.SIAK REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SICHERHEITSAKADEMIE

.SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Haller, Matthias

EU-Fluggastdatensystem und die Grundrechte. Die neue Richtlinie über die Nutzung von Fluggastdaten zur Kriminalitätsbekämpfung im Lichte der Grundrechtecharta

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (3/2016), 86-101.

doi: 10.7396/2016_3_H

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Haller, Matthias (2016). EU-Fluggastdatensystem und die Grundrechte. Die neue Richtlinie über die Nutzung von Fluggastdaten zur Kriminalitätsbekämpfung im Lichte der Grundrechtecharta, SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (3), 86-101, Online: http://dx.doi.org/10.7396/2016_3_H.

Online publiziert: 12/2016

EU-Fluggastdatensystem und die Grundrechte

Die neue Richtlinie über die Nutzung von Fluggastdaten zur Kriminalitätsbekämpfung im Lichte der Grundrechtecharta

MATTHIAS HALLER,
wissenschaftlicher Projektmitarbeiter am Institut für Europarecht und Völkerrecht der Universität Innsbruck.

Nachdem europäische Fluggesellschaften auf Grund von völkerrechtlichen Abkommen der Europäischen Union bereits heute persönliche Informationen über ihre Passagiere an Drittstaaten übermitteln, soll die so genannte Fluggastdatenspeicherung unter dem Eindruck der Terroranschläge auf Paris im Jahr 2015 künftig auch von den EU-Mitgliedstaaten für die Bekämpfung von Terrorismus und schwerer Kriminalität genutzt werden. So sollen die von den Fluggesellschaften erhobenen Daten auf Grund einer kürzlich erlassenen Richtlinie (RL) spätestens ab Mitte 2018 und mindestens in Bezug auf Flüge von und in Drittstaaten von den Behörden der Mitgliedstaaten genutzt werden. Vor diesem hochaktuellen Hintergrund bezweckt der vorliegende Aufsatz zunächst, dem Leser Informationen über Fluggastdaten und deren Speicherung sowie einen Überblick über nationale Systeme und die völkerrechtlichen Abkommen der EU zu vermitteln (1.), bevor die wesentlichen Inhalte der neuen RL dargestellt werden (2.). Da hinsichtlich der Vereinbarkeit einer solch umfassenden Datenspeicherung mit den Unionsgrundrechten Bedenken bestehen, werden diese aufgezeigt (3.), bevor der Aufsatz mit Überlegungen zur Grundrechtskonformität und Effektivität eines solchen Systems, zu Alternativen und mit einer Prognose zu einer etwaigen EuGH-Entscheidung zur RL schließt (4.).

1. GRUNDSÄTZLICHES[1]

2014 nach dem EuGH-Urteil zur Vorratsspeicherung von Telekommunikationsdaten[2] bereits abgeschrieben, erhielt der sicherheitspolitische Plan, unionsweit Fluggastdaten auf Vorrat zu speichern, nach den Pariser Terroranschlägen im Januar und November 2015 wieder Auftrieb und das zunächst vom Europäischen Parlament (EP) blockierte Verfahren wurde am 27.04.2016 mit dem Erlass der RL (EU) 2016/681 „über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität“[3] (im Folgenden: PNR-RL) erfolgreich abgeschlossen. Sie trat am 24.05.2016 in Kraft.

Vor der Analyse dieser aktuellen Debatte um ein EU-Fluggastdatensystem ist es jedoch sinnvoll, den Begriff zu erklären und sich kurz mit bereits bestehenden Systemen und Abkommen – auch (in) der EU – auseinanderzusetzen.

1.1 DEFINITION

Fluggastdaten, oft auch als PNR-Daten (aus dem Englischen: Passenger Name Record data) bezeichnet, sind von Fluggesellschaften für geschäftliche Zwecke erhobene Daten zu Passagieren.[4] Die erhobenen Daten variieren zwar, es handelt

sich aber stets um eine Kombination von Informationen wie Buchungs- und Flugdatum, Namen, Kontaktdaten, Adresse, Zahlungs- und Rechnungsinformationen, Kreditkartennummern, Reiseverlauf, Gepäck- und Sitzplatzinformationen oder allgemeine Hinweise (so genannte „general remarks").[5]

Von den PNR-Daten unterscheiden sich die API-Daten (aus dem Englischen: Advanced Passenger Information), die vor allem Passdaten, wie Name, Geburtsdatum, Nationalität, Geschlecht und Passnummer umfassen. In der EU ist die Übermittlung von API-Daten von Fluggesellschaften an Behörden in der RL 2004/82/EG[6] geregelt.

1.2 STAATLICHE PNR-SYSTEME

Die Nutzung von Fluggastdaten für staatliche Ziele ist im Gegensatz zu ihrer Speicherung für private Zwecke ein relativ rezentes Phänomen: Zwar nutzten sie die USA bereits Ende des 20. Jahrhunderts, systematisch erfolgte dies jedoch erst nach den Terroranschlägen vom 11.09.2001[7], als der Aviation and Transportation Security Act[8] Fluggesellschaften verpflichtete, den Behörden Zugriff zu Passagierdaten von allen Flügen in bzw aus den USA oder über US-Gebiet zu gewähren.[9]

Dem Beispiel der USA folgten etwa Kanada[10], Australien[11], Neuseeland, Südkorea oder Japan.[12] Auch in der EU gibt es mit jenem von Großbritannien bereits ein funktionsfähiges nationales PNR-System; zum Teil genutzt bzw in Ausarbeitungs- oder Testphase befindlich sind solche Systeme ferner in Frankreich, Dänemark, Schweden, Belgien, Spanien und den Niederlanden.[13]

1.3 PNR-ABKOMMEN DER EU

1.3.1 Vor Lissabon

Die europäischen Fluggesellschaften befanden sich auf Grund der 2001 eingeführten US-Gesetzgebung in einer Zwickmühle: Einerseits war die Weitergabe von Fluggastdaten an US-Behörden sehr bedenklich, da Art 25 DatenschutzRL[14] hierfür ein „angemessenes Schutzniveau" verlangt, andererseits drohten die USA für den Fall des Unterbleibens der Informationsweitergabe mit der Einstellung des transatlantischen Flugverkehrs.[15]

Dies hätte die Unternehmen vor große wirtschaftliche Schwierigkeiten gestellt, weshalb die Kommission und der Rat 2004 aktiv wurden: Nach Zusicherung der US-Behörden, ein angemessenes Datenschutzniveau zu gewähren, erklärte die Kommission gemäß Art 25 Abs 6 der nur im damaligen Gemeinschaftsrecht anwendbaren DatenschutzRL die Angemessenheit des Schutzniveaus[16], woraufhin der Rat – ebenso im Rahmen des Gemeinschaftsrechts – den Abschluss eines Abkommens über die Verarbeitung von Fluggastdaten und deren Übermittlung an die USA beschloss.[17]

Das EP legte jedoch Nichtigkeitsklage ein, der der EuGH stattgab: Zwar fielen PNR-Daten beim Ticketverkauf und somit im Rahmen einer Dienstleistung an. Mit ihrer Verarbeitung und Übermittlung an die USA sei jedoch nicht mehr das Gemeinschaftsrecht, sondern die Sicherheit und das Strafrecht und somit die damalige dritte Säule einschlägig, weshalb die Rechtsgrundlage wegfalle.[18] Eine Neuverhandlung des Abkommens wurde erforderlich.[19]

So schloss der Rat 2006[20] und 2007[21] weitere Abkommen mit den USA, wobei das Datenschutzniveau sogar niedriger als 2004 war.[22] PNR-Abkommen wurden – 2006 und damit ebenfalls noch im Rahmen des Gemeinschaftsrechts – auch mit Kanada[23] und 2008 mit Australien geschlossen.[24]

1.3.2 Nach Lissabon

Mit dem am 01.12.2009 in Kraft getretenen Vertrag von Lissabon wurde die

Säulenstruktur der EU aufgelöst; die Politikbereiche Justiz (Art 82 AEUV[25], ex-Art 31 EUV[26]) und Inneres (Art 87 AEUV, ex-Art 30 EUV) gelangten von der intergouvernementalen auf die supranationale Ebene – das Einstimmigkeitserfordernis im Rat wich der qualifizierten Mehrheitsentscheidung, das EP wurde gleichwertiger Mitgesetzgeber des Rats im explizit anwendbaren ordentlichen Gesetzgebungsverfahren (Art 289 Abs 1 und Art 294 AEUV).[27]

Die neue institutionelle Struktur betrifft auch Übereinkünfte, die die Union gemäß Art 216 AEUV mit Drittländern schließen kann: Das Verfahren des Art 218 AEUV sieht für ihren Abschluss zwar nach wie vor einen Ratsbeschluss vor (Abs 6), dem in Bereichen des ordentlichen Gesetzgebungsverfahrens aber die Zustimmung des EP vorausgeht (Abs 6 lit a [v]).

