaten für qualifizierte Verwendungen im Rahmen der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Nachrichtendienste, … ist danach mit Art. 10 GG nicht schlechthin unvereinbar. Der Gesetzgeber kann mit einer solchen Regelung legitime Zwecke verfolgen, für deren Erreichung eine solche Speicherung im Sinne des Verhältnismäßigkeitsgrundsatzes geeignet und erforderlich ist. Einer solchen Speicherung fehlt es auch in Bezug auf die Verhältnismäßigkeit im engeren Sinne nicht von vornherein an einer Rechtfertigungsfähigkeit. Bei einer Ausgestaltung, die dem besonderen Gewicht des hierin liegenden Eingriffs hinreichend Rechnung trägt, unterfällt eine anlasslose Speicherung der Telekommunikationsverkehrsdaten nicht schon als solche dem strikten Verbot einer Speicherung von Daten auf Vorrat im Sinne der Rechtsprechung des Bundesverfassungsgerichts …
>
> Die Effektivierung der Strafverfolgung, der Gefahrenabwehr und der Erfüllung der Aufgaben der Nachrichtendienste sind legitime Zwecke, die einen Eingriff … grundsätzlich rechtfertigen können … Eine vorsorglich anlasslose Datenspeicherung ist allerdings nur ausnahmsweise zulässig. Sie unterliegt sowohl hinsichtlich ihrer Begründung als auch hinsichtlich ihrer Ausgestaltung, insbesondere auch in Bezug auf die vorgesehenen Verwendungszwecke, besonders strengen Anforderungen.[77]

Vor diesem Hintergrund ist festzuhalten, dass sich auch der Rechtsprechung des Bundesverfassungsgerichts kein generelles Verbot der anlasslosen Fluggastdatenverarbeitung entnehmen lässt (a). Analog zum Urteil in Sachen Verkehrsdatenspeicherung lässt sich die Eignung (b) und Erforderlichkeit (c) des Eingriffs in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) bejahen. Darüber hinaus werden die Grundsatzanforderungen des Gerichts an die Ausgestaltung einer entsprechenden gesetzlichen Regelung gewahrt, namentlich hinsichtlich der Beschränkung der Speicherpflicht (d), der Datensicherheit (e), der Datenlöschung (f), der Datenverwendung (g), des Schutzes von Berufsgeheimnisträgern (h), des Zugangs (i) und der Transparenz (j).

a) Kein generelles Verbot der anlasslosen Fluggastdatenverarbeitung

Bei der auf die Bekämpfung terroristischer Straftaten und schwerer Kriminalität zielenden Fluggastdatenverarbeitung handelt es sich wegen der Zweckbindung zunächst um keine schlechthin verfassungsrechtlich unzulässige „Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken“.[78]

Auch ist nach Einführung der (punktuellen) Fluggastdatenverarbeitung die Schwelle einer verfassungsrechtlich unzulässigen, da *flächendeckenden* vorsorglichen Datenspeicherung noch

---

77 Siehe BVerfGE 125, 260, 316 ff.

78 Siehe BVerfGE 125, 260, 320 f.

nicht überschritten, mag auch die kürzlich wiedereingeführte TK-Verkehrsdatenspeicherung den Spielraum für weitere Datensammlungen reduzieren:

> Umgekehrt darf die Speicherung der Telekommunikationsverkehrsdaten nicht als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte. Eine solche Gesetzgebung wäre, unabhängig von der Gestaltung der Verwendungsregelungen, von vornherein mit der Verfassung unvereinbar. Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt vielmehr voraus, dass diese eine Ausnahme bleibt. Sie darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen. Maßgeblich für die Rechtfertigungsfähigkeit einer solchen Speicherung ist deshalb insbesondere, dass sie nicht direkt durch staatliche Stellen erfolgt, dass sie nicht auch die Kommunikationsinhalte erfasst und dass auch die Speicherung der von ihren Kunden aufgerufenen Internetseiten durch kommerzielle Diensteanbieter grundsätzlich untersagt ist. Die Einführung der Telekommunikationsverkehrsdatenspeicherung kann damit nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland …, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss. Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer.[79]

Auch im Urteil zum BKA-Gesetz hat das Bundesverfassungsgericht betont:

> Eigene verfassungsrechtliche Grenzen ergeben sich hinsichtlich des Zusammenwirkens der verschiedenen Überwachungsmaßnahmen. Mit der Menschenwürde unvereinbar ist es, wenn eine Überwachung sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können … Beim Einsatz moderner, insbesondere dem Betroffenen verborgener Ermittlungsmethoden müssen die Sicherheitsbehörden mit Rücksicht auf das dem „additiven" Grundrechtseingriff innewohnende Gefährdungspotenzial koordinierend darauf Bedacht nehmen, dass das Ausmaß der Überwachung insgesamt beschränkt bleibt.[80]

b) Eignung

Kritiker der Einbeziehung von innereuropäischen Flügen im Rahmen der Fluggastdatenverarbeitung bezweifeln bereits deren grundsätzliche Eignung zur Effektivierung von Strafverfolgung und Gefahrenabwehr.[81]

Insoweit ist freilich zu berücksichtigen, dass die verfassungsrechtlichen Anforderungen an die Geeignetheit der gesetzgeberischen Maßnahme nicht zu hoch angesetzt werden dürfen. Nicht erforderlich ist insbesondere, dass durch das eingesetzte Mittel der angestrebte Zweck vollum-

---

79 Siehe BVerfGE 125, 260, 320 f.

80 BVerfG, NJW 2016, 1781, 1787 f., Rn. 130.

81 Vgl. etwa die Aktualisierte Stellungnahme des Bundesverbandes der Deutschen Luftverkehrswirtschaft (BDL) zum Gesetzesentwurf der Bundesregierung Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG) vom 23. März 2017, S. 4.

fänglich erreicht wird, es genügt vielmehr, dass die Wahrscheinlichkeit eines teilweisen Erfolgseintritts zumindest erhöht wird.[82] Vor diesem Hintergrund hat das Bundesverfassungsgericht in seinem Urteil zur Verkehrsdatenspeicherung keine Zweifel an deren Eignung artikuliert:

> Eine vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten zur späteren anlassbezogenen Übermittlung an die für die Strafverfolgung oder Gefahrenabwehr zuständigen Behörden beziehungsweise an die Nachrichtendienste darf der Gesetzgeber zur Erreichung seiner Ziele als geeignet ansehen. Es werden hierdurch Aufklärungsmöglichkeiten geschaffen, die sonst nicht bestünden und angesichts der zunehmenden Bedeutung der Telekommunikation auch für die Vorbereitung und Begehung von Straftaten in vielen Fällen erfolgversprechend sind ... [Dies] erfordert nicht, dass das Regelungsziel in jedem Einzelfall tatsächlich erreicht wird, sondern verlangt lediglich, dass die Zweckerreichung gefördert wird.[83]

Ergänzend, namentlich zum Abgleich mit Mustern, kann auf das zur Unionsgrundrechtskonformität Ausgeführte verwiesen werden (siehe oben, IV.5.). Schließlich sei festgehalten, dass die Einbeziehung von innereuropäischen Flügen die Zielerreichung fördert, da schwere Kriminalität und etwa auch vergangene terroristische Anschläge vielfach von europaweit mobilen Tätern verübt worden sind.[84]

c) Erforderlichkeit

Das Bundesverfassungsgericht hielt darüber hinaus in seinem Urteil zur Vorratsdatenspeicherung fest, dass ein milderes, in seiner Effektivität vergleichbares Mittel nicht ersichtlich sei, und ein solches insbesondere nicht die anlassbezogene Speicherung darstelle.[85]

In Ergänzung des zur Unionsgrundrechtskonformität Ausgeführten (siehe oben, IV.6.) sei festgehalten, dass als milderes Mittel eine 1:1 Umsetzung der FluggastdatenRL in Betracht kommt, ohne dass der Anwendungsbereich auf innereuropäische Flüge ausgeweitet wird. Auch die Einbeziehung nur einzelner innereuropäischer Flüge wäre möglicherweise ein milderes Mittel. Dass diese Möglichkeiten indes gleich effektiv sind, ist mit der Gesetzesbegründung zu bezweifeln:

> Die im Bereich der schweren Kriminalität und des internationalen Terrorismus aktiven Täter und Tätergruppierungen nutzen häufig Reiserouten innerhalb der Europäischen Union. Um die von internationalem Terrorismus und schwerer Kriminalität ausgehenden Gefahren effektiv bekämpfen zu können, ist es erforderlich, auch die Fluggastdaten von Flügen innerhalb der Europäischen Union auszuwerten.[86]

---

82 Siehe BVerfGE 16, 147, 183; E 30, 292, 316; E 33, 171, 187; E 67, 151, 173 ff.; E 96, 10, 23 ff.

83 BVerfGE 125, 260, 317 f.

84 Begründung, BT-Drs. 18/11501, S. 16.

85 BVerfGE 125, 260, 318.

86 Begründung, BT-Drs. 18/11501, S. 17.

d) Umfang der Speicherpflicht

Das Bundesverfassungsgericht verlangt eine sachlich und zeitlich wirksam begrenzte Speicherpflicht.[87] Hinsichtlich des sachlichen Umfangs kann auf die Ausführungen zur Unionsgrundrechtskonformität verwiesen werden (siehe oben, IV.7.d). Zeitlich hat das Bundesverfassungsgericht sechs Monate als absolute Obergrenze für die TK-Verkehrsdatenspeicherung angesehen, hierbei allerdings Umfang und Aussagekraft dieser Daten besonders betont.[88] Berücksichtigt man die geringere Eingriffsintensität der Fluggastdatenverarbeitung (siehe oben, IV.1.), erscheint die in § 13 Abs. 1 S. 1 FlugDaG-E vorgesehene fünfjährige Speicherung noch vertretbar, zumal die Daten nach sechs Monaten depersonalisiert werden (siehe auch oben, IV.2.c).

e) Datensicherheit

Das Bundesverfassungsgericht hat in seinem Urteil zur TK-Verkehrsdatenspeicherung besonders hohe Datensicherheitsstandards gefordert und Einzelanforderungen ausbuchstabiert, dies indes gerade auch vor dem Hintergrund der Speicherung jener Daten bei privaten Wirtschaftsakteuren und der besonderen Aussagekraft der Daten.[89] Dies steht einer unbesehenen Übertragung jener Anforderungen auf die Fluggastdatenverarbeitung entgegen.

Der FlugDaG-E enthält keine spezifischen Bestimmungen zur Gewährleistung der Datensicherheit. Er sieht diese vielmehr dadurch gewährleistet, dass das Bundesdatenschutzgesetz und seine Anforderungen an die Datensicherheit für das Bundeskriminalamt gelten (dazu noch unten, V.5.).[90]

f) Datenlöschung

Neben den Vorgaben hinsichtlich der Speicherung und Übermittlung der TK-Verkehrsdaten fordert das Bundesverfassungsgericht auch wirksame Sicherungsmaßnahmen betreffend die Löschung der gespeicherten Datenbestände.[91] Freilich ist auch hier wieder der Hintergrund einer Speicherung durch Private zu sehen. § 13 FlugDaG-E enthält eine Löschungsregelung.

