18. Wahlperiode

Deutscher Bundestag
Innenausschuss

Wortprotokoll
der 114. Sitzung

Innenausschuss
Berlin, den 24. April 2017, 16:00 Uhr
10557 Berlin, Konrad-Adenauer-Str. 1
Paul-Löbe-Haus, Raum 4 900

Vorsitz: Ansgar Heveling, MdB

Öffentliche Anhörung

Einziger Tagesordnungspunkt

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz - FlugDaG)

BT-Drucksache 18/11501

Federführend:
Innenausschuss

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Verkehr und digitale Infrastruktur
Ausschuss für Tourismus
Ausschuss Digitale Agenda
Ausschuss für die Angelegenheiten der Europäischen Union
Haushaltsausschuss (§ 96 GO)

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:
Abg. Armin Schuster (Weil am Rhein) [CDU/CSU]
Abg. Wolfgang Gunkel [SPD]
Abg. Martina Renner [DIE LINKE.]
Abg. Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]

Inhaltsverzeichnis

		Seite
I.	Anwesenheitslisten	4
II.	Sachverständigenliste	11
III.	Sprechregister der Sachverständigen und Abgeordneten	12
IV.	Wortprotokoll der Öffentlichen Anhörung	13
V.	Anlagen	37
	Änderungsantrag der Fraktionen der CDU/CSU und SPD zu BT-Drucksache 18/11501	18(4)855
	Stellungnahmen der Sachverständigen zur Öffentlichen Anhörung	
	Alexander Sander	18(4)869 B
	Matthias Knetsch	18(4)869 C
	Präsident Holger Münch	18(4)869 D
	Prof. Dr. Ferdinand Wollenschläger	18(4)869 E
	Prof. Dr. Clemens Arzt	18(4)869 F

Unangeforderte Stellungnahme

Die Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit 18(4)869 A

Gutachterliche Stellungnahme des Parlamentarischen Beirats
für nachhaltige Entwicklung

zu BT-Drucksache 18/11501 18(4)798

18. Wahlperiode

Deutscher Bundestag

Sitzung des Innenausschusses (4. Ausschuss)

Montag, 24. April 2017, 16:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
CDU/CSU		**CDU/CSU**	
Baumann, Günter		Albsteiger, Katrin	
Binninger, Clemens		Berghegger Dr., André	
Bosbach, Wolfgang		Brähmig, Klaus	
Frieser, Michael		Brandt, Helmut	
Hellmuth, Jörg		Fabritius Dr., Bernd	
Heveling, Ansgar		Feiler, Uwe	
Hoffmann (Dortmund), Thorsten		Giousouf, Cemile	
Lindholz, Andrea		Gröhler, Klaus-Dieter	
Mayer (Altötting), Stephan		Harbarth Dr., Stephan	
Ostermann Dr., Tim		Hauer, Matthias	
Schäfer (Saalstadt), Anita		Heck Dr., Stefan	
Schuster (Weil am Rhein), Armin		Liebing, Ingbert	
Veith, Oswin		Luczak Dr., Jan-Marco	
Warken, Nina		Monstadt, Dietrich	
Wendt, Marian		Sensburg Dr., Patrick	
Wichtel, Peter		Ullrich Dr., Volker	
Woltmann, Barbara		Wellenreuther, Ingo	
Zertik, Heinrich		Wittke, Oliver	

12. April 2017

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339

VH

18. Wahlperiode

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 24. April 2017, 16:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
SPD		**SPD**	
Castellucci Dr., Lars		Esken, Saskia	
Fograscher, Gabriele		Fechner Dr., Johannes	
Grötsch, Uli		Gerster, Martin	
Gunkel, Wolfgang		Högl Dr., Eva	
Hartmann, Sebastian		Juratovic, Josip	
Lischka, Burkhard		Kolbe, Daniela	
Mittag, Susanne		Lühmann, Kirsten	
Özdemir (Duisburg), Mahmut		Poschmann, Sabine	
Reichenbach, Gerold		Rix, Sönke	
Schmidt (Berlin), Matthias		Spinrath, Norbert	
Veit, Rüdiger		Yüksel, Gülistan	
DIE LINKE.		**DIE LINKE.**	
Jelpke, Ulla		Dağdelen, Sevim	
Korte, Jan		Hahn Dr., André	
Renner, Martina		Karawanskij, Susanna	
Tempel, Frank		Pau, Petra	

18. Wahlperiode

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 24. April 2017, 16:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
BÜ90/GR		**BÜ90/GR**	
Amtsberg, Luise		Haßelmann, Britta	
Beck (Köln), Volker		Künast, Renate	
Mihalic, Irene		Lazar, Monika	
Notz Dr., Konstantin von		Mutlu, Özcan	

12. April 2017

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339

Seite 3 von 3

Anwesenheitsliste für Abgeordnete mitberatender Ausschüsse

Öffentliche Anhörung des Innenausschusses am Montag, 24. April 2017
114. Sitzung

Name (bitte in Druckschrift)	Unterschrift
Krüger-Leißner, Angelika	A. Krüger-L.