Das EP verlangte sogleich Neuverhandlungen der zeitlich beschränkten PNR-Abkommen, ua um sie an die EU-Datenschutznormen anzupassen.[28] So wurden neue Abkommen mit Australien[29] und den USA[30] geschlossen, die aber nur leichte datenschutzrechtliche Verbesserungen bringen und etwa immer noch eine bis zu 15-jährige Speicherfrist vorsehen.[31]

1.3.3 Neueste Entwicklungen

Die 2014 erfolgte Ungültigerklärung der VorratsdatenspeicherungsRL durch den EuGH[32] war für das EP der Auslöser, um das ebenfalls geplante neue Abkommen mit Kanada zu blockieren und stattdessen beim EuGH ein Gutachten über seine Vereinbarkeit mit den Verträgen, insbesondere mit den Grundrechten im Datenschutzbereich, anzufordern.[33]

Bis dato wurde das Gutachten, das großen Einfluss auf die zukünftige Ausgestaltung von PNR-Abkommen hätte, aber auch die Einschätzung des EuGH zum PNR-System der EU offenlegen könnte, nicht erstattet. Dass der EuGH eine datenschutzfreundliche Linie vertritt, zeigt aber neben dem Urteil zur VorratsdatenspeicherungsRL auch das „Safe Harbor"-Urteil (englisch für: sicherer Hafen): In diesem erklärte er die Kommissionsentscheidung 2000/520/EG[34], in der diese laut Art 25 Abs 6 DatenschutzRL feststellte, die USA gewährleiste „hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau",[35] für unionsrechtswidrig.[36] Der EuGH erachtete etwa die behördliche Datennutzung als weit über das hinausgehend, was für die öffentliche Sicherheit absolut notwendig und verhältnismäßig wäre[37] und verwies auf das Urteil zur Vorratsdatenspeicherung.[38]

Zwar ist das Urteil nicht ohne Weiteres auf den hier einschlägigen Raum der Freiheit, der Sicherheit und des Rechts übertragbar, wo die DatenschutzRL gemäß ihres Art 3 Abs 2 nicht anwendbar ist. Weil aber auch der hier noch bis 06.05.2018 anwendbare Datenschutz-Rahmenbeschluss[39] (in Art 13) und die neue DatenschutzRL für den Bereich Justiz und Inneres[40] (in Art 36) ein angemessenes Schutzniveau verlangen, ist das Urteil doch richtungsweisend für das EuGH-Gutachten und somit für die Zukunft des gesamten PNR-Bereichs. Und es zeigt, dass der EuGH einen effektiven Datenschutz einfordert, dessen Einhaltung er durchaus auch inhaltlich überprüft.

2. PNR-RICHTLINIE DER EU

In der EU gab es zumindest seit 2007, als die Kommission einen ersten Vorschlag für einen Rahmenbeschluss des Rats vorlegte[41], Bestrebungen zur Errichtung eines PNR-Systems. Ein RL-Vorschlag der Kommission folgte 2011[42], zu dem der Rat 2012 seine allgemeine Ausrichtung vorlegte[43]. Der Vorschlag wurde jedoch vom LIBE-Ausschuss[44] des EP 2013 abgelehnt[45], was den Gesetzgebungsprozess

vorerst zum Erliegen brachte. Die ablehnende Position des EP kippte aber 2015 nach der ersten Pariser Terrorserie: Eine klare Mehrheit erklärte sich nunmehr dazu bereit, auf den Erlass einer RL hinzuwirken.[46] In Verhandlungsrunden zwischen Rat, Parlament und Kommission im Rahmen eines informellen Trilogs[47] konnten sich die beiden Gesetzgeber im Dezember 2015 schließlich auf die PNR-RL einigen.[48]

2.1 RECHTSGRUNDLAGE UND GEGENSTAND

Als Rechtsgrundlage für ihren Erlass stützt sich die RL laut ihrer Präambel auf Art 82 Abs 1 lit d AEUV (Maßnahmen zur Erleichterung der Kooperation der Justizbehörden der EU-Staaten in der Strafverfolgung) und Art 87 Abs 2 lit a AEUV (Maßnahmen, die das Einholen, Speichern, Verarbeiten, Analysieren und Austauschen von Informationen zum Zweck der polizeilichen Zusammenarbeit der Behörden der Mitgliedstaaten betreffen).

Regelungsgegenstand der PNR-RL ist laut ihrem Art 1 Abs 1 „die Übermittlung von Fluggastdatensätzen (PNR-Daten) zu Fluggästen von Drittstaatsflügen durch Fluggesellschaften“ (lit a) und „die Verarbeitung von Daten gemäß Buchstabe a, unter anderem ihre Erhebung, Verwendung und Speicherung durch Mitgliedstaaten sowie den Austausch dieser Daten zwischen Mitgliedstaaten“ (lit b).

Eine verpflichtende Nutzung von PNR-Daten ist also nur für so genannte internationale Flüge vorgesehen. Den Mitgliedstaaten steht es nach Art 2 PNR-RL aber frei, die Anwendung der RL nach Mitteilung an die Kommission auf ausgewählte oder sämtliche EU-Flüge auszuweiten. In einer Erklärung des Rates gaben alle Mitgliedstaaten an, von dieser eigentlich fakultativen Möglichkeit Gebrauch zu machen.[49] Überdies soll die Kommission bis 25.05.2020 die Erforderlichkeit der obligatorischen Einbeziehung von EU-Flügen prüfen (Art 19 PNR-RL).

2.2 ANWENDUNGSBEREICH

Die einzelnen zu erhebenden PNR-Daten sind taxativ in Anhang I der PNR-RL aufgelistet. Ihre Nutzung ist gemäß Art 1 Abs 2 PNR-RL auf die Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung terroristischer Straftaten und schwerer Kriminalität beschränkt. Als terroristische Straftaten gelten laut Art 3 Nr 8 PNR-RL nach nationalem Recht strafbare Handlungen iSd Art 1 bis 4 Rahmenbeschluss zur Terrorismusbekämpfung[50], während gemäß Art 3 Nr 9 PNR-RL jene in Anhang II der RL angeführten strafbaren Handlungen unter den Begriff der schweren Kriminalität fallen, die nach nationalem Recht mit Freiheitsstrafe von mindestens drei Jahren im Höchstmaß bedroht sind.

2.3 DATENERFASSUNG UND -SPEICHERUNG

Laut Art 4 PNR-RL errichtet jeder Mitgliedstaat – bzw zwei oder mehr Staaten gemeinsam – eine PNR-Zentralstelle (englisch: PIU, Passenger Information Unit) oder benennt eine Abteilung einer bereits bestehenden Fachbehörde als solche. Diese erheben, speichern und verarbeiten die PNR-Daten der Fluggesellschaften, leiten diese oder die Ergebnisse der Datenverarbeitung an die zuständigen Behörden weiter (Art 4 Abs 2 lit a PNR-RL) und tauschen sie mit Zentralstellen anderer Mitgliedstaaten und mit Europol aus (lit b).

Fluggesellschaften werden in Art 8 PNR-RL verpflichtet, von ihnen erfasste PNR-Daten auf elektronischem Weg an die PNR-Zentralstelle, in deren Hoheitsgebiet der Flug landet bzw startet, weiterzuleiten. Dies muss 24 bis 48 Stunden vor Abflug und gleich nach Abfertigungsschluss nach der so genannten „Push-Methode“ erfolgen, die im Vergleich zur „Pull-Methode“,

die Behörden direkten Datenzugriff gewährt, mehr Datenschutz bietet.[51] Für Verstöße sieht Art 14 PNR-RL den Erlass von abschreckenden und wirksamen (Geld-) Sanktionen vor.

Die erhaltenen Daten werden von der Zentralstelle erfasst; beinhalten sie andere als die in Anhang I der PNR-RL angeführten Daten, werden diese unmittelbar nach ihrem Eingang gelöscht (Art 6 Abs 1 PNR-RL).