---

87 BVerfGE 125, 260, 322.

88 BVerfGE 125, 260, 322.

89 BVerfGE 125, 260, 325 ff.

90 Begründung, BT-Drs. 18/11501, S. 36.

91 BVerfGE 125, 260, 325.

g) Verwendungszwecke

aa) Verfassungsrechtlicher Rahmen

In seinem Urteil zur TK-Verkehrsdatenspeicherung hat das Bundesverfassungsgericht strenge Anforderungen an die Datenverwendung formuliert. In allgemeiner Hinsicht hat es freilich festgehalten, dass die Voraussetzungen für die Datenverwendung umso enger zu begrenzen sind, je schwerwiegender der durch die Speicherung erfolgende Eingriff ist. Dies senkt die Anforderungen im hiesigen Kontext ab. Demgegenüber ist in Anbetracht der Schwere des Eingriffs durch die anlasslose systematische Speicherung fast aller TK-Verkehrsdaten eine Verwendung insoweit nur für überragend wichtige Aufgaben des Rechtsgüterschutzes zulässig:

> Die Verwendung der durch eine anlasslos systematische Speicherung praktisch aller Telekommunikationsverkehrsdaten gewonnenen Datenbestände unterliegt dementsprechend besonders hohen Anforderungen. Insbesondere ist diese nicht in gleichem Umfang verfassungsrechtlich zulässig wie die Verwendung von Telekommunikationsverkehrsdaten, die die Diensteanbieter in Abhängigkeit von den jeweiligen betrieblichen und vertraglichen Umständen – von den Kunden teilweise beeinflussbar – nach § 96 TKG speichern dürfen. Angesichts der Unausweichlichkeit, Vollständigkeit und damit gesteigerten Aussagekraft der über sechs Monate systematisch vorsorglich erhobenen Verkehrsdaten hat ihr Abruf ein ungleich größeres Gewicht. Da eine Auswertung dieser Daten tief in das Privatleben eindringende Rückschlüsse und unter Umständen detaillierte Persönlichkeits- und Bewegungsprofile ermöglicht, kann insoweit nicht ohne weiteres davon ausgegangen werden, dass der Rückgriff auf diese Daten grundsätzlich geringer wiegt als eine inhaltsbezogene Telekommunikationsüberwachung … Vielmehr kann auch die Verwendung solcher Daten nur dann als verhältnismäßig angesehen werden, wenn sie besonders hochrangigen Gemeinwohlbelangen dient. Eine Verwendung der Daten kommt deshalb nur für überragend wichtige Aufgaben des Rechtsgüterschutzes in Betracht, das heißt zur Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen[,] oder zur Abwehr von Gefahren für solche Rechtsgüter.[92]

Im Rahmen der Strafverfolgung wurde eine Verwendung aufgrund eines durch bestimmte Tatsachen begründeten **Verdachts einer schweren Straftat** für zulässig erachtet, wobei die Qualifikation der Straftaten als schwer bereits in der jeweiligen Strafnorm angelegt sein muss. Zur Orientierung kann hierbei etwa auf den Strafrahmen der Norm zurückgegriffen werden:

> 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.
>
> Über die abstrakte Festlegung eines entsprechenden Straftatenkatalogs hinaus hat der Gesetzgeber sicherzustellen, dass ein Rückgriff auf die vorsorglich gespeicherten Telekommunikationsverkehrsdaten nur dann zulässig ist, wenn auch im Einzelfall die verfolgte Straftat schwer wiegt … und die Verwendung der Daten verhältnismäßig ist.[93]

Eine Verwendung im Bereich der Gefahrenabwehr ist zulässig, wenn tatsächliche Anhaltspunkte auf das Bestehen einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person, für

---

92 BVerfGE 125, 260, 328.

93 BVerfGE 125, 260, 328 f.

den Bestand oder die Sicherheit des Bundes oder eines Landes oder auf eine gemeine Gefahr hindeuten. Eine Differenzierung zwischen den unterschiedlichen im Rahmen der Gefahrenabwehr tätigen Behörden, insbesondere hinsichtlich der Nachrichtendienste, ist hierbei nicht erforderlich:

> Die Abwägung zwischen dem Gewicht des in der Datenspeicherung und Datenverwendung liegenden Eingriffs und der Bedeutung einer wirksamen Gefahrenabwehr führt dazu, dass ein Abruf der vorsorglich gespeicherten Telekommunikationsverkehrsdaten nur zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zugelassen werden darf … 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. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die die Prognose einer konkreten Gefahr tragen …
>
> Die verfassungsrechtlichen Anforderungen für die Verwendung der Daten zur Gefahrenabwehr gelten für alle Eingriffsermächtigungen mit präventiver Zielsetzung. Sie gelten damit auch für die Verwendung der Daten durch die Nachrichtendienste. Da die Beeinträchtigung durch den Eingriff in allen diesen Fällen für die Betroffenen die gleiche ist, besteht hinsichtlich dieser Anforderungen kein Anlass zu behördenbezogenen Differenzierungen, etwa zwischen Polizeibehörden und anderen mit präventiven Aufgaben betrauten Behörden wie Verfassungsschutzbehörden …[94]

bb) Bewertung

Nach dem FlugDaG-E ist die Verarbeitung der Fluggastdaten und deren Weitergabe ausschließlich zum Zwecke der Identifizierung von Personen zulässig, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie eine der in § 4 Abs. 1 FlugDaG-E genannten Straftaten begangen haben oder innerhalb eines übersehbaren Zeitraums begehen werden. Bei diesen Straftaten handelt es sich um:

1. eine Straftat nach § 129a, auch in Verbindung mit § 129b, des Strafgesetzbuchs,
2. eine in § 129a Absatz 1 Nummer 1 und 2, Absatz 2 Nummer 1 bis 5 des Strafgesetzbuchs bezeichnete Straftat, wenn diese bestimmt ist, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen kann,
3. eine Straftat, die darauf gerichtet ist, eine der in Nummer 2 bezeichneten Straftaten anzudrohen,
4. eine Straftat nach den §§ 89a bis 89c und nach § 91 des Strafgesetzbuchs,
5. eine Straftat im unmittelbaren Zusammenhang mit terroristischen Aktivitäten nach Artikel 3 Absatz 2 des Rahmenbeschlusses 2002/475/JI des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung (ABl. EG Nr. L 164 S. 3), der zuletzt durch Artikel 1 Nummer 1 des Rahmenbeschlusses 2008/919/JI (ABl. L 330 vom 9.12.2008, S. 21) geändert worden ist, oder
6. eine Straftat, die einer in Anhang II der Richtlinie 2016/681 aufgeführten strafbaren Handlung entspricht und die mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht ist.

Der Katalog entspricht dem Ziel, terroristische Straftaten bzw. schwere Kriminialität zu bekämpfen. Ebenso erscheint das Gewicht der Anlasstaten angesichts der Strafrahmen, auch unter

---

[94] BVerfGE 125, 260, 330 f.

Berücksichtigung des gesetzgeberischen Beurteilungsspielraums, grundsätzlich hinreichend.[95] Gerade mit Blick auf die Drei-Jahres-Schwelle des § 4 Abs. 1 Nr. 6 FlugDaG-E ist ferner darauf hinzuweisen, dass das Bundesverfassungsgericht in seinem Urteil zur TK-Speicherung „nur" eine schwere, aber keine besonders schwere Straftat gefordert hat; letzteres erfasst nur Straftaten, die mit einer Höchststrafe von mindestens fünf Jahren Freiheitsstrafe bewehrt sind.[96]

Verfehlt wird das Erfordernis einer nicht nur abstrakt, sondern auch im Einzelfall schwer wiegenden Straftat. Dies betrifft namentlich Tatbestände, die ein breites Spektrum an Verwirklichungsmöglichkeiten unterschiedlichen Gewichts umfassen, etwa den Betrugstatbestand, der vollumfänglich erfasst ist (zur Korrektur unten, V.4.a).

Überdies werfen § 4 Abs. 1 Nr. 5 und 6 FlugDaG-E **Bestimmtheitsfragen** auf (dazu unten, V.4.b).

h) Berufsgeheimnisträger

In seinem Urteil zur TK-Verkehrsdatenspeicherung hat das Bundesverfassungsgericht einen Schutz vom Berufsgeheimnisträgern und vergleichbaren Vertrauensbeziehungen wenn auch nicht auf Speicherungs-, so aber doch auf Erhebungs- respektive Verwertungsebene gefordert.[97] Der FlugDaG-E enthält keine derartigen Regelungen, sie erscheinen aber auch nicht erforderlich (siehe oben, IV.11.).

i) Datenzugang

Mit Blick auf die Gewährleistung effektiven Rechtsschutzes für die Betroffenen fordert das Bundesverfassungsgericht in seinem Urteil zur TK-Verkehrsdatenspeicherung insbesondere, dass die Abfrage oder Übermittlung der Verkehrsdaten aufgrund der Schwere des Grundrechtseingriffs grundsätzlich unter Richtervorbehalt zu stellen ist:

> Nach der Rechtsprechung des Bundesverfassungsgerichts kann bei Ermittlungsmaßnahmen, die einen schwerwiegenden Grundrechtseingriff bewirken, verfassungsrechtlich eine vorbeugende Kontrolle durch eine unabhängige Instanz geboten sein. Dies gilt insbesondere, wenn der Grundrechtseingriff heimlich erfolgt und für den Betroffenen unmittelbar nicht wahrnehmbar ist … Für die Abfrage und Übermittlung von Telekommunikationsverkehrsdaten kann dies der Fall sein. Angesichts des Gewichts des hierin liegenden Eingriffs reduziert sich der Spielraum des Gesetzgebers dahingehend, dass solche Maßnahmen grundsätzlich unter den Vorbehalt richterlicher Anord-

---

95 Vgl. für die Abwehr terroristischer Straftaten auch BVerfG, NJW 2016, 1781, 1783, Rn. 96: „Straftaten mit dem Gepräge des Terrorismus in diesem Sinne zielen auf eine Destabilisierung des Gemeinwesens und umfassen hierbei in rücksichtsloser Instrumentalisierung anderer Menschen Angriffe auf Leib und Leben beliebiger Dritter. Sie richten sich gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes. Die Bereitstellung von wirksamen Aufklärungsmitteln zu ihrer Abwehr ist ein legitimes Ziel und für die demokratische und freiheitliche Ordnung von großem Gewicht (vgl. BVerfGE 115, 320 <357 f.>; 120, 274 <319>; 133, 277 <333 f. Rn. 133>)".

96 BVerfGE 109, 279, 347 f.

97 BVerfGE 125, 260, 333 f.

nung zu stellen sind. Richter können aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren … Eine Ausnahme gilt nach Art. 10 Abs. 2 Satz 2 GG für die Kontrolle von Eingriffen in die Telekommunikationsfreiheit durch die Nachrichtendienste. Hier kann an die Stelle einer vorbeugenden richterlichen Kontrolle die – gleichfalls spezifisch auf die jeweilige Maßnahme bezogene – Kontrolle durch ein von der Volksvertretung bestelltes Organ oder Hilfsorgan treten …[98]

Trotz des Beitrags eines Richtervorbehalts zum prozeduralen Grundrechtsschutz[99] **verbietet sich die unbesehene Verallgemeinerung dieses Erfordernisses**.[100] Zu berücksichtigen ist nämlich, dass das Grundgesetz nur in wenigen Ausnahmefällen einen solchen vorsieht, nämlich für den gravierenden Eingriff des Freiheitsentzugs (Art. 104 Abs. 2 GG) sowie bei bestimmten Eingriffen in die Unverletzlichkeit der Wohnung (Art. 13 Abs. 2 ff. GG). Überdies lässt Art. 19 Abs. 4 GG nachträglichen Rechtsschutz gegen staatliche Maßnahmen grundsätzlich genügen; die Zulässigkeit des vorbeugenden Rechtsschutzes stellt demgegenüber eine begründungsbedürftige Ausnahme dar. Schließlich geht Art. 10 Abs. 2 S. 2 GG von der Einschlägigkeit des „normalen" Rechtsweges auch bei schwerwiegenden Beschränkungen des Telekommunikationsgeheimnisses aus.

Zurückhaltung lässt auch die in Ausnahmefällen einen Richtervorbehalt anerkennende Rechtsprechung des Bundesverfassungsgerichts erkennen. So sind selbst die kumulativen Erfordernisse eines heimlichen und schwerwiegenden Grundrechtseingriffs zwar eine notwendige, aber noch keine hinreichende Bedingung.[101] Denn selbst unter diesen Voraussetzungen erachtet das Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung vom 27.2.2008 lediglich „eine vorbeugende Kontrolle durch eine unabhängige Instanz [für] verfassungsrechtlich geboten". Ein Regelungsspielraum kommt dem Gesetzgeber „allerdings bei der Gestaltung der Kontrolle im Einzelnen, etwa bei der Entscheidung über die kontrollierende Stelle und das anzuwendende Verfahren", zu. Dieser Spielraum verdichtet sich nur dann zum Erfordernis eines Richtervorbehalts, wenn ein „Grundrechtseingriff von besonders hohem Gewicht" vorliegt.[102]

Der FlugDaG-E sieht einen Richtervorbehalt lediglich für eine Repersonalisierung der Fluggastdaten vor (§ 5 Abs. 2 S. 1 Nr. 2). Im Übrigen ist eine Einbeziehung des (unabhängigen) Datenschutzbeauftragten der Fluggastdatenzentralstelle bei Erstellung und Aktualisierung der Muster (§ 4 Abs. 3 S. 1 FlugDaG-E) vorgesehen, daneben eine regelmäßige Kontrolle durch

---

98 BVerfGE 125, 260, 337 f.

99 Siehe nur BVerfGE 109, 279, 357 f.; E 120, 274, 325.

100 Siehe auch *T. E. Aschmann*, Der Richtervorbehalt im deutschen Polizeirecht, 1999, zusammenfassend S. 156, 237; ferner BVerfG, NJW 2016, 1781, 1791 f., Rn. 174.