Tagungsbüro

Deutscher Bundestag

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 24. April 2017, 16:00 Uhr

	Fraktionsvorsitz	Vertreter
CDU/CSU		
SPD		
DIE LINKE.		
BÜNDNIS 90/DIE GRÜNEN		

Fraktionsmitarbeiter

Name (Bitte in Druckschrift)	**Fraktion**	**Unterschrift**
Burczyk, Dirk	LINKE	
Martin, Stephan	Linke	
Uecker, Stefan	SPD	
Leopold, Wiebke	Grüne	

Stand: 20. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

49

Tagungsbüro | **Sitzung des Innenausschusses (4. Ausschuss)** Montag, 24. April 2017, 16:00 Uhr | Seite 3

Bundesrat

Land	Name (bitte in Druckschrift)	Unterschrift	Amts-bezeichnung
Baden-Württemberg			
Bayern	Luderschmid		RD
Berlin			
Brandenburg	Bampl		KgA
Bremen	Kaufmann		
Hamburg			
Hessen			
Mecklenburg-Vorpommern	PAUCH		
Niedersachsen			
Nordrhein-Westfalen			
Rheinland-Pfalz			
Saarland			
Sachsen			
Sachsen-Anhalt	Stövesand		MRi 4
Schleswig-Holstein			
Thüringen			

Stand: 20. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Tagungsbüro

Sitzung des Innenausschusses (4. Ausschuss)
Montag, 24. April 2017, 16:00 Uhr

Ministerium bzw. Dienststelle (bitte in Druckschrift)	**Name** (bitte in Druckschrift)	**Unterschrift**	**Amts-bezeichnung**
BfDI	Dr Gnedler, Iris		RDn
BMI	Dr. Schallenberg		RD
BMI	Heuegel		RDn
BMI	Fährmann		Ref
BMI	Zaunes		KOK
BMI	Dubbert		RD
BK	Seedorf		RD
BMJV	Sommer		Ref in LG
BMF	Dr. Geitzsch		RR

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 24. April 2017, 16.00 Uhr

Prof. Dr. Clemens Arzt
Hochschule für Wirtschaft und Recht Berlin

Matthias Knetsch
Lufthansa Group and Government Services bei SITA, Eschborn

Präsident Holger Münch
Bundeskriminalamt, Wiesbaden

Alexander Sander
Digitale Gesellschaft e.V., Berlin

Prof. Dr. Ferdinand Wollenschläger
Universität Augsburg

Sprechregister der Sachverständigen und Abgeordneten

Sachverständige	Seite
Prof. Dr. Ferdinand Wollenschläger	13, 30, 33
Alexander Sander	15, 28, 34
Präsident Holger Münch	16, 26, 28, 35
Matthias Knetsch	18, 25, 26
Prof. Dr. Clemens Arzt	20, 24, 36

Abgeordnete	
Vors. Ansgar Heveling (CDU/CSU)	13, 15, 16, 18, 20, 22, 23, 24, 25, 26 28, 30, 31, 32, 33, 34, 35, 36
Abg. Stephan Mayer (Altötting) (CDU/CSU)	31
BE Abg. Armin Schuster (Weil am Rhein) (CDU/CSU)	22, 26
BE Abg. Wolfgang Gunkel (SPD)	23, 28
BE Abg. Martina Renner (DIE LINKE.)	23, 32
Abg. Irene Mihalic (BÜNDNIS 90/DIE GRÜNEN)	24, 32

Einziger Tagesordnungspunkt

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz - FlugDaG)

BT-Drucksache 18/11501

Vors. **Ansgar Heveling** (CDU/CSU): So, ich würde jetzt gerne beginnen, auch wenn Herr Prof. Dr. Arzt noch nicht da ist. Aber ansonsten sind alle Sachverständigen anwesend und dann reihen wir Herrn Prof. Dr. Arzt gleich ein.

Dann darf ich die 114. Sitzung des Innenausschusses eröffnen, die heute als öffentliche Anhörung zum Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie 2016/681 (Fluggastdatengesetz) durchgeführt wird.

Ich danke Ihnen sehr geehrte Herren Sachverständige, dass Sie unserer Einladung nachgekommen sind, um die Fragen der Kolleginnen und Kollegen aus dem Innenausschuss und gegebenenfalls der mitberatenden Ausschüsse zu beantworten. Die Ergebnisse der Anhörung dienen dazu, die weiteren Beratungen zu dem Gesetzentwurf vorzubereiten.