Laut Art 12 PNR-RL werden die Daten für einen Zeitraum von fünf Jahren in Datenbanken vorgehalten, wobei Datenelemente, die eine Identitätsfeststellung erlauben, nach sechs Monaten unkenntlich gemacht werden. 2011 sollte die „unmaskierte" Speicherung noch auf 30 Tage beschränkt werden.[52]

Auch nach ihrer Pseudonymisierung können die Daten aber für die Erstellung der so genannten Prüfkriterien genutzt werden (siehe dazu im folgenden Abschnitt). Nach Genehmigung durch Justizbehörden können maskierte Daten auch wieder offengelegt werden, wenn berechtigter Grund zur Annahme besteht, dass dies für die individuelle Beantwortung von gebührend begründeten Behördenanfragen auf Bereitstellung und Verarbeitung von PNR-Daten in spezifischen Fällen und zum Zweck der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Terrorismus oder schwerer Kriminalität sowie für die Bereitstellung der Ergebnisse der Verarbeitung an ebendiese Behörden oder an Europol erforderlich ist.[53]

Nach Ablauf der Fünfjahresfrist werden die Daten endgültig gelöscht.

2.4 NUTZUNGSARTEN DER PNR-DATEN

Die Kommission sprach konzeptuell von drei Nutzungsarten: proaktiv (Datenanalyse und Erstellung von Prüfkriterien für die Echtzeitüberprüfung), in Echtzeit (Überprüfung von Fluggästen zur Verhinderung von Straftaten, Beobachtung oder Festnahme von Personen vor Begehung einer Straftat oder bei bzw unmittelbar nach Begehung einer Straftat durch Abgleich mit den Prüfkriterien und Datenbanken) und reaktiv (Ermittlungen nach Begehung einer Straftat).[54]

Auch Art 6 Abs 2 PNR-RL fixiert drei Zwecke, für die PNR-Zentralstellen die Daten verarbeiten dürfen. Zunächst dürfen Fluggäste vor Ankunft bzw Abflug überprüft werden, um jene Personen zu ermitteln, die an einer terroristischen Straftat oder an einem Akt schwerer Kriminalität beteiligt sein könnten und daher von den nationalen Behörden oder von Europol genauer überprüft werden müssen (lit a). Hierbei dürfen die Daten laut Art 6 Abs 3, 5 und 6 PNR-RL mit den maßgeblichen Datenbanken (etwa dem Schengener Informationssystem [SIS][55]) und „anhand im Voraus festgelegter Kriterien" (der so genannten Prüfkriterien) automatisiert abgeglichen werden, wobei Treffer nichtautomatisiert überprüft werden müssen, um zu klären, ob eine Übermittlung an die Strafverfolgungsbehörden notwendig ist.

Ein weiterer Verarbeitungszweck der Daten ist die individuelle Beantwortung begründeter Behördenanfragen auf Bereitstellung und Verarbeitung der Daten in spezifischen Fällen in den Bereichen Terrorismus und schwerer Kriminalität sowie die Bereitstellung der Ergebnisse dieser Verarbeitung an ebendiese Behörden oder an Europol (lit b).

Die dritte Nutzungsart von PNR-Daten durch die Zentralstellen (lit c) ist ihre Analyse zur Erstellung bzw Anpassung der Prüfkriterien. Diese dienen dazu, Personen zu ermitteln, die an terroristischen Straftaten oder Akten schwerer Kriminalität beteiligt sein könnten.

Dabei müssen Überprüfungen anhand der Prüfkriterien in nichtdiskriminierender

Weise erfolgen und dürfen keinesfalls sensible Daten wie die Rasse, Ethnie oder Religion als Prüfkriterien herangezogen werden (Art 6 Abs 4 PNR-RL).

2.5 WEITERLEITUNG VON PNR-DATEN

Innerstaatlich werden die Daten bzw die Ergebnisse der Datenverarbeitung von gemäß Art 6 Abs 2 lit a PNR-RL ermittelten Personen auf Einzelfallbasis von der Zentralstelle an die zuständigen Behörden übermittelt (Art 6 Abs 6 PNR-RL), die sie nur für Terrorismus und schwere Kriminalität verwenden dürfen (Art 7 Abs 4 PNR-RL).

Zuständig sind laut Art 7 Abs 2 PNR-RL jene Behörden, die in den Bereichen Terrorismus oder schwerer Kriminalität tätig sind.

Der Informationsaustausch zwischen Mitgliedstaaten ist in Art 9 PNR-RL geregelt und unterscheidet sich vom innerstaatlichen: PNR-Daten werden in diesem Fall zunächst von der agierenden Zentralstelle an jene des Empfängerstaats und erst von dieser an die zuständigen Behörden weitergeleitet (Abs 1). Ebenso können Zentralstellen Daten aus der PNR-Datenbank anderer Mitgliedstaaten anfordern (Abs 2). Die eigene Zentralstelle ist im Regelfall auch bei Anfragen der Art 7-Behörden zwischengeschaltet – nur wenn es „in Notfällen erforderlich ist", können sie Daten direkt bei fremden Zentralstellen anfordern (Abs 3). Ist ausnahmsweise ein frühzeitiger Datenzugriff nötig, um eine spezifische, gegenwärtige Bedrohung abzuwehren, sind Zentralstellen berechtigt, von anderen Zentralstellen zu verlangen, dass sie die Datenübermittlung durch Fluggesellschaften zu anderen Zeitpunkten als 24 bis 48 Stunden vor Abflug und sofort nach Abfertigungsschluss anfordern und ihnen die Daten bereitstellen (Abs 4).

Neben den Strafverfolgungsbehörden und den PNR-Zentralstellen ist im Rahmen seiner Kompetenzen auch Europol befugt, PNR-Daten oder die Datenverarbeitungsergebnisse von den Zentralstellen zur Ausübung seiner Aufgaben anzufordern (Art 10 PNR-RL).

Art 11 PNR-RL regelt schließlich die Weitergabe von PNR-Daten an Drittstaaten: Diese darf nur im konkreten Einzelfall und nur dann erfolgen, wenn die Bedingungen des Art 13 Datenschutz-Rahmenbeschluss erfüllt sind (also ua ein angemessenes Schutzniveau für die Datenverarbeitung gewährleistet ist), die Übermittlung für Terrorismus oder schwere Kriminalität erfolgt und sich der Drittstaat bereit erklärt, die Daten nur zu diesen Zwecken, nur bei unbedingter Notwendigkeit und nur mit expliziter Zustimmung des betreffenden Mitgliedstaats an einen anderen Drittstaat weiterzugeben.

2.6 DATENSCHUTZ

Auch hinsichtlich der Datenverarbeitung durch die Mitgliedstaaten legt der Datenschutz-Rahmenbeschluss die Mindestanforderungen fest: Gemäß Art 13 Abs 1 PNR-RL müssen Fluggästen jene Rechte „auf Schutz personenbezogener Daten, Zugang, Berichtigung, Löschung und Einschränkung der Verarbeitung sowie Schadenersatz und Rechtsbehelfe" gewährt werden, die nach Unionsrecht, nationalem Recht und zur Umsetzung der Art 17 bis 20 Datenschutz-Rahmenbeschluss festgelegt sind; ebenso gelten die in Umsetzung der Art 21 und 22 Datenschutz-Rahmenbeschluss erlassenen nationalen Vorschriften zur Vertraulichkeit und Sicherheit der Datenverarbeitung (Art 13 Abs 2 PNR-RL).

Art 13 Abs 4 PNR-RL verbietet darüber hinaus jede Verarbeitung von sensiblen Daten. Langen solche Daten bei der Zentralstelle ein, müssen sie sofort gelöscht werden.

Jede PNR-Zentralstelle ernennt laut Art 5 PNR-RL einen Datenschutzbeauftragten,

Art 15 PNR-RL weitet die Zuständigkeit der bereits nach Art 25 Datenschutz-Rahmenbeschluss errichteten nationalen Kontrollstellen auf das PNR-System aus.