101 BVerfGE 120, 274, 325 f.; siehe auch E 125, 260, 337 f.

102 BVerfGE 120, 274, 325 f.; ferner BVerfG, NJW 2016, 1781, 1791 f., Rn. 174; für einen weiten Spielraum auch SächsVerfGHE 4, 303, juris, Rn. 263.

den/die Bundesbeauftragte(n) für den Datenschutz und die Informationsfreiheit insoweit (§ 4 Abs. 3 S. 8 FlugDaG-E). Des Weiteren sehen §§ 11 f. FlugDaG-E eine externe und interne Datenschutzkontrolle vor.

Angesichts der im Vergleich zur TK-Verkehrsdatenspeicherung geringeren Eingriffsintensität und analog zum unionsrechtlichen Befund (siehe oben, IV.8.a) erscheint eine über den erwähnten Richtervorbehalt hinausgehende Vorabkontrolle entbehrlich.

j) Transparenz

aa) Verfassungsrechtlicher Rahmen

Die Verwendung von vorsorglich anlasslos gespeicherten Telekommunikations-Verkehrsdaten ermöglicht es, tiefgehende Einblicke in das Privatleben der Bürger zu erhalten, ohne dass diese davon Kenntnis erlangen. Das Bundesverfassungsgericht knüpft die Verwendung solcher Datenbestände daher an eine hinreichende Transparenz:

> Zu den Voraussetzungen der verfassungsrechtlich unbedenklichen Verwendung von durch eine solche Speicherung gewonnenen Daten gehören Anforderungen an die Transparenz. Soweit möglich muss die Verwendung der Daten offen erfolgen. Ansonsten bedarf es grundsätzlich zumindest nachträglich einer Benachrichtigung der Betroffenen. Unterbleibt ausnahmsweise auch diese, bedarf die Nichtbenachrichtigung einer richterlichen Entscheidung.
>
> Eine vorsorglich anlasslose Speicherung aller Telekommunikationsverkehrsdaten über sechs Monate ist unter anderem deshalb ein so schwerwiegender Eingriff, weil sie ein Gefühl des ständigen Überwachtwerdens hervorrufen kann; sie erlaubt in unvorhersehbarer Weise tiefe Einblicke in das Privatleben, ohne dass der Rückgriff auf die Daten für den Bürger unmittelbar spürbar oder ersichtlich ist. Der Einzelne weiß nicht, was welche staatliche Behörde über ihn weiß, weiß aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können.
>
> Der Gesetzgeber muss die diffuse Bedrohlichkeit, die die Datenspeicherung hierdurch erhalten kann, durch wirksame Transparenzregeln auffangen ...
>
> Zu den Transparenzanforderungen zählt der Grundsatz der Offenheit der Erhebung und Nutzung von personenbezogenen Daten. Eine Verwendung der Daten ohne Wissen des Betroffenen ist verfassungsrechtlich nur dann zulässig, wenn andernfalls der Zweck der Untersuchung, dem der Datenabruf dient, vereitelt wird. Für die Gefahrenabwehr und die Wahrnehmung der Aufgaben der Nachrichtendienste darf der Gesetzgeber dies grundsätzlich annehmen. Demgegenüber kommt im Rahmen der Strafverfolgung auch eine offene Erhebung und Nutzung der Daten in Betracht (vgl. § 33 Abs. 3 und 4 StPO). Ermittlungsmaßnahmen werden hier zum Teil auch sonst mit Kenntnis des Beschuldigten und in seiner Gegenwart durchgeführt (vgl. zum Beispiel §§ 102, 103, 106 StPO). Dementsprechend ist der Betroffene vor der Abfrage beziehungsweise Übermittlung seiner Daten grundsätzlich zu benachrichtigen. Eine heimliche Verwendung der Daten darf nur vorgesehen werden, wenn sie im Einzelfall erforderlich und richterlich angeordnet ist.[103]

Freilich bestehen keine flächendeckenden Benachrichtigungspflichten, wie das Bundesverfassungsgericht in seinem Urteil zur Zuordnung dynamischer IP-Adressen betont hat:

> Auch ist nicht zu beanstanden, wenn angesichts der geringen Eingriffstiefe kein spezifisches Rechtsschutzverfahren gegen Auskünfte nach den §§ 112 und 113 TKG vorgesehen ist. Rechtsschutz kann insoweit nach allgemeinen Regeln – insbesondere inzident im Zusammenhang mit Rechtsschutzverfahren gegenüber abschließenden Entscheidungen der Behörden – gesucht werden. Aus den Anforderungen des Verhältnismäßigkeitsgrundsatzes ergibt

---

[103] BVerfGE 125, 260, 334 ff. Streng für heimliche Überwachungsmaßnahmen auch BVerfG, NJW 2016, 1781, 1788, Rn. 136.

sich für Auskünfte gemäß § 112 und § 113 TKG – auch auf der Ebene der fachrechtlichen Abrufnormen, wo solche Regelungen kompetenzrechtlich anzusiedeln wären (vgl. BVerfGE 125, 260 [346 f.]) – kein flächendeckendes Erfordernis zur Benachrichtigung der von der Auskunft Betroffenen. Ob Benachrichtigungspflichten oder weitere Maßgaben wie der Vorrang der Datenerhebung beim Betroffenen für bestimmte Fälle bereits in den Abrufnormen geboten sein können, ist nicht Gegenstand des vorliegenden Verfahrens.[104]

Auch in seinem Urteil zum Antiterrordatei-Gesetz hat das Bundesverfassungsgericht die im Wesentlichen auf ein Auskunftsrecht beschränkten Transparenzregelungen nicht beanstandet, dabei aber die Wichtigkeit einer effektiven Datenschutzkontrolle betont:

Im Übrigen kennt das Antiterrordateigesetz weder einen Grundsatz der Offenheit der Datennutzung noch einen Richtervorbehalt noch eigene nachträgliche Benachrichtigungspflichten, die über die Benachrichtigungspflichten aus anderen Vorschriften hinausgehen. Es verzichtet damit auf wichtige Instrumentarien zur Gewährleistung der Verhältnismäßigkeit der Datennutzungsregelungen. Angesichts des Zwecks der Antiterrordatei ist dies jedoch verfassungsrechtlich gerechtfertigt. Die Antiterrordatei dient im Kern der Informationsanbahnung zur Vorbereitung weiterer Ermittlungen im Rahmen der Abwehr des internationalen Terrorismus. Dass solche Ermittlungen grundsätzlich nicht dem Grundsatz der Offenheit folgen können, liegt auf der Hand. Auch ein Richtervorbehalt ist im Rahmen der Antiterrordatei kein geeignetes Mittel, das verfassungsrechtlich geboten wäre. Wegen der geringen rechtlichen Durchformung der Befugnisse gemäß § 5 Abs. 1 ATDG und der Eilbedürftigkeit der Entscheidung bei einem Zugriff gemäß § 5 Abs. 2 ATDG würde ein richterlicher Prüfvorbehalt weitgehend leerlaufen. Ebenfalls ist das Absehen von spezifischen Benachrichtigungspflichten verfassungsrechtlich vertretbar. Eine Benachrichtigungspflicht käme ohne substantielle Beeinträchtigung der Funktionsweise der Datei nur für die Fälle in Betracht, in denen Personen endgültig aus der Datei herausgenommen werden. Der Nutzen einer derart beschränkten Benachrichtigungspflicht ist im Vergleich zum damit verbundenen Aufwand jedoch zu gering, als dass sie unter Verhältnismäßigkeitsgesichtspunkten geboten wäre.

Weil eine Transparenz der Datenverarbeitung und die Ermöglichung individuellen Rechtsschutzes durch das Antiterrordateigesetz nur sehr eingeschränkt sichergestellt werden können, kommt der Gewährleistung einer effektiven aufsichtlichen Kontrolle umso größere Bedeutung zu. Der Verhältnismäßigkeitsgrundsatz stellt deshalb an eine wirksame Ausgestaltung dieser Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis gesteigerte Anforderungen.[105]

Hinsichtlich dieser effektiven Kontrolle hat das Bundesverfassungsgericht namentlich wirksame Kontrollbefugnisse, eine adäquate Protokollierung und eine regelmäßige Kontrolle gefordert:

Die Gewährleistung einer wirksamen Aufsicht setzt zunächst sowohl auf Bundes- wie auf Landesebene mit wirksamen Befugnissen ausgestattete Aufsichtsinstanzen – wie nach geltendem Recht die Datenschutzbeauftragten – voraus. Weiter ist erforderlich, dass Zugriffe und Änderungen des Datenbestandes vollständig protokolliert werden. Dabei muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben für die Zuordnung zu dem zu kontrollierenden Vorgang enthält …

Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz kommt deren regelmäßiger Durchführung besondere Bedeutung zu und sind solche Kontrollen in angemessenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf – durchzuführen. Dies ist bei ihrer Ausstattung zu berücksichtigen.[106]

Und weiter zur Protokollierung:

Auch fehlt es an einer umfassenden Protokollierungspflicht, die es ermöglicht, die jeweiligen Überwachungsmaßnahmen sachhaltig zu prüfen (vgl. BVerfGE 133, 277 <370 Rn. 215>). Das Gesetz sieht zwar vereinzelt Protokollierungspflichten vor wie § 20k Abs. 3 BKAG für den Eingriff in informationstechnische Systeme oder § 20w Abs. 2 Satz 3 BKAG für die Zurückstellung einer Benachrichtigung. Selbst dort, wo eine Protokollierung der

---

104 BVerfGE 130, 151, 209 f.

105 BVerfGE 133, 277, 369. Siehe auch NJW 2016, 1781, 1789, Rn. 140 ff.

106 BVerfGE 133, 277, 370 f. Siehe ferner BVerfG, NJW 2016, 1781, 1789, 1799, Rn. 141, 266.

Benachrichtigung vorgesehen ist, bleibt unklar, ob sie sich auch auf die Gründe für das Absehen bezieht. Die Regelungen bleiben jedenfalls punktuell und stellen eine nachträgliche Kontrolle der Überwachungsmaßnahmen nicht hinreichend sicher. Zwar werden zumindest wichtige Ergebnisse der Datenerhebung auf der Grundlage der allgemeinen Regeln zur Aktenführung dokumentiert. Jedoch ist dies weder umfassend klar noch in Bezug auf die datenschutzrechtlichen Erfordernisse einer wirksamen Kontrolle gesetzlich geregelt. Dies fällt umso mehr für den Bereich der Gefahrenabwehr ins Gewicht, wo die Aufklärung und Abwehr von Gefahren nicht wie im Strafprozess als Ermittlungsverfahren gegen bestimmte einzelne Personen durchgeführt werden müssen. Es ist insoweit nicht ersichtlich, dass die Nachvollziehbarkeit der Datenerhebung - auch für Betroffene in etwaigen späteren Strafverfahren - sichergestellt ist. Daran ändert die richterliche Anordnung der Maßnahme nichts. Denn aus dieser ergibt sich nur die Erlaubnis zu deren Durchführung, nicht aber, ob und wie hiervon Gebrauch gemacht wurde. Im Übrigen ist anders als für das Strafverfahren in § 100b Abs. 4 Satz 2 StPO noch nicht einmal eine Unterrichtung des anordnenden Gerichts über die Ergebnisse der Ermittlungen vorgesehen.[107]

Schließlich hat das Bundesverfassungsgericht Berichtspflichten gefordert:

Zur Gewährleistung von Transparenz und Kontrolle bedarf es schließlich einer gesetzlichen Regelung von Berichtspflichten.

Da sich die Speicherung und Nutzung der Daten nach dem Antiterrordateigesetz der Wahrnehmung der Betroffenen und der Öffentlichkeit weitgehend entzieht, dem auch die Auskunftsrechte nur begrenzt entgegenwirken und weil eine effektive gerichtliche Kontrolle nicht ausreichend möglich ist, sind hinsichtlich Datenbestand und Nutzung der Antiterrordatei regelmäßige Berichte des Bundeskriminalamts gegenüber Parlament und Öffentlichkeit gesetzlich sicherzustellen. Sie sind erforderlich und müssen hinreichend gehaltvoll sein, um eine öffentliche Diskussion über den mit der Antiterrordatei ins Werk gesetzten Datenaustausch zu ermöglichen und diesen einer demokratischen Kontrolle und Überprüfung zu unterwerfen.[108]

Auch dies hat das Bundesverfassungsgericht noch vertieft:

Schließlich fehlt es für eine verhältnismäßige Ausgestaltung der angegriffenen Überwachungsbefugnisse auch an Berichtspflichten gegenüber Parlament und Öffentlichkeit (vgl. BVerfGE 133, 277 <372 Rn. 221 f.>). Weder sieht das Gesetz Berichte darüber vor, in welchem Umfang von den Befugnissen aus Anlass welcher Art von Verdachtslagen Gebrauch gemacht wurde, noch darüber, wieweit die Betroffenen hierüber benachrichtigt wurden. Da sich die Wahrnehmung der in Frage stehenden Befugnisse sowohl dem Betroffenen als auch der Öffentlichkeit weitgehend entzieht, sind solche Berichte zur Ermöglichung einer öffentlichen Diskussion und demokratischen Kontrolle in regelmäßigen Abständen verfassungsrechtlich geboten.[109]

bb) Ausgestaltung

(1) Verzicht auf eine Benachrichtigungspflicht

In Einklang mit Art. 13 Abs. 1 FluggastdatenRL finden im nationalen Recht vorgesehene Benachrichtigungsgebote keine Anwendung. Prinzipiell einschlägig ist § 56 BDSG-E (Benachrichtigung betroffener Personen):

(1) Ist die Benachrichtigung betroffener Personen über die Verarbeitung sie betreffender personenbezogener Daten in speziellen Rechtsvorschriften, insbesondere bei verdeckten Maßnahmen, vorgesehen oder angeordnet, so hat diese Benachrichtigung zumindest die folgenden Angaben zu enthalten:

1. die in § 55 genannten Angaben,

2. die Rechtsgrundlage der Verarbeitung,

3. die Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Fristen,

---

[107] BVerfG, NJW 2016, 1781, 1799 f., Rn. 267.