Leider muss ich dem Ausschuss mitteilen, dass der Sachverständige Prof. Dr. Schwarz, der ursprünglich auch geladen war, aufgrund eines Trauerfalls seine Teilnahme heute absagen musste.

Ich darf sehr herzlich die Gäste und Zuhörer begrüßen und für die Bundesregierung Herrn Staatssekretär Dr. Krings.

Die Sitzung wird im Parlamentsfernsehen des Deutschen Bundestages weltweit übertragen. Schriftliche Stellungnahmen haben wir trotz der Kürze der Vorbereitungszeit erbeten. Für die eingegangenen Stellungnahmen darf ich mich bei Ihnen, sehr geehrte Herren Sachverständige, sehr herzlich bedanken. Sie sind an die Mitglieder des Innenausschusses und der mitberatenden Ausschüsse verteilt worden und werden dem Protokoll über diese Sitzung beigefügt. Ich gehe davon aus, dass Ihr Einverständnis zur öffentlichen Durchführung der Anhörung auch das Einverständnis zur Aufnahme der Stellungnahmen in eine Gesamtdrucksache umfasst? Ich sehe da keinen Widerspruch.

Von der heutigen Anhörung wird für ein Wortprotokoll eine Bandabschrift gefertigt. Das Protokoll wird Ihnen, sehr geehrte Herren Sachverständige, zur Korrektur übersandt. Im Anschreiben werden Ihnen weitere Details zur Behandlung mitgeteilt. Die Gesamtdrucksache, bestehend aus Protokoll und schriftlichen Stellungnahmen, wird im Übrigen dann auch ins Internetangebot des Deutschen Bundestages eingestellt.

Zum zeitlichen Ablauf darf ich anmerken, dass insgesamt eine Zeit bis 18.00 Uhr für die Anhörung vorgesehen ist. Einleitend erhält jeder der Herren Sachverständigen die Gelegenheit, in einer Eingangsstellungnahme von maximal fünf Minuten zum Beratungsgegenstand Stellung zu nehmen. Dann wird die Befragung durch die Vertreter der Fraktionen beginnen – die Berichterstatterinnen und Berichterstatter sowie dann möglicherweise in einer weiteren Runde auch noch weitere Abgeordnete.

Ich möchte jetzt schon darum bitten, dass die Fragesteller denjenigen Sachverständigen ausdrücklich benennen, an den eine Frage gerichtet wird und limitiert und knapp gehaltene Fragen ermöglichen es natürlich, dass möglichst viele Kolleginnen und Kollegen mit Fragen zu Wort kommen oder wir möglichst viele Fragen abarbeiten können. Wenn Sie damit einverstanden sind würden wir so verfahren.

Und angesichts dessen, dass Prof. Dr. Arzt am Anfang des Alphabetes steht und wir normalerweise dort beginnen, er aber noch nicht da ist, machen wir es diesmal umgekehrt und fangen auf der anderen Seite des Alphabetes an. Insofern darf ich Ihnen, sehr geehrter Prof. Dr. Wollenschläger, als erstem Sachverständigen das Wort geben.

Wenn fünf Minuten um sind, dann werde ich mich durch Hüsteln bemerkbar machen.

SV **Prof. Dr. Ferdinand Wollenschläger** (Universität Augsburg): Vielen Dank Herr Vorsitzender, meine sehr geehrten Damen und Herren Abgeordnete, sehr geehrte Damen und Herren. Ich bedanke mich zunächst herzlich für die Einladung zur Anhörung zur Fluggastdatenverarbeitung. Angesichts der Kürze der Zeit steige ich gleich in den Inhalt ein. Die Regelung zur „Fluggastdatenverarbeitung“, darauf möchte ich

einleitend hinweisen, erfasst – anders als die Telekommunikationsvorratsdatenspeicherung – ein ganzes Bündel informationeller Maßnahmen bezüglich dessen, was mit den Daten geschieht, die die Fluggesellschaften an das Bundeskriminalamt übermitteln müssen. Im Wesentlichen sprechen wir neben der Übermittlungspflicht über drei Eingriffe: Einmal den relativ unproblematischen Abgleich mit Fahndungsdatenbanken, dann den Abgleich mit Mustern, die auf gewisse Gefährdungsprofile hinweisen, und darüber hinaus noch eine fünfjährige Vorratsdatenspeicherung der Fluggastdaten.

Bei einer Bewertung dieser Eingriffe ist zunächst festzuhalten, dass es sich durchaus um gewichtige Grundrechtseingriffe handelt, weil jedenfalls ein größerer Teil dieser informationellen Maßnahmen jeden Passagier unabhängig von einem Bezug zu terroristischen Straftaten und schwerer Kriminalität trifft. Auf der anderen Seite ist aber auch festzuhalten, dass die Ziele, denen die Fluggastverarbeitung dient, auf Verfassungsebene sehr hoch anzusiedeln sind, nämlich terroristische Straftaten und schwere Kriminalität zu verhüten; beide Ziele sind nicht nur in der Rechtsprechung des Bundesverfassungsgerichts, sondern auch in der Rechtsprechung des Europäischen Gerichtshofs anerkannt als prinzipiell tauglich, Eingriffe dieser Art zu rechtfertigen.