3. PNR-SYSTEM UND DIE EU-GRUNDRECHTECHARTA

Dass Fluggastdatensysteme mit ihrer systematischen Erfassung und Speicherung von persönlichen Daten sehr invasiv sind, liegt auf der Hand und macht eine Prüfung ihrer Grundrechtskonformität unverzichtbar. Die Unionsgrundrechte bestehen laut Art 6 EUV aus der Charta der Grundrechte der EU[56] (GrC) und aus so genannten allgemeinen Grundsätzen, die sich wiederum aus der EMRK und aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben.[57]

3.1 BETROFFENE GRUNDRECHTE

Durch das PNR-System der EU eindeutig betroffen sind die Grundrechte im Bereich des Datenschutzes, sollen doch persönliche Daten aller Fluggäste an Behörden übermittelt, von diesen verarbeitet und über einen langen Zeitraum gespeichert werden.[58] Einschlägig ist dabei einerseits der Schutz der personenbezogenen Daten in Art 8 GrC, Art 8 EMRK in der Auslegung des Europäischen Gerichshofes für Menschenrechte (EGMR) und Art 16 AEUV, andererseits die Achtung des Privat- und Familienlebens in Art 7 GrC und Art 8 EMRK.[59]

Hinzu kommt die Gefahr von Verstößen gegen das in Art 21 GrC und Art 14 EMRK sowie im AEUV verankerte Diskriminierungsverbot, etwa durch den nicht eindeutig begrenzten Datensatz der „allgemeinen Hinweise“ (Nr 12 in Anhang I der PNR-RL) oder auf Grund des automatisierten Fluggast-Screenings anhand von Prüfkriterien,[60] bei der die Gefahr einer so genannten „discrimination by computer“ besteht.[61]

Gerechtfertigt werden kann ein PNR-System dagegen mit dem in Art 6 GrC und Art 5 EMRK verankerten Recht auf Sicherheit, was umso mehr gilt, als die Gewährleistung der öffentlichen Sicherheit nicht nur ein Bürgerrecht und eine Pflicht des Rechtsstaats ist, sondern gewissermaßen eine Grundvoraussetzung für den Genuss anderer Grundrechte und -freiheiten darstellt. Eine Güterabwägung ist daher nötig.[62]

3.2 RECHTFERTIGUNG DES EINGRIFFS: ART 52 GrC

Grundrechtseingriffe sind nicht per se verboten, sondern können unter bestimmten Voraussetzungen gerechtfertigt werden. So normiert etwa Art 8 Abs 2 GrC, dass personenbezogene Daten „nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden“ dürfen.

Neben dieser speziellen Schrankenregelung im Datenschutzrecht schafft die allgemeine Regelung des Art 52 Abs 1 GrC einen gemeinsamen Überbau für alle Grundrechte.[63] Demnach müssen Einschränkungen von in der GrC garantierten Rechten und Freiheiten zunächst einem von der Union anerkannten, dem Gemeinwohl dienenden Ziel oder dem Erfordernis des Schutzes der Rechte und Freiheiten anderer entsprechen. Ebenso muss der Eingriff gesetzlich vorgesehen sein, den Wesensgehalt der Rechte achten und – unter Wahrung des Verhältnismäßigkeitsgrundsatzes – notwendig sein.

Diese mehrstufige Prüfung muss auch die PNR-RL bestehen, wobei neben der Judikatur des EuGH auch die umfangreichere Rechtsprechung des EGMR zu berücksichtigen ist: Art 52 Abs 3 GrC normiert nämlich, dass die in der GrC enthaltenen und jenen der EMRK entspre-

chenden Rechte die gleiche Bedeutung und Tragweite wie in dieser haben.

3.2.1 Anerkanntes Ziel

Zunächst müssen Einschränkungen der Grundrechte „den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen“ (Art 52 Abs 1 GrC), der EGMR spricht von legitimen Zwecken eines demokratischen Staates.

Art 8 Abs 2 EMRK sieht ua die nationale Sicherheit und Ordnung sowie die Verhinderung von Straftaten als legitime Zwecke für Eingriffe in das in Abs 1 garantierte Recht auf Achtung des Privatlebens vor. Die mit dem PNR-System bezweckten Ziele der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Terrorismus und schwerer Kriminalität stellen eindeutig einen legitimen Zweck bzw ein anerkanntes Ziel dar, mit dem laut EGMR auch Überwachungsmaßnahmen[64] oder die verdeckte Informationsgewinnung[65] gerechtfertigt werden können.[66]

So ist die öffentliche Sicherheit – und mit ihr auch die Bekämpfung von Terrorismus und schwerer Kriminalität – nicht nur selbst ein Grundrecht nach Art 5 EMRK, sondern auch eine Schranke des in Art 8 EMRK verankerten Rechts auf Achtung des Privatlebens; und neben Grundrecht und Grundrechtsschranke ist die Sicherheit, wie erwähnt, auch eine Grundvoraussetzung für die Ausübung anderer Grundrechte und -freiheiten.

Der Grundrechtseingriff kann daher auf dieser ersten Prüfungsebene sowohl mit den von der EU anerkannten Zielen als auch mit dem Schutz der Freiheiten anderer gerechtfertigt werden – mit der öffentlichen Sicherheit dient die RL einem eindeutig legitimen Zweck.[67]

3.2.2 Gesetzesvorbehalt

Ebenso müssen Eingriffe „gesetzlich vorgesehen sein“. Formell ist dieses Erfordernis hier gewahrt, erfolgt der Eingriff doch durch eine RL, die in verbindliches nationales Recht umgesetzt werden muss.[68] Das Erfordernis geht in der EGMR-Rechtsprechung aber weiter und erstreckt sich auf den Inhalt des Gesetzes: Dessen Qualität, Zugänglichkeit und Vorhersehbarkeit werden geprüft. Zugänglichkeit bedeutet, dass klar ist, welche Vorschriften wann zur Anwendung gelangen, Vorsehbarkeit, dass die Formulierung eine Ausrichtung des Verhaltens nach der Vorschrift ermöglicht, was Klarheit und Bestimmtheit erfordert.[69]

Dieses Zugänglichkeits- und Vorhersehbarkeitserfordernis schützt Bürger vor Willkür, was gerade bei Überwachungsmaßnahmen wichtig ist, wo laut EGMR eine erhöhte Gefahr willkürlicher Nutzung besteht – Zugänglichkeit und Vorhersehbarkeit müssten hier noch strenger geprüft werden.[70] Nun könnte das Screening anhand von Prüfkriterien als Überwachungsmaßnahme gesehen werden – und gerade in diesem Bereich ist die Zugänglichkeit und Vorhersehbarkeit eingeschränkt, da Fluggäste wohl kaum (genaue) Informationen zu den Prüfkriterien erhalten und die Vorhersehbarkeit bei automatisierten Screening-Vorgängen nicht wirklich gegeben ist. Kritisch ist ferner der unbestimmte Datensatz der „allgemeinen Hinweise“ (Nr 12 in Anhang I der PNR-RL).[71]

Davon abgesehen ist die RL in Bezug auf Qualität, Zugänglichkeit und Vorhersehbarkeit wesentlich ausgereifter als die Kommissionsvorschläge von 2007 und 2011, da sie ein durchaus rigides Verfahren, aber auch die Figur eines Datenschutzbeauftragten in den PNR-Zentralstellen vorsieht, womit angemessene und effektive Schutzmechanismen gegen Missbrauch bestehen.[72]

3.2.3 Notwendigkeit

Das PNR-System der EU muss aber zwei weitere Prüfungsschritte durchlaufen: Zunächst dürfen Einschränkungen gemäß Art 52 Abs 1 GrC „nur vorgenommen werden, wenn sie notwendig sind". Der EGMR spricht von Erforderlichkeit und versteht darunter, dass der Eingriff auf einem allgemeinen Belang von überragender Bedeutung beruhen und für die Erreichung des Ziels erforderlich sein muss, was zwar nicht unerlässlich, aber doch mehr als nur sinnvoll oder vernünftig bedeute.[73]

Dass das PNR-System gerade mit dem hochaktuellen Thema des Terrorismus allgemeine Belange von zentraler Bedeutung betrifft, ist unstrittig.[74] Viel wichtiger ist die Frage, ob der Eingriff für die Erreichung des Ziels erforderlich ist: Dies muss stichhaltig anhand einer Folgenabschätzung begründet werden, um die Erforderlichkeit und Wirksamkeit der Maßnahmen für die öffentliche Sicherheit zu beweisen.[75] Nun legte die Kommission 2011 zwar eine Folgenabschätzung vor[76], ohne jedoch die Relevanz und Notwendigkeit der Nutzung von PNR-Daten nachzuweisen, was wohl auch daran liegt, dass es schlichtweg kaum Statistiken dazu gibt.[77]

Ebensowenig prüfte die Kommission, ob die schon bestehenden Formen polizeilicher und justizieller Zusammenarbeit – etwa die API-RL oder das SIS[78] in Verbindung mit einer verstärkten Kooperation – bereits für die Erreichung des Ziels ausreichen würden, ob das PNR-System also überhaupt als weiteres Instrument im Kampf gegen Terrorismus und schwere Kriminalität erforderlich ist.[79]

3.2.4 Verhältnismäßigkeit

Eingriffe in Grundrechte müssen aber nicht nur notwendig sein, sondern dabei auch den Grundsatz der Verhältnismäßigkeit wahren „und den Wesensgehalt dieser Rechte und Freiheiten achten". Laut EGMR muss ein angemessenes Verhältnis zwischen Grund und Ausmaß des Eingriffs bestehen.[80]