[108] BVerfGE 133, 277, 372. Siehe ferner BVerfG, NJW 2016, 1781, 1789, Rn. 142 f.

[109] BVerfG, NJW 2016, 1781, 1800, Rn. 268.

4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten sowie

5. erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

(2) In den Fällen des Absatzes 1 kann der Verantwortliche die Benachrichtigung insoweit und solange aufschieben, einschränken oder unterlassen, wie andernfalls

1. die Erfüllung der in § 45 genannten Aufgaben,

2. die öffentliche Sicherheit oder

3. Rechtsgüter Dritter

gefährdet würden, wenn das Interesse an der Vermeidung dieser Gefahren das Informationsinteresse der betroffenen Person überwiegt.

(3) Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Im Fall der Einschränkung nach Absatz 2 gilt § 57 Absatz 7 entsprechend.

Diese Benachrichtigungspflicht geht jedoch gemäß § 56 Abs. 1 BDSG-E mangels Verweises im FlugDaG-E auf das BDSG-E ins Leere (Voraussetzung: „Benachrichtigung … in speziellen Rechtsvorschriften … vorgesehen oder angeordnet“); auch der BKAG-E (insb. § 74 BKAG-E) enthält keinen entsprechenden Verweis.

Wie im unionsrechtlichen Kontext auch lassen sich, gerade mit Blick auf die eingangs zitierte Rechtsprechung des Bundesverfassungsgerichts, für eine Rechtfertigung des Verzichts auf spezifische Benachrichtigungspflichten die geringere Eingriffsintensität der Fluggastdatenverarbeitung im Vergleich zur TK-Verkehrsdatenspeicherung sowie Rechtsschutzmöglichkeiten, die im Rahmen sich an die Übermittlung anschließender Maßnahmen von Polizei- bzw. Strafverfolgungsbehörden bestehen, anführen. Hinzu kommen das Auskunftsrecht des § 57 BDSG-E sowie Benachrichtigungspflichten bei Rechtsverletzung (§§ 65 f. BDSG-E). Dies steht freilich unter dem Vorbehalt einer wirksamen Datenschutzaufsicht [zu dieser sogleich, V.1.j.bb.(2)]. Erwägenswert erscheint überdies, ob nicht durch die Statuierung einer Benachrichtigungspflicht unter Gebrauchmachen von Ausnahmemöglichkeiten die Betroffenenrechte gestärkt werden könnten bei gleichzeitiger hinreichender Sicherung von öffentlichen Geheimhaltungsinteressen.

(2) Wirksame Datenschutzkontrolle

Gemäß § 11 FlugDaG-E nimmt die Aufgaben der nationalen Kontrollstelle für den Datenschutz die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wahr. Dieser kommen die in §§ 14 ff. BDSG-E verankerten Kontrollaufgaben und -befugnisse zu. Sie umfassen namentlich ein Beanstandungsrecht (§ 16 Abs. 2 BDSG-E), die Erstellung von Stellungnahmen und Tätigkeitsberichten (§ 14 Abs. 2, § 15 BDSG-E) sowie die Bearbeitung von Beschwerden

(§ 14 Abs. 1 S. 2 i.V.m. § 60 BDSG-E). Am Rande vermerkt sei, dass mit Blick auf den wesentlich umfangreicheren Befugniskatalog in Art. 47 Abs. 2 RL 2016/680 bezweifelt wird, ob die Befugnisse gemäß § 16 Abs. 2 BDSG-E unionsrechtskonform sind.[110] Zu beachten ist jedoch, dass es der BfDI, abweichend von § 16 Abs. 2 BDSG-E, gemäß 69 Abs. 2 BKAG-E möglich ist, im Anschluss an einer Beanstandung nach § 16 Abs. 2 BDSG-E „geeignete Maßnahmen anordnen, wenn dies zur Beseitigung eines erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich ist." Auch hier stellt sich jedoch die Frage, ob eine Beschränkung auf „erheblich[e]" Verstöße richtlinienkonform ist. Es bestünde die Möglichkeit, Kontrollbefugnisse im FlugDaG-E selbst einzuräumen.[111]

Mit Blick auf das Gebot einer transparenten Richtlinienumsetzung erscheint ein ausdrücklicher Verweis auf die Kontrollaufgaben und -befugnisse der §§ 14 ff. BDSG-E geboten.

Mit Blick auf die einleitend zitierten Anforderungen des Bundesverfassungsgerichts an eine wirksame und damit **regelmäßige Kontrolle** fehlt – jenseits der Erstellung und Aktualisierung der Muster (§ 4 Abs. 3 S. 8 FlugDaG-E) – das Erfordernis einer regelmäßigen Kontrolle durch den/die Bundesbeauftragte(n) für den Datenschutz und die Informationsfreiheit. § 11 FlugDaG-E ist entsprechend zu ergänzen.

§ 14 und 15 FlugDaG-E sehen umfassende **Protokollierungs- und Dokumentationspflichten** vor. Die Dokumentation ist gemäß § 15 Abs. 3 FlugDaG-E auf Anfrage vollständig der BfDI zur Verfügung zu stellen. Der Änderungsantrag der Fraktionen CDU/CSU und SPD[112] normiert die Protokollierungspflichten im FlugDa-E selbst unter Verzicht auf § 76 BDSG-E; überdies sieht § 14 Abs. 5 i.d.F. des Änderungsantrags eine Vorlagepflicht der Protokolle vor. Die Präzisierung im FlugDaG-E selbst erscheint vorzugswürdig.

Berichtspflichten sieht das FlugDaG-E – jenseits der Erstellung und Aktualisierung der Muster (§ 4 Abs. 3 S. 9 FlugDaG-E) und neben den allgemeinen Tätigkeitsberichten der BfDI (§ 15 BDSG-E) – nicht vor. Mit Blick auf das einleitend zitierte Berichtserfordernis des Bundesverfassungsgerichts ist § 11 FlugDaG-E entsprechend zu ergänzen (alternativ käme auch eine Ergänzung des § 88 BKAG-E in Betracht).

---

110 Siehe insbesondere das Positionspapier des Bundesbeauftragten für Datenschutz und Informationsfreiheit zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, abrufbar unter: https://www.bundestag.de/blob/499112/c1c5844dba7cdbb809878b7d03b676cc/18-4-824-h--18-4-788--data.pdf (20.4.2017), S. 3 f.

111 Das BDSG steht dieser Möglichkeit auch nicht entgegen, vgl. dazu Begründung, BT-Drs. 18/11325, S. 88: „Es bleibt dem Gesetzgeber unbenommen, in sicherheitsbehördlichen fachgesetzlichen Regelungen … die in Absatz 2 genannten Befugnisse weiter auszugestalten und gegebenenfalls um Durchgriffsbefugnisse auch anzureichern."

112 A-Drs. 18(4)855.

2. Einbeziehung anderer Unternehmen als Fluggesellschaften

Erwägungsgrund 33 FluggastRL stellt klar, dass diese einer Datenübermittlungspflicht für andere PNR-Daten verarbeitende Unternehmen als Fluggesellschaften nicht entgegensteht:

> Die vorliegende Richtlinie hindert die Mitgliedstaaten nicht daran, nach ihrem jeweiligen nationalen Recht eine Regelung zur Erhebung und Verarbeitung von PNR-Daten durch Wirtschaftsteilnehmer, die keine Beförderungsunternehmen sind, wie etwa Reisebüros oder Reiseveranstalter, die Dienstleistungen im Zusammenhang mit Reisen – einschließlich Flugbuchungen – erbringen, für die sie PNR-Daten erheben und verarbeiten, oder durch andere als in dieser Richtlinie angegebene Beförderungsunternehmen vorzusehen, sofern dieses nationale Recht mit dem Unionsrecht in Einklang steht.

§ 3 FlugDaG-E macht von dieser Möglichkeit Gebrauch und bestimmt:

> Für den Fall, dass andere Unternehmen, die an der Reservierung oder Buchung von Flügen oder an der Ausstellung von Flugscheinen beteiligt sind, im Rahmen ihrer Geschäftstätigkeit Fluggastdaten an Luftfahrtunternehmen übermitteln, gilt Folgendes:
>
> 1. die Luftfahrtunternehmen haben diese Fluggastdaten unbeschadet des § 2 Absatz 1 zu den in § 2 Absatz 5 Satz 1 und 2 genannten Zeitpunkten an die Fluggastdatenzentralstelle zu übermitteln;
> 2. die anderen Unternehmen haben die Fluggastdaten so rechtzeitig an das jeweilige Luftfahrtunternehmen zu übermitteln, dass eine Weiterleitung der Daten durch das Luftfahrtunternehmen zu den in § 2 Absatz 5 Satz 1 und 2 genannten Zeitpunkten an die Fluggastdatenzentralstelle erfolgen kann.

Hierbei handelt es sich um einen als Berufsausübungsregelung an Art. 12 GG zu messenden Eingriff.[113] Hinsichtlich der Rechtfertigung desselben ist zunächst festzuhalten, dass es sich um einen relativ geringfügigen Eingriff handelt, bezieht sich die Übermittlungspflicht doch nur auf solche „Fluggastdaten, die die genannten anderen Unternehmen bereits heute zur Durchführung eines Fluges über die bestehenden technischen Strukturen an die jeweiligen Luftfahrtunternehmen übermitteln."[114] Beschwerend wirkt mithin lediglich das Rechtzeitigkeitserfordernis des § 3 Nr. 2 FlugDaG-E. Die Rechtfertigungsfähigkeit dieses Eingriffs ist angesichts des vom Bundesverfassungsgericht betonten „Gestaltungsspielraum[s des Gesetzgebers], welche Pflichten zur Sicherstellung von Gemeinwohlbelangen er Privaten im Rahmen ihrer Berufstätigkeit auferlegt"[115], zu bejahen (siehe oben, IV.12.). Selbiges gilt mit Blick auf Art. 16 GRC.

3. Übermittlungszeitpunkt

Hinsichtlich des Zeitpunkts, zu welchem die Fluggastdaten seitens der Luftfahrtunternehmen an die PNR-Zentralstelle übermittelt werden müssen, heißt es in § 2 Abs. 5 des FlugDaG-E:

> Die Luftfahrtunternehmen haben die Fluggastdaten der Fluggastdatenzentralstelle nach Absatz 7 Satz 1 zu übermitteln:
>
> 1. 48 bis 24 Stunden vor der planmäßigen Abflugzeit und

---

113 Näher zu Eingriffen in die Berufsfreiheit und Rechtfertigungsanforderungen: *F. Wollenschläger*, in: R. Schmidt/ders. (Hrsg.), Kompendium Öffentliches Wirtschaftsrecht, 4. Aufl. 2016, § 2, Rn. 43 ff.

114 Begründung, BT-Drs. 18/11501, S. 25.

115 BVerfGE 125, 260, 361 f.

2. unmittelbar nachdem sich die Fluggäste vor dem Start an Bord des Luftfahrzeugs begeben haben und sobald keine Fluggäste mehr an Bord kommen oder von Bord gehen können.

Sind zu einem Fluggast im Zeitpunkt der Übermittlung nach Satz 1 Nummer 1 keine Fluggastdaten vorhanden, so hat das Luftfahrtunternehmen die Fluggastdaten dieses Fluggastes der Fluggastdatenzentralstelle *spätestens zwei Stunden vor der geplanten Abflugzeit nachzumelden, sofern diese Daten dem Luftfahrtunternehmen bis zu diesem Zeitpunkt vorliegen* [Hervorhebung nicht im Original]; Satz 1 Nummer 2 bleibt unberührt. Die Übermittlung der Daten nach Satz 1 Nummer 2 kann auf eine Aktualisierung der übermittelten Daten nach Satz 1 Nummer 1 beschränkt werden.