Im vorliegenden Sachverhalt kommt, und das macht die Bewertung insoweit ein bisschen komplizierter, erschwerend hinzu, dass wir hier über keinen autonomen Gesetzentwurf des Bundestags sprechen, sondern das Gesetz dient, wie es auch im Titel zum Ausdruck kommt, der Umsetzung der EU-Fluggastdatenrichtlinie, die die meisten der hier in Frage stehenden Grundrechtseingriffe für den deutschen Gesetzgeber zwingend vorgibt. In diesem Kontext ist zu berücksichtigen, dass der Bundestag als deutscher Gesetzgeber verpflichtet ist, diese Vorgaben der Richtlinie in nationales Recht umzusetzen. In Bezug auf Einwände gegen die Umsetzung wegen möglicher Grundrechtsverletzungen, insbesondere aufgrund der Anlasslosigkeit, der Weite der Datenkategorien, der Speicherdauer, der Arbeit mit Mustern oder auch aufgrund der fehlenden Benachrichtigung, ist festzuhalten, dass der EuGH eine sehr strenge Linie verfolgt und nur sehr schwere, evidente Europarechtsverstöße als Rechtfertigung für eine Nichtumsetzung genügen lässt.

Bei Betrachtung der bestehenden Rechtsprechung auf europäischer Ebene ist festzuhalten, dass keine unmittelbar einschlägige Rechtsprechung des Europäischen Gerichtshofs existiert. Die Rechtsprechung des Europäischen Gerichtshofs, unabhängig davon, wie streng man auch die letzte Entscheidung von Dezember 2016 zur Vorratsdatenspeicherung versteht, ist nicht unmittelbar auf den hiesigen Sachverhalt zu übertragen, weil die Fluggastdatenverarbeitung meines Erachtens, und das hat auch der Generalanwalt in seiner Stellungnahme deutlich gemacht, der deutlich geringere Eingriff ist im Vergleich zur Telekommunikationsverkehrsdatenspeicherung. Denn die Aussagekraft der Daten und die Streubreite ist bei der Fluggastdatenverarbeitung wesentlich geringer. Auch wenn man den Schlussantrag der beiden Generalanwälte zu den bisherigen Verfahren betrachtet, die allerdings beide noch nicht zu einem Urteil in der Sache geführt haben, ergibt sich eine im Grunde positive Bewertung. Es ist daher kein evidenter und schwerer Verstoß gegen europäische Grundrechte anzunehmen. Aber auch im Übrigen halte ich die Fluggastdatenverarbeitung auf der Basis der Rechtsprechung, insoweit man sie nicht für übertragbar hält, sowie der Schlussanträge der Generalanwälte für prinzipiell mit den Unionsgrundrechten vereinbar. Im Einzelnen habe ich das in meiner relativ umfangreichen Stellungnahme versucht auszubuchstabieren, auf die ich an dieser Stelle pauschal verweisen darf.

Der Deutsche Bundestag hat darüber hinaus eine sehr gewichtige Entscheidung autonom getroffen. Die Richtlinie ermöglicht, über die zwingend erfassten Flugverbindungen zu Drittstaaten auch alle EU-Flüge einzubeziehen. Von dieser Möglichkeit hat der deutsche Gesetzgeber – wie im Übrigen alle anderen Mitgliedstaaten – Gebrauch gemacht. Diese Entscheidung muss sich nun nicht nur an europäischen Grundrechten messen lassen, sondern auch am deutschen Verfassungsrecht. Für das deutsche Verfassungsrecht, auch das habe ich in meiner Stellungnahme näher ausgeführt, ergibt sich meines Erachtens aber nichts grundsätzlich anderes: Ihm lässt sich kein prinzipielles Verbot der Fluggastdatenverarbeitung entnehmen, sodass

auch insoweit im Grundsatz keine durchgreifenden Einwände bestehen.