Neben dem bereits erwähnten und auch in Bezug auf die Verhältnismäßigkeit relevanten Problem, dass selbst die Eignung und Effektivität des PNR-Systems für die Bekämpfung von Terrorismus und schwerer Kriminalität keineswegs erwiesen ist, bestehen auf Ebene der Verhältnismäßigkeit weitere kritische Aspekte. Grundsätzlich stellt sich die Frage, ob eine nicht gezielte, sondern systematische, alle Fluggäste und viele Daten betreffende Vorratsspeicherung überhaupt verhältnismäßig sein kann.[81]

In diesem Zusammenhang steht das Problem des Umgangs mit falsch-positiven Treffern (so genannte „false positives"). Zumal das PNR-System auch dazu dient, bisher unbekannte Verdächtige aufzuspüren[82], werden unweigerlich Personen falsch verdächtigt. Übersteigt die Zahl dieser zu Unrecht Verdächtigten jene der zu Recht Verdächtigten um ein Vielfaches, stellt dies ebenfalls die Verhältnismäßigkeit des Systems in Frage.[83]

Zu guter Letzt spielt auch die Speicherfrist eine große Rolle, denn eine unverhältnismäßig lange Datenspeicherung kann einen unzulässigen Eingriff darstellen[84], wie auch das EuGH-Urteil zur VorratsdatenspeicherungsRL zeigt.

3.3 EuGH-URTEIL ZUR VORRATSDATENSPEICHERUNG

Zuletzt gilt es, den Blick auf die Grundrechtsjudikatur des EuGH im einschlägigen Bereich zu richten. Neben dem „Safe Harbor"-Urteil fällte dieser mit dem 2014 ergangenen Urteil[85] zur RL 2006/24/EG über die Vorratsspeicherung von Telekommunikationsdaten[86] ein weiteres elementares Urteil in einem dem PNR-System sehr ähnlichen Bereich, was wichtige Rückschlüsse zu dessen Grundrechtskonformität ermöglicht.

Für den EuGH betrifft die in der RL 2006/24/EG vorgesehene Datenspeicherung mit dem Zweck, diese bei Bedarf den Behörden zugänglich zu machen, unmittelbar und speziell das Privatleben (Art 7 GrC), und zwar unabhängig davon, ob die Daten sensibel sind.[87] Ebenso greife die RL in Art 8 GrC ein, da sie personenbezogene Daten verarbeite.[88]

Der EuGH stellt grundsätzlich fest, dass der Eingriff von großem Ausmaß und besonders schwerwiegend sei. Ferner sei der Umstand, dass Benutzer nichts über die Speicherung und Nutzung der Daten wüssten, geeignet, bei Betroffenen „das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist."[89]

In der Folge prüft der EuGH die Rechtfertigung des Eingriffs. Nach der Feststellung, dass der Wesensgehalt der berührten Grundrechte nicht verletzt werde[90] und die Bekämpfung schwerer Kriminalität eine dem Gemeinwohl dienende Zielsetzung sei[91], folgt die Prüfung der Verhältnismäßigkeit – diese sei gegeben, wenn „die Handlungen der Unionsorgane geeignet sind, die mit der fraglichen Regelung verfolgten Ziele zu erreichen und nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist".[92] Er prüft sie somit zugleich mit der Notwendigkeit.

Die Eignung der Vorratsdatenspeicherung zur Erreichung des Ziels stellt der EuGH nicht in Frage[93], ihre Erforderlichkeit ergebe sich dadurch aber nicht automatisch: Die Achtung des Privatlebens verlange nämlich eine Beschränkung der Nutzung personenbezogener Daten „auf das absolut Notwendige".[94] Hierzu betont der EuGH die verbreitete Nutzung elektronischer Kommunikationsmittel und kritisiert, dass die Speicherung – ohne jedwede Differenzierung – alle elektronischen Kommunikationsmittel, alle Daten und alle Personen betrifft, unabhängig davon, ob diese in Zusammenhang mit einer Straftat stehen könnten oder nicht.[95] Ferner beschränke sich die Speicherung nicht auf einzelne geografische Gebiete oder auf Personenkreise, die in Straftaten verwickelt sein könnten.[96]

Aus verfahrensrechtlicher Sicht wird ua kritisiert, dass der Zugang zu den Daten nicht einer vorherigen Kontrolle eines Gerichts oder einer unabhängigen Verwaltungsbehörde unterliegen soll.[97] Hinsichtlich der Speicherfrist wird einerseits gerügt, dass deren Dauer mindestens sechs Monate beträgt, ohne dass zwischen den verschiedenen Datengruppen oder den betroffenen Personen unterschieden wird, andererseits, dass die Speicherfrist bis zu 24 Monate beträgt, ohne dass objektive Kriterien festgelegt werden müssten, die die Beschränkung der Speicherdauer auf das absolut Notwendige gewähren.[98]

So gelangt der EuGH schließlich zur Ansicht, dass ein Eingriff von großem Ausmaß und von besonderer Schwere vorliege, der nicht auf das absolut Notwendige beschränkt sei[99], weshalb er die RL für ungültig erklärt.[100]

4. SCHLUSSBETRACHTUNGEN

Vergleicht man nun die definitiv grundrechtsinvasive PNR-RL mit den Voraussetzungen, um derartige Eingriffe zu rechtfertigen, und mit dem Urteil zur Vorratsdatenspeicherung, lassen sich einige Rückschlüsse zur Frage der Grundrechtskonformität der RL ziehen.

Zunächst muss anerkannt werden, dass die PNR-RL hinsichtlich des Datenschutzes und der Verfahrensbestimmungen zur Vermeidung von Willkür und Diskriminierung gegenüber der VorratsdatenspeicherungsRL, aber auch im Vergleich zu den Entwürfen von 2007 und 2011, Fortschritte gemacht hat. So monierte der EuGH bei der Vorratsdatenspeicherung noch, dass keine materiell- und verfahrensrechtlichen

Bestimmungen den Zugang der Behörden zu den Daten und deren spätere Nutzung regelten[101], was hier sehr wohl der Fall ist.[102]

Ebenfalls müssen die Unterschiede zwischen der Invasivität der Vorratsdatenspeicherung und jener des PNR-Systems berücksichtigt werden: Telekommunikationsdaten und die zugehörigen Standortdaten ermöglichen einen sehr tiefen Einblick in das Leben einer Person, was – in Verbindung mit der Tatsache, dass Telekommunikation von fast der gesamten Bevölkerung regelmäßig genutzt wird – einen sehr schweren Eingriff in das Privatleben bedeutet.[103] Im Gegensatz dazu geht der Einblick durch PNR-Daten weniger weit und ist dieser auch nicht so regelmäßig. Auch die vom EuGH erwähnte Eignung der Vorratsdatenspeicherung, das Gefühl ständiger Überwachung zu erzeugen, trifft auf das PNR-System nicht oder nur in Bezug auf eine isolierte Tätigkeit bzw Personengruppe – das Fliegen bzw die Fluggäste – zu.[104]

Demgegenüber steht hinter der Grundrechtskonformität der Speicherdauer von insgesamt fünf Jahren ein großes Fragezeichen, was umso mehr gilt, als die offene Speicherung von 30 Tagen auf sechs Monate verlängert wurde. Ebendiese mindestens sechsmonatige Frist hatte der EuGH bereits bei der Vorratsdatenspeicherung kritisiert – und ob die ebenfalls eingeforderte Beschränkung der Speicherdauer auf das absolut Notwendige eingehalten wurde, ist auch mehr als fraglich, zumal die Kommission keinen Nachweis für die Notwendigkeit einer so langen Speicherfrist vorbrachte.[105]

Angreifbar wird das PNR-System auch dadurch, dass die Datenspeicherung vollkommen verdachtsunabhängig erfolgen soll, was nicht dafür spricht, dass die Speicherung sich auf das absolut Notwendige beschränkt.[106] Überdies soll die Datenübermittlung von den Unternehmen an die PNR-Zentralstellen im Gegensatz zu den Vorratsdaten nicht nur im konkreten Bedarfsfall, sondern andauernd und automatisch erfolgen.