In Art. 8 Abs. 3 und 4 der FluggastdatenRL[116] ist eine solche weitere Übermittlung („spätestens zwei Stunden vor Abflug") hingegen nicht vorgesehen, so dass das Umsetzungsgesetz in diesem Fall über den Wortlaut der Richtlinie hinausgeht. Art. 8 Abs. 3 FluggastdatenRL bezieht sich jedoch nur auf solche PNR-Daten, die zu den genannten Zeitpunkten auch schon verfügbar sind. Eine Regelung zu solchen Daten, die erst zu einem späteren Zeitpunkt vorliegen, trifft die Richtlinie nicht. In der Richtlinie sind zudem keine Anhaltspunkte für ein Verbot der Nachlieferung dieser Daten erkennbar, so dass daher die Einführung dieses zusätzlichen Übermittlungszeitpunktes zulässig ist.[117]

4. Straftatenkatalog

a) Erfasste Straftaten

Angesichts des Erfordernisses hinreichend gewichtiger Bezugstaten erscheint die Einbeziehung aller Betrugstaten sehr weitgehend, ebenso das Fehlen einer Erheblichkeitsschwelle im Einzelfall (dazu oben, IV.7.a und V.1.g). Daher sei angeregt, den Betrugstatbestand auf hinreichend schwere Begehungsformen zu beschränken, und eine Erheblichkeitsschwelle im Einzelfall für die Datenübermittlung an Behörden und den Datenabruf zu prüfen.

b) Bestimmtheit

Während § 4 Abs. 1 Nr. 1–4 FlugDaG-E auf konkrete Straftatbestände Bezug nehmen:

1. eine Straftat nach § 129a, auch in Verbindung mit § 129b, des Strafgesetzbuchs,

---

116 Art. 8 FluggastdatenRL lautet: … (3) Die Fluggesellschaften übermitteln die PNR-Daten auf elektronischem Wege unter Verwendung der nach dem Prüfverfahren des Artikels 17 Absatz 2 festzulegenden gemeinsamen Protokolle und unterstützten Datenformate oder bei technischen Störungen auf jede andere geeignete Weise, die ein angemessenes Datensicherheitsniveau gewährleistet, und zwar a) 24 bis 48 Stunden vor der planmäßigen Abflugzeit sowie b) sofort nach Abfertigungsschluss, d. h., unmittelbar nachdem sich die Fluggäste vor dem Start an Bord des Flugzeugs begeben haben und keine Fluggäste mehr an Bord kommen oder von Bord gehen können. (4) Die Mitgliedstaaten gestatten den Fluggesellschaften, die Übermittlung nach Absatz 3 Buchstabe b auf Aktualisierungen der gemäß Absatz 3 Buchstabe a übermittelten Daten zu beschränken.

117 Insgesamt kritisch zur mit einem zusätzlichen Übermittlungszeitpunkt einhergehenden uneinheitlichen Rechtslage und der Impraktikabilität des zusätzlichen Übermittlungszeitpunktes: Aktualisierte Stellungnahme des Bundesverbandes der Deutschen Luftverkehrswirtschaft (BDL) zum Gesetzesentwurf der Bundesregierung Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG) vom 23. März 2017, S. 4.

2. eine in § 129a Absatz 1 Nummer 1 und 2, Absatz 2 Nummer 1 bis 5 des Strafgesetz-buchs bezeichnete Straftat, wenn diese bestimmt ist, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen kann,

3. eine Straftat, die darauf gerichtet ist, eine der in Nummer 2 bezeichneten Straftaten anzudrohen,

4. eine Straftat nach den §§ 89a bis 89c und nach § 91 des Strafgesetzbuchs,

enthalten § 4 Abs. 1 Nr. 5 und 6 FlugDaG-E Verweise auf EU-Normen, die lediglich bestimmte (strafbare) Handlungen in Bezug nehmen, ohne konkrete deutsche Straftatbestände zu nennen:

5. eine Straftat im unmittelbaren Zusammenhang mit terroristischen Aktivitäten nach Artikel 3 Absatz 2 des Rahmenbeschlusses 2002/475/JI des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung (ABl. EG Nr. L 164 S. 3), der zuletzt durch Artikel 1 Nummer 1 des Rahmenbeschlusses 2008/919/JI (ABl. L 330 vom 9.12.2008, S. 21) geändert worden ist, oder

6. eine Straftat, die einer in Anhang II der Richtlinie 2016/681 aufgeführten strafbaren Handlung entspricht und die mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht ist.

In seinem Urteil zur TK-Verkehrsdatenspeicherung hat das Bundesverfassungsgericht eine „Generalklausel oder lediglich die Verweisung auf Straftaten von erheblicher Bedeutung“ als verfassungsrechtlich ungenügend erachtet.[118] Angesichts der Bezugnahme auf konkrete Handlungen und nicht lediglich auf abstrakte Kategorien namentlich einer hinreichenden Schwere der Straftat lässt sich das verfassungsrechtliche Mindesterfordernis an Bestimmtheit für noch gewahrt erachten, zumal im verfassungsrechtlichen Kontext eine Lockerung von Bestimmtheitsanforderungen im nationalen Recht anerkannt ist, so im EU-Recht hinreichend bestimmte Vorgaben bestehen[119]. Gleichwohl sollte zur Erhöhung der Bestimmtheit ein Straftatenkatalog formuliert werden.[120]

5. Datensicherheit

Im FlugDaG-E findet sich keine explizite Regelung zur in der FluggastdatenRL geforderten Datensicherheit (siehe insoweit oben, IV.9.). Dies begründet die Gesetzesbegründung mit der generellen Anwendbarkeit des BDSG:

Da das Bundesdatenschutzgesetz unmittelbare Anwendung findet, gelten insbesondere auch die dortigen Vorschriften … zur Datensicherheit … bei der Verarbeitung von Fluggastdaten im Rahmen des Fluggastdaten-Informationssystems.[121]

---

118 BVerfGE 125, 260, 328 f.

119 Nämlich im Kontext des Art. 80 Abs. 1 GG (Beispiele: § 6a Abs. 1 WHG; § 16 Abs. 6 GenTG; § 48a Abs. 1 BImSchG; § 53 Abs. 1 BNatSchG; § 62 LFGB): BVerwGE 121, 382, 386 ff.; *I. Härtel*, JZ 2007, 431, 432 ff.; *T. Klink*, Pauschale Ermächtigung zur Umsetzung von Europäischem Gemeinschaftsrecht mittels Rechtsverordnung, 2005, S. 163 ff.; *F. Ossenbühl*, DVBl. 1999, 1, 6 f. A.A. *R. Breuer*, ZfW 1999, 220, 225 ff.; *J. Saurer*, JZ 2007, 1073, 1074 ff.

120 So auch Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681, https://www.bundestag.de/blob/503038/628d1d052f362f0740fb7f5f6f1d032a/18-4-869-a-data.pdf (20.4.2017), S. 5.

121 Begründung, BT-Drs. 18/11501, S. 36.

Einschlägig ist § 64 BDSG-E (Anforderungen an die Sicherheit der Datenverarbeitung), der den unionsrechtlichen Anforderungen genügt.[122] Aufgrund der Bezugnahme auf den „Stan[d] der Technik" und die Verpflichtung zur Berücksichtigung der „einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik" in § 64 Abs. 1 BDSG-E ist davon auszugehen, dass ein angemessenes Sicherheitsniveau gewährleistet wird.

Mit Blick auf das Gebot einer transparenten Richtlinienumsetzung[123] erscheint indes ein ausdrücklicher Verweis auf § 64 BDSG-E geboten.

6. Weitere Datenschutzregelungen

Mit Blick auf das Gebot einer transparenten Richtlinienumsetzung erscheint auch ein expliziter Verweis auf die weiteren von der FluggastdatenRL vorgegebenen Datenschutzvorkehrungen angezeigt, namentlich:

- Aufgaben und Befugnisse des Datenschutzbeauftragten der Fluggastdatenzentralstelle (§ 7 BDSG-E, § 71 f. BKAG-E);
- Auskunftsrecht (§ 57 BDSG-E);[124]
- Benachrichtigungspflichten bei Rechtsverletzung (§§ 65 f. BDSG-E);
- Recht auf Berichtigung, Löschung oder Sperrung (§ 58 BDSG-E);
- Recht auf Schadenersatz (§§ 83 BDSG-E, 86 BKAG-E);
- Rechtsbehelfe (§§ 60 f. BDSG-E).

---

122 Kritisch zu den in § 64 Abs. 2 und 3 BDSG beispielhaften Aufzählungen, Positionspapier des Bundesbeauftragten für Datenschutz und Informationsfreiheit zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, abrufbar unter: https://www.bundestag.de/blob/499112/c1c5844dba7cdbb809878b7d03b676cc/18-4-824-h--18-4-788--data.pdf (20.4.2017), S. 20 ff.: „fachlich als veraltet anzusehen" und „an den technischen Möglichkeiten vorbei[gehend]".

123 Siehe zu diesem EuGH, Rs. C-16/95, Slg. 1995, I-4883 – Kommission/Spanien; Rs. C-220/94, Slg. 1995, I-1589 – Kommission/Luxemburg; siehe auch *M. Nettesheim*, in: E. Grabitz/M. Hilf/ders. (Hrsg.), Das Recht der Europäischen Union, 60. EL 2016, Art. 288 AEUV Rn. 120.

124 Kritisch zur Verfassungskonformität der Ausnahmeklausel des Art. 57 Abs. 7 S. 3 BDSG-E *H. Aden*, Stellungnahme zum Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, https://www.bundestag.de/blob/500874/6cf1062c31311c6f0f88a22748f695bd/18-4-824-g-data.pdf (21.4.2017), S. 7 f.

7. Fluggastdatenzentralstelle und Auftragsdatenverarbeitung

Gemäß Art. 4 Abs. 1 der FluggastdatenRL haben die Mitgliedstaaten eine für die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten und schwerer Kriminalität zuständige Behörde oder eine Abteilung einer solchen Behörde zu errichten oder zu benennen, die als die PNR-Zentralstelle handelt.

§ 1 Abs. 1 FlugDaG-E legt fest, dass das Bundeskriminalamt die zuständige nationale zentrale Stelle für die Verarbeitung von Fluggastdaten ist, und § 1 Abs. 3 FlugDaG-E legt fest, dass das Bundesverwaltungsamt die Fluggastdaten im Auftrag und nach Weisung des BKA verarbeitet.

Das Bundesverwaltungsamt ist insofern Auftragsdatenverarbeiter für das BKA, so dass die Vorgaben der Art. 22 ff. JI-Richtlinie und deren nationale Umsetzungsakte zu beachten sind. In der Gesetzesbegründung zu § 1 Abs. 3 FlugDaG-E heißt es dazu:

> Als Auftragsverarbeiter nimmt das Bundesverwaltungsamt die Fluggastdaten zentral entgegen, bereitet sie technisch auf, gleicht sie nach den fachlichen Vorgaben der Fluggastdatenzentralstelle automatisiert ab und sichtet sie in technischer Hinsicht. Hierdurch wird sichergestellt, dass das Bundesverwaltungsamt nur qualitativ hochwertige Treffer zu relevanten Personen an die Fluggastdatenzentralstelle weiterleitet, das die Daten fachlich validiert und weiter verdichtet. Beim Bundesverwaltungsamt verbleiben dagegen ca. 99,9 Prozent der Datensätze, bei denen sich keine Treffer ergeben haben. Sie werden nur im konkreten Einzelfall retrograd weiter genutzt.[125]

Hinsichtlich der von GA *Menozzi* geforderten[126] Notwendigkeit einer Regelung, die eine hinreichend klare und präzise Bestimmung der zur Verarbeitung von PNR-Daten zuständigen Behörde ermöglicht, wirft die Aufgabenverteilung zwischen Bundeskriminalamt und Bundesverwaltungsamt infrage gestellt. So kritisiert etwa der Deutsche Richterbund, dass es nach der vorliegenden Regelung vollständig dem Bundeskriminalamt überlassen ist, zu entscheiden, inwieweit das Bundesverwaltungsamt die Fluggastdaten verarbeitet.[127] Insofern ist allerdings zu beachten, dass hier das zukünftige BDSG-E[128] Anwendung finden wird und daher auch dessen §§ 62 ff. zu berücksichtigen sind. Von Bedeutung ist dabei insbesondere § 62 Abs. 5 BDSG-E, der bestimmt, dass die „Verarbeitung durch einen Auftragsverarbeiter … auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments zu erfolgen [hat], der oder das den Auftragsverarbeiter an den Verantwortlichen bindet und der oder das den Gegenstand, die Dauer, die Art