Gleichwohl erachte ich den Gesetzentwurf an einigen Punkten für überarbeitungsfähig. Die Punkte habe ich der Reihe nach mit den Normen in der Zusammenfassung meiner Stellungnahme aufgelistet, ich gehe daher im Folgenden nur kurz darauf ein. Meines Erachtens sollte man zur Erhöhung der Bestimmtheit einen Straftatenkatalog aufnehmen. Das ist der erste Punkt. Der zweite Punkt ist, dass unter den Begriff „schwere Kriminalität“ auch alle Betrugsstraftaten fallen, auch ein Betrug im niedrigen Eurobereich; das schießt meines Erachtens über das Ziel hinaus. Man sollte vielleicht prüfen, hier eine Erheblichkeitsschwelle im Einzelfall in das Gesetz aufzunehmen, wie das bei anderen Eingriffsnormen der Fall ist. Ich erachte diese beiden Punkte, wie die Folgenden auch, für vereinbar auch mit der europäischen Richtlinie, jedenfalls bei einer grundrechtskonformen Auslegung.

Geändert werden sollte zudem, wie das auch die Gesetzesbegründung andeutet, die Möglichkeit für Strafverfolgungsbehörden, die Fluggastdaten auch zu anderen Zwecken als zur Verfolgung schwerer Kriminalität und terroristischer Straftaten zu nutzen. Diese sehr weit reichende Verwendungsmöglichkeit ist in der Richtlinie enthalten; sie muss meines Erachtens, auch vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts, eingeschränkt werden.

Wenn Sie noch zwei Punkte zusammenfassend gestatten? Vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts zum BKA-Gesetz und zur Antiterrordatei sind meines Erachtens die Aufsichtsbefugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit über die Erstellung von Mustern hinaus zu erstrecken. Schließlich: mit Blick auf eine transparente Richtlinienumsetzung würde ich dafür plädieren, die Datenschutzvorgaben, die die Richtlinie enthält, die das deutsche Recht aber auch der Sache nach gewährleistet, durch einen expliziten Verweis in das Fluggastdatengesetz aufzunehmen. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Prof. Dr. Wollenschläger. Dann erhält als nächstes Herr Alexander Sander von der Digitalen Gesellschaft das Wort. Bitte sehr.

SV **Alexander Sander** (Digitale Gesellschaft e.V., Berlin): Vielen Dank Herr Vorsitzender. Ich sehe das ein bisschen anders als mein Vorredner. Und zwar glaube ich sehr wohl, dass die Fluggastdatenspeicherung und -auswertung gegen die Grundrechte verstößt, gegen die europäischen Grundrechte und ich möchte das auch kurz erklären. Und das fängt zum einem damit an, welche Daten überhaupt gespeichert werden. Also es sind Daten, die in ihrer Gesamtheit den Bereich des Privatlebens umfassen und die auch Rückschlüsse auf das Intimleben der Reisenden zulassen. Es handelt sich um Informationen wie Kontaktdaten, wie E-Mail-Adresse oder die Telefonnummer. Informationen über die Mitreisenden, Zahlungsinformationen und der absolute Gipfel dieser Datensammelwut ist dann eben ein Feld „Allgemeine Hinweise“. Das ist im Grunde ein Freifeld, wo alles Mögliche eingetragen werden kann, wo auch nicht nachvollziehbar ist, was dann eben in diesem Feldnamen am Ende drinnen steht und wo eben durchaus sensible Informationen mit umfasst sind.

Auch die Erstreckung der Fluggastdatenspeicherung auf innereuropäische Flüge ist für mich jetzt nicht wirklich nachvollziehbar. In der Begründung des Gesetzes heißt es lapidar, dass diese Täter und Tätergruppierungen sich auch häufig auf Reiserouten innerhalb der Europäischen Union bewegen. Unklar ist aber, wie sie das machen. Es wird nicht erklärt, ob sie dabei tatsächlich Flugzeuge nutzen, in welchem Umfang das geschieht und in welcher Art und Weise da überhaupt diese Fluggastdatenspeicherung Sinn macht. Also weder bei den Daten, die gespeichert werden, wird erklärt, warum diese Daten notwendig sind und auch bei der Erstreckung auf innereuropäische Flüge ist es auch nicht klar. Es bleibt zum Beispiel offen, warum nicht Passdaten ausreichen, also sowas wie Name oder eben diese Informationen, also Advance Passenger Information, die bereits jetzt schon gesammelt werden. Es bleibt also vollkommen unklar, warum noch weitere Daten gespeichert werden. All das was hier dazu erzählt wird, sind immer Anekdoten, dass das irgendwie gebraucht wird. Es ist aber eben völlig unklar, warum tatsächlich genau diese

Informationen gebraucht werden. Dafür gibt es keine Begründung.