Letztlich würde auch eine mangelnde Eignung des PNR-Systems, die Bekämpfung von Terrorismus und schwerer Kriminalität wirksam zu stützen, die Grundrechtskonformität der RL ausschließen. Diese Eignung, die der EuGH der Vorratsdatenspeicherung zugestand, da diese – auch auf Grund der ständigen Nutzung von Telekommunikation – wesentlich zur Aufklärung von Straftaten beitragen kann[107], ist hinsichtlich des PNR-Systems, dessen Effektivität oft bezweifelt wird, weniger eindeutig. Es muss berücksichtigt werden, dass mit der schweren Kriminalität, va aber mit dem Terrorismus Phänomene bekämpft werden, die selten bis äußerst selten vorkommen. Dies führt zwangsläufig zu vielen „false positives“[108], aber auch zum umgekehrten Problem: Werden einzelne Täter unter unzähligen Fluggästen gesucht, sind auch falsch-negative Treffer, also nicht erkannte Straftäter, die logische Folge.[109] Zusammen könnten diese Fehltreffer nicht nur die Effektivität und damit die Verhältnismäßigkeit des PNR-Systems, sondern sogar dessen grundsätzlichen Nutzen für die Erreichung der Sicherheitsziele in Frage stellen – eine Meinung, die nicht selten vertreten wird.[110]

Alternativ könnte etwa die Nutzung der bereits bestehenden Datenbanken in Verbindung mit einer besseren Kooperation der Behörden angedacht werden: Laut dem Europäischen Datenschutzbeauftragten Giovanni Buttarelli würden Verdächtige bereits jetzt überwacht und Informationen zu diesen in verschiedenen Datenbanken gespeichert. Die wahren Probleme seien einerseits fehlende Mittel für eine gezielte Überwachung, andererseits der viel zu geringe Datenaustausch zwischen Polizei-

behörden der EU – trotz bestehender Möglichkeiten im Rahmen von Europol und Eurojust.[111]

Aller Kritik zum Trotz wurde die PNR-RL am 27.04.2016 erlassen. Dass sie nun vor den EuGH gelangt, ist wahrscheinlich. Kommt es dazu, ist es zumindest auf den ersten Blick ebenso wahrscheinlich, dass sie das Schicksal der VorratsdatenspeicherungsRL erleidet und als unionsrechtswidrig eingestuft wird. Jedoch könnte neben den Verbesserungen im Datenschutzbereich auch die derzeitige Sicherheitslage Einfluss auf die Beurteilung der Grundrechtskonformität des PNR-Systems haben: So ist es zumindest denkbar, dass der EuGH ua die Terroranschläge auf Paris zum Anlass nimmt, um seine bisherige Judikatur im Datenschutzbereich zu überdenken. Es ist nämlich unbestritten, dass die Sicherheit eine Grundvoraussetzung für die Ausübung weiterer Rechte und Freiheiten darstellt. Sieht der EuGH die öffentliche Sicherheit ohne solch invasive Speichersysteme als nicht mehr gewährleistet an, ist eine Neuabwägung zwischen den Rechten auf Achtung des Privatlebens und Datenschutz auf der einen und dem Recht auf Sicherheit auf der anderen Seite nicht auszuschließen.[112]

[1] *Dieser Aufsatz ist eine gekürzte und aktualisierte Fassung einer Arbeit, die der Autor an der Universität Innsbruck im Rahmen der Lehrveranstaltung „Law Clinic: Innere Sicherheit und Migrationspolitik der EU" verfasst hat. Das Seminar wurde im Wintersemester 2015/2016 unter Werner Schroeder, auf Anregung und in Zusammenarbeit mit dem BMI unter Antonio-Maria Martino angeboten. Die (Zwischen)Ergebnisse der Arbeiten wurden im Dezember 2015 im Innenministerium in Wien den Praktikern des Hauses vorgestellt und mit diesen diskutiert.*

[2] *EuGH, verbRs C-293/12 und C-594/12, Digital Rights Ireland ua, ECLI:EU:C:2014:238.*

[3] *ABl L 119 vom 04.05.2016, 132 ff.*

[4] *House of Lords European Union Committee (2008) 7.*

[5] *U.S. Department of Homeland Security/ U.S. Customs and Border Protection (2013) 3.*

[6] *ABl L 261 vom 06.08.2004, 24 ff.*

[7] *Korff/Georges (2015) 12 f.*

[8] *Public Law 107-71, November 19, 2001, https://www.gpo.gov/fdsys/pkg/PLAW-107publ71/pdf/PLAW-107publ71.pdf (16.01.2016).*

[9] *Keiler/Kristoferitsch (2006) 485 f.*

[10] *Vgl ua Customs Act, Section 107.1, http://www.cbsa-asfc.gc.ca/security-securite/api_ipv-eng.html (16.01.2016).*

[11] *Siehe die Informationsseite der Regierung https://www.border.gov.au/Trav/Ente/Goin/passenger-cards/collection-of-passenger-name-records (16.01.2016).*

[12] *Mitteilung der Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer vom 21.09.2010, KOM(2010) 492 endg, 3.*

[13] *Siehe dazu Bakowski/Voronova (2015) 7 ff.*

[14] *RL 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995, ABl L 281 vom 23.11.1995, 31 ff.*

[15] *Vgl Keiler/Kristoferitsch (2006) 485 f.*

[16] *Entscheidung der Kommission 2004/535/EG vom 14.05.2004, ABl L 235 vom 06.07.2004, 11 ff.*

[17] *Beschluss des Rates 2004/496/EG vom 17.05.2004, ABl L 183 vom 20.05.2004, 83 ff.*

[18] *EuGH, verbRs C-317/04 und C-318/04, Parlament ua/Rat und Kommission ua, ECLI:EU:C:2006:346, Rn 54 ff.*

[19] *Siehe zu den Ausführungen in diesem Abschnitt Keiler/Kristoferitsch (2006) 485 ff; für die damalige Säulenstruktur und die weitere Entwicklung bis zum Vertrag von Lissabon siehe etwa Suhr (2011).*

[20] *Beschluss 2006/729/GASP/JI des Rates vom 05.10.2006, ABl L 298 vom 27.10.2006, 27 ff.*

[21] *Beschluss 2007/551/GASP/JI des Rates vom 23.07.2007, ABl L 204 vom 04.08.2007, 16 ff.*

[22] *Siehe dazu Westphal (2009) 87 f.*

[23] *Beschluss 2006/230/EG des Rates vom 18.07.2005, ABl L 82 vom 21.03.2006, 14 ff.*

[24] *Beschluss 2008/651/GASP/JI des Rates vom 30.06.2008, ABl L 213 vom 08.08.2008, 47 ff.*

[25] *Vertrag über die Arbeitsweise der Europäischen Union.*

[26] *Vertrag über die Europäische Union.*

[27] *Siehe dazu mwN Satzger (2012) Rn 1 sowie Dannecker (2012) Rn 1 und 3 f.*

[28] *Entschließung des EP vom 05.05.2010 zum Start der Verhandlungen über Abkommen über Fluggastdatensätze mit den USA, Australien und Kanada, ABl C 81 E vom 15.03.2011, 70 ff.*

[29] *Beschluss 2012/381/EU des Rates vom 13.12.2011, ABl L 186 vom 14.07.2012, 3 ff.*

[30] *Beschluss 2012/472/EU des Rates vom 26.04.2012, ABl L 215 vom 11.08.2012, 4 ff.*

[31] *Siehe etwa Artikel-29-Datenschutzgruppe (2012) 1 ff oder Lehner (2013) 976 f.*

[32] *Siehe dazu infra im Kapitel 3.*

[33] *Entschließung des EP vom 25.11.2014 zur Einholung eines Gutachtens des Gerichtshofs über die Vereinbarkeit des Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) mit den Verträgen (2014/2966[RSP]), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2014-0058+0+DOC+XML+V0//DE (11.01.2016), Pkt 1 f.*

[34] *Entscheidung der Kommission vom 26.07.2000 […], ABl L 215 vom 25.08.2000, 7 ff.*

[35] *Siehe dazu Art 25 Abs 2 Datenschutz-RL, wo die Angemessenheit des Schutzniveaus näher definiert wird.*

[36] *EuGH, Rs C-362/14, Schrems vs Data Protection Commissioner, ECLI:EU:C:2015:650.*

[37] *EuGH, Rs C-362/14, Rn 90.*

[38] *EuGH, Rs C-362/14, Rn 91 ff.*

[39] *Rahmenbeschluss 2008/977/JI des Rates vom 27.11.2008, ABl L 350 vom 30.12.2008, 60 ff.*

[40] *RL (EU) 2016/680 des EP und des Rates vom 27.04.2016, ABl L 119 vom 04.05.2016, 89 ff.*

[41] *Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken, KOM(2007) 654 endg vom 06.11.2007.*

[42] *KOM(2011) 32 endg vom 02.02.2011, http://ec.europa.eu/dgs/home-affairs/what-is-new/news/pdf/com_2011_32_final_de.pdf (28.10.2015).*