---

125 Begründung, BT-Drs. 18/11501, S. 25 f.

126 Vgl. GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 328.

127 So auch die Stellungnahme des Deutschen Richterbundes zum Referentenentwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG) vom Dezember 2016, Nr. 22/16, abrufbar unter http://www.drb.de/fileadmin/docs/Stellungnahmen/2016/DRB_161205_Stn_Nr_22_Umsetzung_Fluggastdatenrichtlinie.pdf (11.4.2017), S. 3

128 Abrufbar unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/entwurf-datenschutzgrundverordnung.pdf?__blob=publicationFile (13.4.2017).

und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen festlegt." Auch die Gesetzesbegründung zum FlugDaG-E verweist insofern auf eine solche nach Maßgabe des § 62 des zukünftigen BDSG auszugestaltenden Vereinbarung zwischen Bundeskriminalamt und Bundesverwaltungsamt:

> Die Einzelheiten der Verarbeitung von Fluggastdaten durch das Bundesverwaltungsamt als Auftragsverarbeiter werden entsprechend den gesetzlichen Vorgaben des § 62 des künftigen Bundesdatenschutzgesetzes (BDSG-E) an eine Auftragsdatenverarbeitung in einer Vereinbarung festgelegt, die das Bundesverwaltungsamt an die Fluggastdatenzentralstelle bindet. In der Vereinbarung sind unter anderem der Gegenstand, die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten der Fluggastdatenzentralstelle zu regeln. Dabei wird insbesondere entsprechend den gesetzlichen Vorgaben zur Auftragsdatenverarbeitung vorgesehen, dass das Bundesverwaltungsamt auf Weisung der Fluggastdatenzentralstelle handelt, sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichten und das Bundesverwaltungsamt der Fluggastdatenzentralstelle die erforderlichen Informationen zum Nachweis der Einhaltung der Vereinbarung zur Verfügung stellt.[129]

Es ist davon auszugehen, dass durch diese Vereinbarung eine hinreichend klare Aufgabeverteilung sichergestellt wird.

Mit Blick auf den Kreis der Zugangsberechtigten ist zu beachten, dass gemäß § 64 Abs. 3 BDSG-E Zugangs- und Zugriffskontrollen zur Gewährleistung der Datensicherheit vorgesehen sind.[130] Hinzuweisen ist zudem auf § 15 Abs. 2 Nr. 1 FlugDaG-E, der die „Namen und die Kontaktdaten der Fluggastdatenzentralstelle und der Mitarbeiterinnen und Mitarbeiter der Fluggastdatenzentralstelle, die mit der Verarbeitung der Fluggastdaten beauftragt sind, und die verschiedenen Ebenen der Zugangsberechtigungen" explizit der Dokumentationspflicht unterwirft. Diese Protokolle sind auf Anfrage zudem vollständig der nationalen Kontrollstelle (hier der BfDI) zur Verfügung zu stellen. Insgesamt ist daher von einer hinreichenden Begrenzung des Kreises der Zugangsberechtigten auszugehen.

8. Speicherort im Hoheitsgebiet der Mitgliedstaaten

Die in Art. 6 Abs. 8 der FluggastdatenRL enthaltene Vorgabe, dass eine Speicherung, Verarbeitung und Auswertung von PNR-Daten durch die PNR-Zentralstelle ausschließlich an einem gesicherten Ort bzw. gesicherten Orten *im Hoheitsgebiet der Mitgliedstaaten* zu erfolgen hat, fehlt im FlugDaG-E. Die Aufnahme dieser Vorschrift in das FlugDaG-E ist mit Blick auf die FluggastdatenRL und die Notwendigkeit eines hohen Standards an Datenschutz und Datensicherheit erforderlich, mag aufgrund der Zuständigkeitsregelungen auch eine Speicherung im Inland naheliegen.

---

129 Begründung, BT-Drs. 18/11501, S. 25.

130 Siehe dazu schon oben, V.5.

9. Aufgabe der Zweckbindung im Kontext der Strafverfolgung (§ 6 Abs. 4 FlugDaG-E)

Gemäß § 6 Abs. 3 FlugDaG-E dürfen die Empfangsbehörden „die übermittelten Daten nur zu den Zwecken, zu denen sie ihnen übermittelt worden sind, verarbeiten", d.h. zur Verhütung oder Verfolgung terroristischer Straftaten und schwerer Kriminalität. In Umsetzung von Art. 7 Abs. 5 FluggastdatenRL relativiert § 6 Abs. 4 FlugDaG-E diese strenge Zweckbindung für Strafverfolgungsbehörden:

> Die in Absatz 1 Satz 1 genannten Behörden können, soweit sie Aufgaben der Strafverfolgung wahrnehmen, die übermittelten Daten zu anderen Zwecken verarbeiten, wenn Erkenntnisse, auch unter Einbezug weiterer Informationen, den Verdacht einer bestimmten anderen Straftat begründen.

Die damit einhergehende Aufgabe der eingangs erwähnten Zweckbindung (Bekämpfung terroristischer Straftaten und schwerer Kriminalität) ist nicht nur unionsrechtlich, sondern auch verfassungsrechtlich mit Blick auf die namentlich im Urteil zum BKA-Gesetz formulierten Anforderungen an eine Zweckänderung problematisch.[131]

Die Gesetzesbegründung relativiert diese Aufgabe der Zweckbindung mit Blick auf den in § 16 FlugDaG-E enthaltenen Verweis auf das BKAG:

> Absatz 4 dient der Konkretisierung von Artikel 7 Absatz 5 der Richtlinie (EU) 2016/681. Absatz 4 bestimmt, dass die in Absatz 1 Satz 1 genannten Behörden, soweit sie Aufgaben der Strafverfolgung wahrnehmen, die von der Fluggastdatenzentralstelle übermittelten Daten ausnahmsweise zu anderen Zwecken als den der Übermittlung zugrundeliegenden Zwecken verarbeiten können, wenn Erkenntnisse, auch unter Einbezug weiterer Informationen, den Verdacht einer bestimmten anderen Straftat begründen. Hierbei ist über § 17 insbesondere der Grundsatz der hypothetischen Datenneuerhebung nach § 12 Absatz 2 des künftigen Bundeskriminalamtgesetzes zu berücksichtigen.[132]

Der in Bezug genommene § 12 Abs. 2 BKAG-E lautet:

> Das Bundeskriminalamt kann zur Erfüllung seiner Aufgaben personenbezogene Daten zu anderen Zwecken, als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten, wenn
>
> 1. mindestens
>
> a) vergleichbar schwer wiegende Straftaten verhütet, aufgedeckt oder verfolgt oder
>
> b) vergleichbar bedeutsame Rechtsgüter geschützt werden sollen und
>
> 2. sich im Einzelfall konkrete Ermittlungsansätze
>
> a) zur Verhütung, Aufdeckung oder Verfolgung solcher Straftaten ergeben oder
>
> b) zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter erkennen lassen.
>
> Die §§ 21 und 22 bleiben unberührt.

Mag diese Norm auch eine Zweckänderung begrenzen, so ist doch zu berücksichtigen, dass sie das BKA adressiert, vorliegend jedoch eine Verwendung bereits übermittelter Daten (auch) durch andere Behörde als das BKA infrage steht. Überdies könnte jedenfalls der Wortlaut des

---

131 BVerfG, NJW 2016, 1781, 1801 f., Rn. 284 ff. Siehe ferner E 125, 260, 333; E 133, 277, 323 f., Rn. 114.

132 Begründung, BT-Drs. 18/11501, S. 30.

§ 16 FlugDaG-E eine Unanwendbarkeit des § 12 Abs. 2 BKAG-E nahelegen, da § 6 Abs. 4 FlugDaG-E als Spezialregelung verstanden werden könnte; § 16 FlugDaG-E stellt die entsprechende Anwendbarkeit des BKA-G unter den Vorbehalt, dass im FlugDaG „keine spezielleren Regelungen enthalten sind."

Unabhängigkeit davon verbietet sich jedenfalls aus Gründen der Normklarheit und eines effektiven Grundrechtsschutzes, im Wortlaut nicht angelegte, aber grundrechtlich bedeutsame Kautelen über einen nur mittels der Gesetzesbegründung erschließbaren Verweis einzuführen. Daher ist § 6 Abs. 4 FlugDaG-E in Einklang mit der Intention des Gesetzgebers umzuformulieren:

Die in Absatz 1 Satz 1 genannten Behörden können, soweit sie Aufgaben der Strafverfolgung wahrnehmen, die übermittelten Daten zu anderen Zwecken verarbeiten, wenn

1. mindestens vergleichbar schwer wiegende Straftaten verfolgt und

2. sich im Einzelfall konkrete Ermittlungsansätze zur Verfolgung solcher Straftaten ergeben.

10. Anordnungsbefugnis bei Gefahr im Verzug

Nach § 5 Abs. 3 S. 2 FlugDaG-E kann bei Gefahr im Verzug die Präsidentin oder der Präsident des Bundeskriminalamtes oder ihre oder seine Vertretung die Genehmigung zur Depersonalierung erteilen. Kritisiert wird dies, da keine Kontrolle durch Dritte stattfindet.[133] Indes ist gemäß § 5 Abs. 3 S. 3 FlugDaG-E in einem solchen Fall die gerichtliche Entscheidung unverzüglich nachzuholen. Zudem ist es auch unionsrechtlich zulässig, „in hinreichend begründeten Eilfällen" vom Erfordernis der Vorabkontrolle abzusehen.[134] Ferner wird infrage gestellt, ob diese Eilkompetenz mit der Richtlinie selbst vereinbar ist.[135] Art. 12 Abs. 3 S. 1 lit. b Nr. ii FluggastdatenRL spricht diesbezüglich ausdrücklich von einer „anderen" Behörde. Eine Ausnahme für Eilfälle ist zwar gerade nicht vorgesehen, allerdings kann sich „andere" im Kontext des Art. 12 Abs. 3 S. 1 lit. b Nr. ii FluggastdatenRL auch darauf beziehen, dass neben den in Nr. i genannten Justizbehörden auch eine „andere nationale Behörde" als eine Justizbehörde zuständig ist; eine

---

133 So auch die Stellungnahme des Deutschen Richterbundes zum Referentenentwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG) vom Dezember 2016, Nr. 22/16, abrufbar unter http://www.drb.de/fileadmin/docs/Stellungnahmen/2016/DRB_161205_Stn_Nr_22_Umsetzung_Fluggastdatenrichtlinie.pdf (11.4.2017), S. 3. Kritisch zur Eilfallkompetenz des Präsidenten des Bundeskriminalamts in § 20l Abs. 3 S. 2 BKAG a.F. *M. Thiel*, Die „Entgrenzung" der Gefahrenabwehr, 2011, S. 342 ff.

134 EuGH, verb. Rs. C-203/15 u. C-698/15, EU:C:2016:970, Rn. 120 – Tele2 Sverige u.a.

135 Stellungnahme des Deutschen Richterbundes zum Referentenentwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG) vom Dezember 2016, Nr. 22/16, abrufbar unter http://www.drb.de/fileadmin/docs/Stellungnahmen/2016/DRB_161205_Stn_Nr_22_Umsetzung_Fluggastdatenrichtlinie.pdf (11.04.2017), S. 3.

nachträgliche gerichtliche Kontrolle ist der dort genannten Ex-post-Kontrolle zumindest gleichwertig.

11. Benachrichtigungspflichten bei Rechtsverletzungen

Art. 13 Abs. 8 FluggastdatenRL sieht eine (beschränkte) Benachrichtigungspflicht Betroffener bei Rechtsverletzungen vor:

> Die Mitgliedstaaten sorgen dafür, dass die PNR-Zentralstelle die betroffene Person und die nationale Kontrollstelle unverzüglich von einer Verletzung des Schutzes personenbezogener Daten benachrichtigt, wenn diese Verletzung voraussichtlich ein hohes Risiko für den Schutz der personenbezogenen Daten oder eine Verletzung der Privatsphäre der betroffenen Person zur Folge hat.