Bei der Datenverarbeitung selbst ist es eben relativ nachvollziehbar, dass gesagt wird, dass man mit bestehenden Datenbanken diese Informationen abgleichen will, wobei da auch unklar bleibt, was jetzt diese bestehenden Datenbanken sind, also wahrscheinlich alle, die bis jetzt da sind und alle, die vielleicht irgendwann mal dazu kommen. Sehr problematisch ist aber eben der Abgleich mit Mustern. Dieser Musterabgleich ist nichts anderes als eine Profiling-Maßnahme, die auf verdachtsbegründende und verdachtsentlastende Prüfmerkmale zurückgreift und die so miteinander kombiniert, dass, Zitat: „Die Zahl der unter ein Muster fallenden Personen möglichst gering ist“. Also Leute, die nicht verdächtig sind. Das bedeutet ganz klar, dass hier eben unbescholtene Bürgerinnen und Bürger durch diese Maßnahmen in das Visier von Ermittlungsbehörden geraten und dadurch mit weiteren Überwachungsmaßnahmen konfrontiert sind.

Hinzu kommt, dass dann im Rahmen der CeBIT auch das technische Konzept vorgestellt wurde. Da wurde gesagt, dass 0,07 Prozent der Datensätze dann an die Ermittlungsbehörden zu einer genaueren Überprüfung weitergeleitet werden sollen. Auch hier bleibt völlig unklar, wie man auf diese Zahl kommt. Es gibt auch da eben keinen Beleg dafür, dass genau diese Zahl die notwendige Anzahl von Leuten ist, die überwacht werden müssen. Und auch hier eben zu sagen, dass ist die Anzahl von Leuten, die eben überwacht werden müssen, ist völlig unklar.

Auch die Speicherdauer an sich von fünf Jahren ist völlig ohne Begründung aus der Luft gegriffen. Im Gesetz, also vor allen Dingen eben von der EU vorgegeben worden, aber auch hier kann diese Speicherdauer weder als verhältnismäßig noch angemessen bezeichnet werden, weil völlig unklar ist, warum diese Speicherdauer fünf Jahre ist und nicht zum Beispiel ein halbes Jahr, ein Jahr oder fünfzehn Jahre, wie es zum Beispiel in den USA der Fall ist.

Problematisch ist auch die Weitergabe an verschiedene Institutionen. Auch die Weitergabe an verschiedene Mitgliedstaaten und vor allen Dingen eben an Drittstaaten. Das ist ein völlig unkontrollierbarer Kreis von Personen, die am Ende des Tages Zugriff auf diese Datensätze haben. Auch hier wieder, wenn man in die USA schaut, haben 14.000 Departement of Homeland Security Officers Zugriff auf diese Datensätze, die von der EU in die USA übermittelt werden. Das ist eine ganze Menge von Leuten und diese Datensammlung wird natürlich in entsprechender Weise auch gewisse Begehrlichkeiten wecken und bringt ein gewisses Missbrauchspotenzial mit. Also, es bleibt an vielen Stellen völlig unklar, warum diese Maßnahmen so getroffen werden, wie sie getroffen werden. Es fehlt jeder konkrete Nachweis dafür, dass es ein taugliches Mittel ist. Und wenn wir uns die letzten Anschläge anschauen, so ist es so, dass die Attentäter oft schon zuvor im Visier der Ermittlungsbehörden waren und das vor allen Dingen der Austausch der Informationen das Problem war und das man jetzt mit dieser Datenbank schaffen wird, nämlich 27 solcher Silos in den Mitgliedstaaten der Europäischen Union, die dann die Daten miteinander tauschen zu wollen. Das wird dazu führen, dass genau dieses Problem, was wir aus der Vergangenheit kennen, noch weiter verschärft wird und daher ist eben aus verschiedenen Gründen dieses Gesetz für mich anlasslos und verdachtsunabhängig. Es ist nicht angemessen, es ist nicht verhältnismäßig und verstößt gegen europäische und deutsche Grundrechte. Danke.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Sander. Dann schwenken wir nun auf meine andere Seite. Herr Münch, Präsident des BKA, Sie haben das Wort.

SV **Präsident Holger Münch** (Bundeskriminalamt, Wiesbaden): Vielen Dank Herr Vorsitzender, meine Damen und Herren. Ich glaube nachdem, was Herr Sander gesagt hat, konzentriere ich mich auf die Umsetzungsfragen, um vielleicht das eine oder andere hier auch schon mal anzusprechen, wie wir uns das auch in der weiteren Ausgestaltung vorstellen. Zunächst einmal wird der termingerechte Aufbau des Fluggastdaten-Informationssystems uns hier in Deutschland vor eine große Herausforderung stellen und auch in allen anderen EU-Mitgliedstaaten ist das so, aber gleichzeitig auch eine Chance bieten, einen fachlichen Mehrwert bieten. Wir sehen hier schon die Chance, dass das Instrumentarium der kriminalpolizeilichen Auswertung einen weiteren Beitrag zu einer Verbesserung der Sicherheitslage in

Deutschland leisten kann. Es ist kein Allheilmittel, aber es kann einen Beitrag leisten.