[43] *Siehe das Dokument des Rates der Europäischen Union (2012) Anlage.*

[44] *Ausschuss für Bürgerliche Freiheiten, Justiz, Inneres.*

[45] *Europäisches Parlament (2013) 5.*

[46] *Entschließung des EP vom 11.02.2015 zu Maßnahmen zur Terrorismusbekämpfung, 2015/2530(RSP), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//TEXT+TA+P8-TA-2015-0032+0+DOC+XML+V0//DE (01.12.2015), Rn 13.*

[47] *Obwohl das ordentliche Gesetzgebungsverfahren nach Art 294 AEUV eine Einigung zwischen Rat und Parlament in bis zu drei Lesungen vorsieht, wird in der Praxis oft eine solche Kompromissfindung noch vor der ersten Lesung angestrebt: Diese nicht im geschriebenen Recht verankerten Verhandlungsrunden sollen das Gesetzgebungsverfahren effizienter gestalten und eine raschere Einigung der Gesetzgeber ermöglichen. Vgl Lay (2010) 65.*

[48] *Siehe die betreffende Pressemitteilung vom 04.12.2015 auf der Website des EP unter http://www.europarl.europa.eu/news/de/news-room/20151204IPR06267/EU-PNR-EP's-rapporteur-welcomes-Home-Affairs-Ministers-green-light-to-deal (06.12.2015).*

[49] *Siehe die Erklärung des Rates vom 18.04.2016, Ratsdokument Nr 7829/16 ADD 1, 1, http://data.consilium.europa.eu/doc/document/ST-7829-2016-ADD-1/de/pdf (30.05.2016).*

[50] *Rahmenbeschluss des Rates 2002/475/JI vom 13.06.2002, ABl L 164 vom 22.06.2002, 3 ff.*

[51] *Laut Erwägungsgrund 16 der PNR-RL.*

[52] *Vgl Art 9 Abs 1 und 2 RL-Vorschlag 2011.*

[53] *Vgl für den Unterschied zwischen Anonymisierung und Pseudonymisierung, bei der die Wiederherstellung der Daten noch möglich ist, im Allgemeinen etwa Kühling ua (2011) 83 ff, im Speziellen ua Artikel-29-Datenschutzgruppe (2011) 7.*

[54] *Europäische Kommission (2011) 3.*

[55] *Siehe dazu etwa Frenz (2011) 794 ff.*

[56] *ABl C vom 18.12.2000, 1 ff.*

[57] *Zu den Grundrechten im Allgemeinen siehe etwa Schroeder (2015) 300 ff.*

[58] *Vgl ua Kroschwald (2012) 123.*

[59] *Vgl etwa FRA – Agentur der Europäischen Union für Grundrechte (2011) 6 ff; Brouwer (2011) 7 ff.*

[60] *Ibidem.*

[61] *Siehe dazu Korff/Georges (2015) 26 ff.*

[62] *Vgl Bescos Pou (2014) 199.*

[63] *Zum Verhältnis zwischen allgemeinen und speziellen Schrankenregelungen sowie zu diesen Regelungen selbst siehe ausführlich in Frenz (2008) 163 ff.*

[64] *EGMR, Urteil vom 06.09.1978, Klass ua/Bundesrepublik Deutschland, Beschwerde Nr 5029/71, Abs-Nr 46.*

[65] *EGMR, Urteil vom 26.03.1987, Leander/Schweden, Beschwerde Nr 9248/81, Abs-Nr 48 f.*

[66] *Vgl Korff/Georges (2015) 42 f sowie FRA – Agentur der Europäischen Union für Grundrechte (2011) 12 f.*

[67] *So auch FRA – Agentur der Europäischen Union für Grundrechte (2011) 13; Kroschwald (2012) 125.*

[68] *So die stRsp des EuGH, siehe zB Rs C-361/88, Kommission/Deutschland, Slg 1991, I-2567, Rn 15 f.*

[69] *Vgl mwN, auch zur einschlägigen Judikatur des EGMR, FRA – Agentur der Europäischen Union für Grundrechte (2011) 13 f oder Brouwer (2009) 17 f.*

[70] *Siehe dazu FRA – Agentur der Europäischen Union für Grundrechte (2011) 14, mwN.*

[71] *In diesem Sinne auch FRA – Agentur der Europäischen Union für Grundrechte (2011) 14 f.*

[72] *Vgl dazu das Urteil des EGMR vom 04.05.2000, Rotaru/Rumänien, Beschwerde Nr 28341/95, Abs-Nr 56 ff. Zu dieser Ansicht gelangt man auch, wenn man die PNR-RL mit den Leitlinien der Grundrechte-Agentur für nationale PNR-Systeme vergleicht: FRA – Agentur der Europäischen Union für Grundrechte (2014).*

[73] *Siehe dazu FRA – Agentur der Europäischen Union für Grundrechte (2011) 16, mwN zur Judikatur des EGMR sowie Artikel-29-Datenschutzgruppe (2011) 2 ff.*

[74] *So auch Bescos Pou (2014) 206.*

[75] *Vgl dazu etwa Artikel-29-Datenschutzgruppe (2011) 2 ff.*

[76] *Europäische Kommission (2011) 133 endg, cit.*

[77] *Europäischer Datenschutzbeauftragter (2011) Rn 9 ff; FRA – Agentur der Europäischen Union für Grundrechte (2011) 17 f.*

[78] *In diesem Sinne auch Kroschwald (2012) 127 f.*

[79] *Siehe Artikel-29-Datenschutzgruppe (2011) 4.*

[80] *FRA – Agentur der Europäischen Union für Grundrechte (2011) 16 f.*

[81] *FRA – Agentur der Europäischen Union für Grundrechte (2011) 19 f.*

[82] *Siehe die dem RL-Vorschlag vorangestellte Begründung der Europäischen Kommission, KOM(2011) 32 endg vom 02.02.2011, 4 f.*

[83] *Vgl FRA – Agentur der Europäischen Union für Grundrechte (2011) 19 ff; Artikel-29-Datenschutzgruppe (2011) 5.*

[84] *Siehe etwa Kroschwald (2012) 133 ff.*

[85] *EuGH, verbRs C-293/12 und C-594/12, Digital Rights Ireland ua, ECLI:EU:C:2014:238.*

[86] *ABl L Nr 105 vom 13.04.2006, 54 ff.*

[87] *EuGH, verbRs C-293/12 und C-594/12, Rn 29 und 33 f.*

[88] *EuGH, verbRs C-293/12 und C-594/12, Rn 36.*

[89] *EuGH, verbRs C-293/12 und C-594/12, Rn 37.*

[90] *EuGH, verbRs C-293/12 und C-594/12, Rn 39 f.*

[91] *EuGH, verbRs C-293/12 und C-594/12, Rn 41 ff.*

[92] *EuGH, verbRs C-293/12 und C-594/12, Rn 46.*

[93] *EuGH, verbRs C-293/12 und C-594/12, Rn 49.*

[94] *EuGH, verbRs C-293/12 und C-594/12, Rn 51 f.*

[95] *EuGH, verbRs C-293/12 und C-594/12, Rn 56 ff.*

[96] *EuGH, verbRs C-293/12 und C-594/12, Rn 59.*

[97] *EuGH, verbRs C-293/12 und C-594/12, Rn 62.*

[98] *EuGH, verbRs C-293/12 und C-594/12, Rn 63 f.*

[99] *EuGH, verbRs C-293/12 und C-594/12, Rn 65.*

[100] *EuGH, verbRs C-293/12 und C-594/12, Rn 71.*

[101] *EuGH, verbRs C-293/12 und C-594/12, Rn 61.*

[102] *Siehe dazu supra va in den Abschnitten 2.3. bis 2.6. sowie im Abschnitt 3.3. In diesem Sinne äußerte sich auch die Kommission nach dem Urteil zur Vorratsdatenspeicherung auf Anfrage des EP: Europäische Kommission, Brief an EP-Präsident Martin Schulz, Ares(2015)1078948 vom 11.03.2015, 2.*

[103] *Siehe dazu die Ausführungen im Abschnitt 3.3.*

[104] *EuGH, verbRs C-293/12 und C-594/12, Rn 37. Siehe auch Rn 59 und die diesbezüglichen Ausführungen in Europäische Kommission (2015) 2.*

[105] *Vgl dazu supra im Abschnitt 3.3.*

[106] *Siehe ibidem.*

[107] *EuGH, verbRs C-293/12 und C-594/12, Rn 49.*

[108] *Siehe dazu die Ausführungen im Abschnitt 3.2.4. sowie Europäischer Datenschutzbeauftragter (2015) 7.*