Im FlugDaG-E findet sich keine explizite Regelung zu entsprechenden Benachrichtigungspflichten, was die Gesetzesbegründung mit der generellen Anwendbarkeit des BDSG begründet:

> Da das Bundesdatenschutzgesetz unmittelbare Anwendung findet, gelten insbesondere auch die dortigen Vorschriften zum Datenschutz, zur Datensicherheit und zu den Rechten der Betroffenen bei der Verarbeitung von Fluggastdaten im Rahmen des Fluggastdaten-Informationssystems.[136]

Einschlägig sind § 65 (Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den Bundesbeauftragten) und § 66 (Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten) BDSG-E. Festzuhalten ist zum einen, dass § 66 Abs. 3 ff. BDSG-E Ausnahmetatbestände enthält, die Art. 13 Abs. 8 FluggastdatenRL seinem Wortlaut nach nicht kennt (wohl aber Art. 31 Datenschutz-RL 2016/680/EU, den Art. 13 Abs. 1 FluggastdatenRL i.V.m. Art. 59 Datenschutz-RL 2016/680/EU in Bezug nimmt). Zum anderen ist, wie im Kontext des allgemeinen Datenschutzrechts auch,[137] eine von Art. 13 Abs. 8 FluggastdatenRL abweichende Terminologie zu verzeichnen: Art. 13 Abs. 8 FluggastdatenRL verlangt, dass eine Benachrichtigungspflicht besteht, wenn eine Verletzung (des Schutzes personenbezogener Daten) voraussichtlich „ein hohes Risiko" für den Schutz personenbezogener Daten oder eine Verletzung der Privatsphäre zur Folge hat. Mit dem Verweis auf § 66 Abs. 1 BDSG wird diese Benachrichtigungspflicht auf Fälle beschränkt, bei denen eine „erhebliche Gefahr" für Rechtsgüter der betroffenen Person besteht.

---

136 Begründung, BT-Drs. 18/11501, S. 36.

137 Kritisch zur verwendeten Terminologie („Gefahr"; Richtlinie: „Risiko") im BDSG-E, *C. Piltz*, zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, abrufbar unter: https://www.bundestag.de/blob/499522/5906693d148b00ac6b768ec9b09070b2/18-4-824-c-data.pdf (20.4.2017), S. 34.

12. Sanktionen

Gemäß Art. 14 der FluggastdatenRL ist es den Mitgliedstaaten überlassen, die Ausgestaltung der erforderlichen Sanktionen zu regeln:

> Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen die gemäß dieser Richtlinie erlassenen nationalen Vorschriften zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen.
>
> Insbesondere erlassen die Mitgliedstaaten Vorschriften über Sanktionen einschließlich Geldbußen gegen Fluggesellschaften, die die Daten nicht gemäß Artikel 8 übermitteln oder hierzu nicht das vorgeschriebene Format verwenden.
>
> Die vorgesehenen Sanktionen müssen wirksam, angemessen und abschreckend sein.

Der Umsetzungsgesetzgeber hat in § 18 des FlugDaG-E eine Bußgeldvorschrift zur Umsetzung des Art. 14 FluggastdatenRL eingeführt:

> (1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig
>
> 1. entgegen § 2 Absatz 5 Satz 1 in Verbindung mit § 2 Absatz 2 Nummer 1 bis 8 dort genannte Fluggastdaten nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig übermittelt, oder
>
> 2. entgegen § 2 Absatz 5 Satz 2 erster Halbsatz in Verbindung mit § 2 Absatz 2 Nummer 1 bis 8 dort genannte Fluggastdaten nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig nachmeldet.
>
> (2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.
>
> (3) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesverwaltungsamt.

Entgegen der Kritik[138] ist die Festlegung eines Bußgeldrahmens bis 50.000 € mit Blick auf unternehmerische Grundrechte (Art. 16 GRC) angemessen, zumal die Luftfahrtunternehmen lediglich angehalten werden, Daten, die sie ohnehin schon zu eigenen Geschäftszwecken erheben und verarbeiten, den Fluggastdatenzentralstellen zur Verhütung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität zur Verfügung zu stellen.[139]

13. Abgleich mit Mustern und Datenbanken

In Ergänzung zu den Ausführungen zur Grundrechtskonformität des (unionsrechtlich zwingend vorgegebenen) Abgleichs mit Mustern (siehe oben, IV.7.b)[140] ist darauf hinzuweisen, dass § 4 Abs. 3 FlugDaG-E diesen in Umsetzung des unionsrechtlichen Konkretisierungsauftrags (siehe Art. 6 Abs. 4, EG 7 FluggastdatenRL) einhegt.

---

138 Bundesverband der Deutschen Luftverkehrswirtschaft (BDL) in seiner Stellungnahme vom 23.3.2017: Bemessung des Sanktionsrahmens anhand des bestehenden Rahmens des § 17 OWiG.

139 Vgl. dazu auch die Sanktionsrahmen in ähnlichen Gesetzen: § 18 LuftSiG-E (Geldbuße bis zu 30.000 Euro bzw. bis zu 10.000 Euro) oder § 149 Abs. 2 S. 1 Nr. 1 TKG (Geldbuße bis 500.000 Euro).

140 Kritisch Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681, https://www.bundestag.de/blob/503038/628d1d052f362f0740fb7f5f6f1d032a/18-4-869-a-data.pdf (20.4.2017), S. 4 f.

So dürfen die Muster nicht nur „verdachtsbegründende", sondern müssen auch „verdachtsentlastende Prüfungsmerkmale" enthalten (§ 4 Abs. 3 S. 2, 5 FlugDaG-E); beide Kategorien sind zudem so „zu kombinieren, dass die Zahl der unter ein Muster fallenden Personen möglichst gering ist" (§ 4 Abs. 3 S. 6 FlugDaG-E). Zur hinreichenden Fundierung müssen verdachtsbegründende Prüfungsmerkmale gemäß § 4 Abs. 3 S. 3 f. FlugDaG-E überdies „auf den Tatsachen zu bestimmten Straftaten [beruhen], die den [Empfangsb]ehörden vorliegen" und „geeignet sein, Personen zu identifizieren, die für die Verhütung oder Verfolgung der in Absatz 1 genannten Straftaten bedeutsame Prüfungsmerkmale erfüllen." Des Weiteren verlangt § 4 Abs. 3 S. 7 FlugDaG-E, dass bestimmte sensible Merkmale nicht Gegenstand eines Prüfungsmerkmals sein dürfen.

In prozeduraler Hinsicht ist festzuhalten, dass § 4 Abs. 3 S. 1 FlugDaG-E eine Erstellung der Muster „unter Einbeziehung der oder des Datenschutzbeauftragten der Fluggastdatenzentralstelle" verlangt, ebenso wie eine regelmäßige Prüfung „in Zusammenarbeit mit den [Empfangsb]ehörden sowie mit der oder dem Datenschutzbeauftragten der Fluggastdatenzentralstelle …, mindestens alle sechs Monate". Zudem kontrolliert „[d]ie oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit … die Erstellung und Anwendung der Muster mindestens alle zwei Jahre" und „erstattet der Bundesregierung alle zwei Jahre Bericht" (§ 4 Abs. 3 S. 8 f. FlugDaG-E).[141]

Hinsichtlich der Datenbestände, mittels derer ein automatisierter Abgleich durchgeführt werden darf, ist festzuhalten, dass § 4 Abs. 2 S. 1 Nr. 1 FlugDaG-E (anders als die Gesetzesbegründung[142]) keine bestimmten Datenbanken nennt, sondern einen Abgleich „mit Datenbeständen, die der Fahndung oder Ausschreibung von Personen oder Sachen dienen", zulässt. Hier kann eine Präzisierung zur Erhöhung der Bestimmtheit erwogen werden.[143] Ebenso fehlt der von GA *Mengozzi* geforderte Ausschluss sensibler Merkmale.[144]

---

141 Die BfDI spricht sich dafür aus, dass der Bericht auch an den Bundestag zu richten ist, Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681, https://www.bundestag.de/blob/503038/628d1d052f362f0740fb7f5f6f1d032a/18-4-869-a-data.pdf (20.4.2017), S. 4 f.

142 Siehe Begründung, BT-Drs. 18/11501, S. 26: „Hierbei kommt insbesondere ein Abgleich mit den Datenbeständen des ‚Schengener Informationssystems' (SIS), von ‚INPOL-zentral' (INPOL-Z) und der ‚Automated Search Facility – Stolen and Lost Travel Documents Database' (ASF-SLTD) in Betracht."

143 Siehe Commission Staff Working Document v. 28.11.2016, SWD(2016) 426 final, abrufbar unter: https://ec.europa.eu/transparency/regdoc/rep/10102/2016/EN/SWD-2016-426-F1-EN-MAIN.PDF (7.4.2017), S. 3: "In drawing up their regulatory framework, Member States should consider providing for: A clear indication of the databases against which PNR data may be compared within the meaning of Article 6(3)(a); …".

144 GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 258.

Darüber hinaus sind – wie bei der Erstellung und Aktualisierung der Muster (§ 4 Abs. 3 S. 8 f. FlugDaG-E) – eine regelmäßige Kontrolle und Berichtspflichten vorzusehen [siehe bereits oben, V.1.j.bb.(2)].[145]

Schließlich legt § 4 Abs. 2 S. 2 FlugDaG-E sowohl für den Abgleich mit Datenbanken als auch für den Abgleich mit Mustern explizit fest, dass Treffer, die aus einem vorzeitigen Abgleich resultieren, von der Fluggastdatenzentralstelle individuell überprüft werden müssen.

14. Weitergabe der Daten

a) Allgemeine Anforderungen und Übermittlung im Inland

Die Nutzung der Daten durch andere Behörden stellt in der Terminologie des BKA-Gesetz-Urteils des Bundesverfassungsgerichts eine Zweckänderung und keine weitere Nutzung innerhalb der ursprünglichen Zwecksetzung dar, da die Weiternutzung nicht (lediglich) durch dieselbe Behörde im Rahmen derselben Aufgabe erfolgt.[146]

Die vom Bundesverfassungsgericht postulierten Erfordernisse der Zulässigkeit einer „hypothetischen Datenneuerhebung" bzw. „einer Gleichgewichtigkeit der neuen Nutzung"[147] sichert § 6 Abs. 3 FlugDaG-E, der eine Datenverarbeitung nach Übermittlung nur zu den ursprünglichen Erhebungszwecken, nämlich zur Verhütung oder Verfolgung terroristischer Straftaten und schwerer Kriminalität zulässt. Überdies muss die Weitergabe der Daten den Anforderungen des Bestimmtheitsgebots genügen. Die möglichen Adressaten einer Übermittlung müssen dabei „auf der Grundlage der Zuständigkeitsvorschriften hinreichend verlässlich bestimmbar" sein.[148] Dies sichert die abschließende Aufzählung in § 6 Abs. 1 und Abs. 2 FlugDaG-E.

Erforderlich ist ferner „eine sachhaltige Protokollierung und eine effektive Kontrolle durch die Bundesdatenschutzbeauftrage".[149] Hinsichtlich der effektiven Kontrolle und Modifikationserfordernissen kann nach oben verwiesen werden [siehe V.1.j.bb.(2)]. §§ 14 f. FlugDaG-E sieht Protokollierungs- und Dokumentationspflichten vor; der Änderungsantrag der Fraktionen CDU/CSU und SPD[150] normiert die Protokollierungspflichten im FlugDa-E selbst unter Verzicht auf § 76 BDSG-E; er verwendet indes den Begriff „Übermittlung" statt „Offenlegung"

---

145 Vgl. auch GA Mengozzi, in: EuGH, Gutachten 1/15, EU:C:2016:656, Rn. 260.
146 BVerfG, NJW 2016, 1781, 1800 ff., Rn. 276 ff.
147 BVerfG, NJW 2016, 1781, 1801 f., Rn. 284 ff.
148 BVerfG, NJW 2016, 1781, 1803, Rn. 306.
149 BVerfG, NJW 2016, 1781, 1805, Rn. 322.
150 A-Drs. 18(4)855.

(Art. 13 Abs. 6 FluggastdatenRL) bzw. „Offenlegung einschließlich Übermittlung“ (§ 76 Abs. 1 Nr. 4 BDSG-E). Überdies sieht § 14 Abs. 5 i.d.F. des Änderungsantrags eine Vorlagepflicht der Protokolle vor. Die Präzisierung im FlugDaG-E selbst erscheint vorzugswürdig. Diese Bewertung gilt auch für die Nutzung durch das Bundeskriminalamt selbst.

b) Weitergabe an Drittstaaten

Gemäß § 10 Abs. 1 S. 1 FlugDaG kann die Fluggastdatenzentralstelle im Einzelfall und unter Beachtung der §§ 78 bis 80 BDSG-E (Allgemeine Voraussetzungen, Datenübermittlung bei geeigneten Garantien und Übermittlung ohne geeignete Garantien) auf Ersuchen an die Behörden von Drittstaaten übermitteln, wenn diese Behörden für die Verhütung oder Verfolgung von terroristischen Straftaten oder schwerer Kriminalität zuständig sind und die Datenübermittlung zu diesem Zweck erforderlich ist.