Das zeigen auch die Erfahrungen anderer Staaten, wie Australien, USA und Großbritannien, die bereits über etablierte Systeme verfügen und so konnten in Ländern, die solche Systeme haben, Terrorverdächtige schon vor der Einreise im jeweiligen Abflugland identifiziert werden oder aber in den Dschihad ausreisende Teenager werden rechtzeitig vor ihrer Ausreise nach Syrien erkannt und daran gehindert und den Sorgeberechtigten übergeben. Auch in anderen Deliktbereichen, wie zum Beispiel dem international organisierten Rauschgiftschmuggel, sind die Erfahrungen der Länder durchaus positiv und auch aus Sicht von Deutschland als vielversprechend zu bewerten.

Die Einbeziehung der Intra-Schengenflüge in das Fluggastdatengesetz ist aus unserer Sicht sinnvoll und auch notwendig. Erfahrungen, insbesondere aus dem Phänomenbereich des islamistischen Terrorismus haben gezeigt, dass sich islamistische Gefährder sehr wohl des Schengenraums und seiner Herausforderung für die Sicherheitsbehörden bewusst sind. Und so werden Ein- und Ausreisen nach bzw. aus Europa über den Luftweg zur Umgehung nationaler Sicherheitsmaßnahmen einfach aus einem anderen europäischen Mitgliedstaat heraus angetreten und die hierfür genutzten Intra-Schengentransitflüge bleiben dann mangels fehlender Grenzkontrollen unerkannt.

Gleiches gilt natürlich auch für zur Fahndung ausgeschriebene Straftäter. Die Nutzung von Fluggastdaten, auch für Intra-Schengenflüge, stellt daher eigentlich dieses Element dar, soweit Abgleichstreffer einen Katalogtatenbezug aufweisen, das ist ja immer dann auch die Bedingung.

Die Verarbeitung von Fluggastdaten erfordert auf der einen Seite strenge Vorgaben für den Datenschutz und die Datensicherheit und auf der anderen Seite ist es eine hohe Anforderung an die Verarbeitungsgeschwindigkeit, denn das Verfahren muss ja in Echtzeit funktionieren. Für die Verarbeitung der Daten wird das BKA als nationale Fluggastdatenzentralstelle zuständig sein. Und hierzu wird das BKA ein Fluggastdaten-Informationssystem nach Maßgabe des Fluggastdatengesetzes unterhalten. Unter engen rechtlichen Voraussetzungen dürfen die von den Luftfahrtunternehmen übermittelten Daten auf dreierlei Weise genutzt werden. Erstens können mit den Datenbeständen Fahndungen oder zur Ausschreibung stehende Personen oder Sachen abgeglichen werden. Wir werden uns auf den Abgleich mit den Datenbeständen des Schengener Informationssystems als europäischem Fahndungssystem und von INPOL-zentral als nationalem Auskunfts- und Fahndungssystem konzentrieren. Andere Systeme werden wir zurzeit nicht andenken, auch weil wir die Zahl der Falsch-Positivtreffer dafür auch zu hoch halten. Beispiel: Stolen and Lost Travel Documents von Interpol, wo viele abhanden gekommene Dokumente gespeichert sind, die aber dann später von den rechtmäßigen Benutzern wiedergefunden werden und weil wir das wissen, werden wir das nicht tun.

Zweitens besteht die Möglichkeit, die Fluggastdaten mit sogenannten Mustern abzugleichen, um so Personen zu identifizieren, die im Zusammenhang mit terroristischen Straftaten oder einer Straftat der schweren Kriminalität stehen könnten, aber den Behörden bislang nicht namentlich bekannt sind.

Die aus dem Abgleich resultierenden Treffer können stets nach einer technischen und individuellen Trefferverifikation unter den engen Voraussetzungen des § 6 des Fluggastdatengesetzentwurfs an das BKA von der Zentralstelle selbst oder an die LKÄ, Zollverwaltung, Bundespolizei übermittelt werden. Und darüber hinaus ist auch eine Übermittlung an das BfV, die Verfassungsschutzbehörden der Länder, den MAD oder den Bundesnachrichtendienst grundsätzlich möglich, soweit das zur Erfüllung von deren Aufgaben im Zusammenhang mit den Katalogtaten, die im Fluggastdatengesetz aufgeführt sind, erforderlich ist.

Und drittens können die genannten berechtigten Stellen Anfragen an die Fluggastdaten-Zentralstelle zur Recherche stellen. Es wird also nicht so sein, dass andere Dienststellen Zugriff haben, so wie das in den USA ist, sondern die Recherche wird nur durch die Fluggastdaten-Zentralstelle gestellt und die prüft zunächst den Katalogtatenbezug und führt dann die Recherche selbst durch. Das gilt im Übrigen auch für Mitarbeiter des BKA, die das nicht selbst machen können, sondern nur Mitarbeiter der Fluggastdaten-Zentralstelle.