[109] *Vgl Korff/Georges (2015) 24 f.*

[110] *So etwa der Europäische Datenschutzbeauftragte Buttarelli in Tiefenthaler (2015); Hametner (2015); Korff/Georges (2015) 24 ff; Rath (2015); Rudmin (2006).*

[111] *Vgl die Interviews mit Buttarelli in Tiefenthaler (2015) und in Bonanni (2015). Im ORF-Interview wird auch das neue Datenschutzpaket (allgemeine Verordnung und RL im einschlägigen Bereich der Zusammenarbeit von Polizei und Justiz) angesprochen, das zusammen mit der PNR-RL verhandelt und verabschiedet wurde, und das den Informationsaustausch auf eine neue Ebene stellen könnte.*

[112] *Vgl etwa die Ausführungen des GA Philippe Léger in den Schlussanträgen vom 22.11.2005 (verbRs C-317/04 und C-318/04, Slg I-4726 ff), wonach die Politik angesichts des Wesens und der Bedeutung des Zieles der Terrorismusbekämpfung einen weiten Spielraum bei der Beurteilung der Angemessenheit und Zweckmäßigkeit der Maßnahmen im Kampf gegen Terror und schwere Straftaten haben sollte (Rn 231 ff). Der EuGH ging auf diese Ausführungen nicht ein, da er ein kompetenzrechtliches Urteil fällte.*

Quellenangaben

Artikel-29-Datenschutzgruppe, Stellungnahme Nr 10/2011 vom 05.04.2011, WP 181, Online: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_de.pdf (07.06.2016).

Artikel-29-Datenschutzgruppe, Stellungnahme Ares(2012)15841 vom 06.01.2012, Online: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120106_letter_libe_pnr_en.pdf (07.06.2016).

Bakowski/Voronova, Briefing: The proposed EU passenger name records (PNR) directive. Revived in the new security context (2015), Wissenschaftlicher Dienst des Europäischen Parlaments, Online: http://www.europarl.europa.eu/EPRS/EPRS-Briefing-554215-The-EU-PNR-Proposal-FINAL.pdf (07.06.2016).

Bescos Pou, Data Protection vs. Security in the European Union, in European Yearbook on Human Rights (2014) 197.

Bonanni/Buttarelli, „Schedare i passeggeri è contro i Trattati Ue". Il garante europeo boccia la stretta sui voli, Repubblica.it vom 10.12.2015, Online: http://www.repubblica.it/esteri/2015/12/10/news/giovanni_buttarelli_schedare_i_passeggeri_e_contro_i_trattati_ue_il_garante_europeo_boccia_la_stretta_sui_voli-129173883/ (07.06.2016).

Brouwer, The EU Passenger Name Record System and Human Rights: Transferring passenger data or passenger freedom?, CEPS Working Document No 320/September 2009, Online: https://www.ceps.eu/system/files/book/2009/09/1903.pdf (07.06.2016).

Brouwer, Ignoring Dissent and Legality: The EU's proposal to share the personal information of all passengers, in: CEPS Liberty and Security in Europe (2011), Online: https://www.ceps.eu/publications/ignoring-dissent-and-legality-eu%E2%80%99s-proposal-share-personal-information-all-passengers (07.06.2016).

Dannecker, AEUV Art 87, in: Streinz (Hrsg), EUV/AEUV[2] (2012).

Europäische Kommission, SEK(2011) 133 endg vom 02.02.2011, Arbeitsdokument der Kommissionsdienststellen. Zusammenfassung der Folgenabschätzung. Begleitdokument zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über ein gemeinsames Konzept für die Verwendung von Fluggastdatensätzen, Online: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sec/com_sec%282011%290133_/comsec%282011%290133_de.pdf (07.06.2016).

Europäische Kommission, Brief an EP-Präsident Martin Schulz, Ares(2015)1078948 vom 11.03.2015, Online: http://www.eppgroup.eu/system/files_force/news_attachement/Timmermans%20letter%20EU-PNR.PDF?download=1 (07.06.2016).

Europäischer Datenschutzbeauftragter, Stellungnahme [zum RL-Vorschlag], 2011/C 181/02, ABl C 181 vom 22.06.2011, 24 ff.

Europäischer Datenschutzbeauftragter, Zweite Stellungnahme [zum RL-Vorschlag], Stellungnahme Nr 5/2015, Online: http://tinyurl.com/znzvfok (07.06.2016).

Europäisches Parlament, Plenarsitzungsdokument, A7-0150/2013 vom 29.04.2013, Online: http://tiny url.com/zf8dljn (07.06.2016).

FRA – Agentur der Europäischen Union für Grundrechte, Gutachten Nr 1/2011, Fluggastdatensätze, Online: http://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_DE.pdf (07.06.2016).

FRA – Agentur der Europäischen Union für Grundrechte, Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data (2014), Online: https://fra.europa.eu/sites/default/files/fra-2014-fundamental-rights-considerations-pnr-data-en.pdf (07.06.2016).

Frenz, Handbuch Europarecht, Band 4: Europäische Grundrechte (2008).

Frenz, Handbuch Europarecht, Band 6: Institutionen und Politiken (2011).

Frenz, Europarecht[2] (2015).

Hametner, Mehr Überwachung bringt nicht zwingend mehr Sicherheit, derStandard.at vom 13.01.2015, Online: http://derstandard.at/2000010279942/Mehr-Ueberwachung-bringt-nicht-zwingend-mehr-Sicherheit (07.06.2016).

House of Lords European Union Committee, 15[th] Report of Session 2007–08: The Passenger Name Record (PNR) Framework Decision (2008), Online: http://tinyurl.com/zbytx2o (07.06.2016).

Keiler/Kristoferitsch, Passagierdaten auf dem Flug in die USA: Neues Abkommen der EU mit den USA über die Weitergabe von Passagiedaten nach dem Urteil des EuGH verb Rs C-317/04, C-318/04, ZVR 2006/189, 484 ff.

Korff/Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards (2015), Online: http://tinyurl.com/gt2fc29 (07.06.2016).

Kroschwald, Sicherheitsmaßnahmen an Flughäfen im Lichte der Grundrechte (2012).

Kühling/Seidel/Sivridis, Datenschutzrecht[2] (2011).

Lay, Das Europäische Parlament in der Justiz- und Innenpolitik der Europäischen Union (2010).

Lehner, Democrazia e tutela dei dati personali nell'Unione europea: l'evoluzione della negoziazione sul PNR dopo il Trattato di Lisbona, in: Torre (Hrsg), Costituzioni e sicurezza dello Stato (2013) 941.

Rat der Europäischen Union, Dokument Nr 8916/12 vom 23.04.2012, Vermerk des Vorsitzes für den Rat, Online: http://register.consilium.europa.eu/doc/srv?f=ST+8916+2012+INIT&l=de (07.06.2016).

Rath, Nach dem Germanwings-Crash: Bessere Daten, bessere Überwachung, TAZ.de vom 02.04.2015, Online: http://www.taz.de/Nach-dem-Germanwings-Crash/!5014079/ (07.06.2016).

Rudmin, The Politics of Paranoia and Intimidation, LewRockwell.com, 26.05.2006, Online: http://archive.lewrockwell.com/orig7/rudmin1.html (07.06.2016).

Satzger, AEUV Art 82, in Streinz (Hrsg), EUV/AEUV[2] (2012).

Schroeder, Grundkurs Europarecht[4] (2015).

Suhr, AEUV Art 67, in: Calliess/Ruffert (Hrsg), EUV/AEUV[4] (2011).

Tiefenthaler, Die „Illusion" des Tech-Mythos: „Kühlen Kopf bewahren", news.ORF.at vom 26.11.2015, Online: http://orf.at/stories/2311151/2311137/ (07.06.2016).

U.S. Department of Homeland Security/U.S. Customs and Border Protection, Passenger Name Record (PNR) Privacy Policy (2013), Online: http://www.cbp.gov/sites/default/files/documents/pnr_privacy.pdf (07.06.2016).

Westphal, Grundlagen und Bausteine des europäischen Datenschutzrechts, in: Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 53.

Weiterführende Literatur und Links

Europäisches Parlament, Plenarsitzungsdokument, A8-0248/2015 vom 07.09.2015, Online: http://tinyurl.com/jcr8vb9 (07.06.2016).

Maan, EU-Innenminister einigen sich auf Fluggastdatenspeicherung, derStandard.at vom 04.12.2015, Online: http://derstandard.at/2000026671380/EU-Innenminister-einigen-sich-auf-Fluggastdatenspeicherung (07.06.2016).

Rossi Dal Pozzo, EU Legal Framework for Safeguarding Air Passenger Rights (2015).