Für die Übermittlung an Drittstaaten verlangt das Bundesverfassungsgericht zunächst, wie im nationalen Kontext auch, hinreichend gewichtige Übermittlungs- und Nutzungszwecke.[151] Dies sichert § 10 Abs. 1 S. 1 FlugDaG-E. Darüber hinaus setzt die Weitergabe eine „Vergewisserung über einen rechtsstaatlichen Umgang mit diesen Daten im Empfängerland voraus … Im Übrigen bedarf es auch hier der Sicherstellung einer wirksamen inländischen Kontrolle … Die Anforderungen sind durch normenklare Grundlagen im deutschen Recht sicherzustellen“.[152]

Demnach setzt die Übermittlung personenbezogener Daten ins Ausland [zunächst] einen datenschutzrechtlich angemessenen und mit elementaren Menschenrechtsgewährleistungen vereinbaren Umgang mit den übermittelten Daten im Empfängerstaat (1) und eine entsprechende Vergewisserung hierüber seitens des deutschen Staates (2) voraus:

(1) Eine Übermittlung von Daten ins Ausland verlangt, dass ein hinreichend rechtsstaatlicher Umgang mit den Daten im Empfängerstaat zu erwarten ist.

(a) Für die Anforderungen an den datenschutzrechtlichen Umgang mit den übermittelten Daten ist allerdings nicht erforderlich, dass im Empfängerstaat vergleichbare Regelungen zur Verarbeitung personenbezogener Daten wie nach der deutschen Rechtsordnung gelten oder ein gleichartiger Schutz gewährleistet ist wie nach dem Grundgesetz. ...

Erlaubt ist eine Übermittlung der Daten ins Ausland jedoch nur, wenn auch durch den dortigen Umgang mit den übermittelten Daten nicht die Garantien des menschenrechtlichen Schutzes personenbezogener Daten unterlaufen werden. Dies bedeutet nicht, dass in der ausländischen Rechtsordnung institutionelle und verfahrensrechtliche Vorkehrungen nach deutschem Vorbild gewährleistet sein müssen; insbesondere müssen nicht die formellen und institutionellen Sicherungen vorhanden sein, die datenschutzrechtlich für deutsche Stellen gefordert werden (siehe oben C IV 6). Geboten ist in diesem Sinne die Gewährleistung eines angemessenen materiellen datenschutzrechtlichen Niveaus für den Umgang mit den übermittelten Daten im Empfängerstaat … In Betracht zu nehmen ist insoweit insbesondere, ob für die Verwendung der Daten die - bei der Übermittlung mitgeteilten - Grenzen durch

---

151 BVerfG, NJW 2016, 1781, 1806, Rn. 330 f.

152 BVerfG, NJW 2016, 1781, 1806, Rn. 329.

Zweckbindung und Löschungspflichten sowie grundlegende Anforderungen an Kontrolle und Datensicherheit wenigstens grundsätzlich Beachtung finden. Maßgeblich für diese Beurteilung sind die innerstaatlichen Rechtsvorschriften und die internationalen Verpflichtungen des Empfängerstaats sowie ihre Umsetzung in der täglichen Anwendungspraxis …

(b) Hinsichtlich der Besorgnis etwaiger Menschenrechtsverletzungen durch die Nutzung der Daten im Empfängerstaat muss insbesondere gewährleistet erscheinen, dass sie dort weder zu politischer Verfolgung noch unmenschlicher oder erniedrigender Bestrafung oder Behandlung verwendet werden (vgl. Art. 16a Abs. 3 GG). Der Gesetzgeber hat insgesamt Sorge zu tragen, dass der Schutz der Europäischen Menschenrechtskonvention und der anderen internationalen Menschenrechtsverträge (vgl. Art. 1 Abs. 2 GG) durch eine Übermittlung der von deutschen Behörden erhobenen Daten ins Ausland und an internationale Organisationen nicht ausgehöhlt wird.

(2) Die Gewährleistung des geforderten Schutzniveaus im Empfängerstaat muss nicht für jeden Fall einzeln geprüft und durch völkerrechtlich verbindliche Einzelzusagen abgesichert werden. Der Gesetzgeber kann diesbezüglich auch eine generalisierende tatsächliche Einschätzung der Sach- und Rechtslage der Empfängerstaaten durch das Bundeskriminalamt ausreichen lassen. Diese kann so lange Geltung beanspruchen, wie sie nicht durch entgegenstehende Tatsachen in besonders gelagerten Fällen erschüttert wird.

Lassen sich Entscheidungen mit Blick auf einen Empfängerstaat nicht auf solche Beurteilungen stützen, bedarf es aber einer mit Tatsachen unterlegten Einzelfallprüfung, aus der sich ergibt, dass die Beachtung jedenfalls der grundlegenden Anforderungen an den Umgang mit Daten hinreichend gewährleistet ist … Erforderlichenfalls können und müssen verbindliche Einzelgarantien abgegeben werden. Grundsätzlich ist eine verbindliche Zusicherung geeignet, etwaige Bedenken hinsichtlich der Zulässigkeit der Datenübermittlung auszuräumen, sofern nicht im Einzelfall zu erwarten ist, dass die Zusicherung nicht eingehalten wird … Welche Anforderungen im Einzelnen gelten, kann der Gesetzgeber auch von einer Einzelfallabwägung abhängig machen.

Die Vergewisserung über das geforderte Schutzniveau – sei es generalisiert, sei es im Einzelfall – ist eine nicht der freien politischen Disposition unterliegende Entscheidung deutscher Stellen. Sie hat sich auf gehaltvolle wie realitätsbezogene Informationen zu stützen und muss regelmäßig aktualisiert werden. Ihre Gründe müssen nachvollziehbar dokumentiert werden. Die Entscheidung muss durch die Datenschutzbeauftragten überprüfbar sein und einer gerichtlichen Kontrolle zugeführt werden können.[153]

Hinsichtlich dieser Voraussetzungen ist zu beachten, dass § 10 Abs.1 FlugDaG-E explizit auf die entsprechenden Vorgaben der §§ 78–80 BDSG-E verweist. § 78 Abs. 1 Nr. 2 BDSG-E betrifft dabei den Fall, dass eine Datenübermittlung in einen Drittstaat erfolgt, für den ein Angemessenheitsbeschluss der Kommission vorliegt. § 79 und § 80 BDSG-E regeln die Übermittlung von Daten an Drittstaaten, für die zwar kein Angemessenheitsbeschluss vorliegt, es aber im Einzelfall dennoch geeignete Garantien für den Schutz personenbezogener Daten (§ 79 BDSG-E) gibt oder keine solche Garantien vorliegen, die Übermittlung aber zu bestimmten Schutz- und Abwehrzwecken erforderlich ist (§ 80 BDSG-E). Die Angemessenheitsbeschlüsse der Kommission können über § 21 BDSG-E einer gerichtlichen Kontrolle zugeführt werden. In jedem dieser Fälle müssen die allgemeinen Voraussetzungen des § 78 BDSG-E gewahrt werden: Datenübermittlung nur an Stellen, die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständig sind (§ 78 Abs. 1 Nr. 1 BDSG-E); Weiterübermittlung von Daten aus anderen Mitgliedstaaten nur nach vorheriger Genehmigung (§78 Abs. 3 BDSG-E); geeignete Maßnahmen zur Sicherstellung, dass der Empfänger die übermittelten Daten nur dann an andere Drittstaaten oder andere internationale

153 BVerfG, NJW 2016, 1781, 1806 f., Rn. 332 ff.

Organisationen weiter übermittelt, wenn der Verantwortliche diese Übermittlung zuvor genehmigt hat (§ 78 Abs. 4 BDSG-E). § 78 Abs. 2 BDSG-E knüpft die Weitergabe von Daten im Einzelfall – sowohl bei Vorliegen als auch bei Nichtvorliegen eines Angemessenheitsbeschlusses – an die Gewährleistung eines datenschutzrechtlich angemessenen und die elementaren Menschenrechte wahrenden Umgangs mit den Daten beim Empfänger.

Hinsichtlich der erforderlichen Aufsichts-, Protokollierungs- und Dokumentationsanforderungen kann auf oben verwiesen werden (siehe soeben, V.14.a). Im Übrigen ist der Datenschutzbeauftragte der Fluggastdatenkontrollstelle über jede Datenübermittlung durch die Fluggastdatenkontrollstelle zu unterrichten, § 10 Abs. 3 FlugDaG-E. Hält dieser eine Datenverarbeitung für rechtswidrig, kann er die entsprechende Angelegenheit gemäß § 12 Abs. 2 FlugDaG-E an die nationale Kontrollstelle verweisen.

Schließlich müssen

> [d]ie vorstehend entwickelten Maßgaben … in einer den Grundsätzen der Bestimmtheit und Normenklarheit entsprechenden Weise gesetzlich ausgeformt sein. Dazu gehört auch, dass Ermächtigungsgrundlagen, die, soweit zulässig, eine Übermittlung von Daten zur Informationsgewinnung durch einen Abgleich mit Daten ausländischer Behörden und einen Rückfluss ergänzender Erkenntnisse herbeiführen sollen, als solche normenklar ausgestaltet sind.[154]

Insoweit genügen die expliziten Verweise auf §§ 78–80 BDSG-E in § 10 Abs. 1 FlugDaG-E.

c) Weitergabe innerhalb der EU und an Europol

Mit Blick auf die soeben skizzierten Anforderungen und die unionsweit einheitlichen Datenschutzstandards erscheinen die Regelungen zur Weitergabe an andere Mitgliedstaaten (§§ 7 f. FlugDaG-E) und Europol (§ 9 FlugDaG-E) unproblematisch.

15. Ausgestaltung der Datenübermittlung (Doppeltür-Modell)

Eine Datenweiterleitung bedarf nach dem Doppeltür-Modell des Bundesverfassungsgerichts nicht nur einer Übermittlungs-, sondern auch einer spezifischen Abfragebefugnis:

> § 20v Abs. 5 BKAG stellt verschiedene Rechtsgrundlagen zur Übermittlung von zur Terrorismusabwehr erhobenen Daten an andere Behörden bereit. Es handelt sich hierbei um Ermächtigungen, mit denen der Gesetzgeber im Einzelfall anlassbezogen eine Zweckänderung der Datennutzung erlaubt. Er öffnet damit die Datennutzung durch andere Behörden, die – nach dem Bild einer Doppeltür – dabei auch ihrerseits zur Abfrage und Verwendung dieser Daten berechtigt sein müssen.[155]

Das Bundesverfassungsgericht hat die Zusammenfassung in einer Norm für zulässig erachtet:

> Bei der Regelung eines Datenaustauschs zur staatlichen Aufgabenwahrnehmung ist darüber hinaus aber auch zwischen der Datenübermittlung seitens der auskunftserteilenden Stelle und dem Datenabruf seitens der auskunftsu-

---

154 BVerfG, NJW 2016, 1781, 1807, Rn. 341.

155 BVerfG, NJW 2016, 1781, 1803, Rn. 305.

chenden Stelle zu unterscheiden. Ein Datenaustausch vollzieht sich durch die einander korrespondierenden Eingriffe von Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen. Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten. Dies schließt – nach Maßgabe der Kompetenzordnung und den Anforderungen der Normenklarheit – nicht aus, dass beide Rechtsgrundlagen auch in einer Norm zusammengefasst werden können.[156]

Mangels Anhaltspunkten im Gesetzentwurf und in der Gesetzesbegründung ist davon auszugehen, dass § 4 Abs. 5 FlugDaG-E als einheitliche Übermittlungs- und Abfragebefugnis zu verstehen ist:

Die Fluggastdatenzentralstelle kann im Einzelfall auf ein begründetes Ersuchen einer in § 6 Absatz 1 Satz 1 genannten zuständigen Behörde die von der ersuchenden Behörde übermittelten Daten in besonderen Fällen mit den im Fluggastdaten-Informationssystem gespeicherten Daten zu den in § 1 Absatz 2 genannten Zwecken abgleichen. Satz 1 gilt mit Blick auf die in § 6 Absatz 2 Satz 1 genannten Behörden entsprechend mit der Maßgabe, dass der Abgleich zum Zweck der Erfüllung von deren Aufgaben im Zusammenhang mit Straftaten nach Absatz 1 erfolgen kann.[157]

Insoweit ist darauf hinzuweisen, dass aus kompetentiellen Gründen auf diese Norm kein Ersuchen der Landeskriminalämter im präventiven Bereich gestützt werden kann. Hier ist gesetzgeberisches Tätigwerden auf Landesebene erforderlich, da die bestehenden Grundlagen der Weitergabebegrenzung nicht hinreichend Rechnung tragen dürften.

München, den 21. April 2017

Gez. Prof. Dr. Ferdinand Wollenschläger

---

156 BVerfGE 130, 151, 184.

157 Anders zur Anti-Terror-Datei BVerfGE 133, 277, 320, Rn. 103.