Unter engen Voraussetzungen ist noch ein Datenaustausch mit den Fluggastdaten-Zentralstellen anderer EU-Mitgliedstaaten und Europol möglich. Und ebenso dann unter Beachtung der Vorgaben des Bundesdatenschutzgesetzes, auch des Entwurfs zum veränderten Bundesdatenschutzgesetz, bei den zur Verhütung und Verfolgung von terroristischen Straftaten zuständigen Behörden von Drittstaaten. Technisch soll aus datenschutzrechtlichen Gründen die Erhebung und Speicherung der Fluggastdaten getrennt werden von der polizeilichen Verarbeitung und außerhalb des BKA erfolgen. Die technische Realisierung wird im Bundesverwaltungsamt angesiedelt, das die Fluggastdaten im Auftrag des BKA verarbeitet. Das Bundesverwaltungsamt nimmt die Fluggastdaten von den Luftfahrtunternehmen entgegen und stellt auch die Betreuung der Fluggesellschaften sicher. Erst im Falle eines technischen Treffers wird ein Vorgang mit den relevanten Daten durch das Bundesverwaltungsamt an die Fluggastdaten-Zentralstelle im BKA übermittelt. Hierdurch soll sichergestellt werden, dass nur solche Treffer zur Person angezeigt werden, die auch eine gewisse Relevanz haben. Das bedeutet, in der Fluggastdaten-Zentralstelle sollen über 99 Prozent der Daten nicht ankommen.

Und dann kommt der zweite Filter: die Trefferverifikation, die dann zu dem Wert führen soll, den Sie schon genannt haben, also dass dann auch weitere, nur technische Treffer aussortiert werden. Dieser automatisierte Abgleich mit Ausschreibung zur Fahndung ist in Deutschland, so glauben wir, technisch gut umsetzbar. In Europa wird es etwas schwieriger, weil das Schengener Informationssystem die Fahndungskategorien nicht hinterlegt. Hier sind wir auch mit anderen europäischen Staaten im Gespräch, wie wir das realisieren ohne einen zusätzlichen Aufwand, um auch noch hier eindeutig den Katalogtatenbezug nachzuweisen.

Die technische Anbindung der Luftfahrtunternehmen wird ab dem Zeitpunkt des Inkrafttretens des Gesetzes schrittweise erfolgen, das halten wir für wichtig, weil wir zunächst die Prozesse einüben müssen. Unser Ziel ist es, an einem Flughafen mit einer Fluggesellschaft zu beginnen und dann schrittweise auszubauen, beginnend mit dem Thema „Fahndung“ und dann weiter aufbauend das Thema „Muster“, weil wir es für wichtig halten, zunächst jetzt einmal die Prozesse auch in Zusammenarbeit mit den Sicherheitsbehörden eingeübt zu haben, bevor wir dann schrittweise weiter ausbauen. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Münch. Dann erhält nun das Wort Herr Knetsch von der Lufthansa Group.

SV **Matthias Knetsch** (Lufthansa Group and Government Services bei SITA, Eschborn): Sehr geehrter Herr Vorsitzender Heveling, sehr geehrte Damen und Herren. Ich möchte mich zunächst bedanken für die Einladung als Sachverständiger zum Thema „Fluggastdaten“ und für die damit verbundene Möglichkeit, aus Sicht und Erfahrung der SITA in diesem Hohen Haus zum Thema Auskunft geben zu dürfen.

Eine kleine Korrektur noch zu meiner Person. Ich bin nicht von der Lufthansa sondern von der SITA und dort verantwortlich für den Geschäftsbereich der Lufthansa Group und Regierungsgeschäfte.

Meine Ausführungen sollen zunächst Auskunft geben über die Erfahrung beim Aufbau und Betrieb von Fluggastdaten in anderen Ländern, wie sie dort betrieben und aufgebaut wurden. Bitte erlauben Sie mir, dass ich kurz einige Worte zur SITA selber verliere, um ihre besondere Rolle in der Datenkommunikation in der Luftfahrtindustrie sowie bei den Grenzsicherungssystemen zu verdeutlichen. SITA ist außerhalb der Luftfahrtindustrie eher wenig bekannt. SITA wurde vor über 60 Jahren von Fluglinien gegründet, um deren Daten weltweit mit deren Geschäftspartnern auszutauschen. Über die Jahre ist die Anzahl der Fluglinien, welche auch die Eigentümer der SITA sind, auf über 500 gewachsen. SITA ist zum Teil genossenschaftlich organisiert und wird auch von anderen internationalen Organisationen, wie den Vereinten Nationen, der WHO oder der Weltbank, für deren Datenkommunikation genutzt. Seit über 20 Jahren entwickelt SITA Risikoanalysesysteme für Regierungen zur Verbesserung der Grenzsicherheit, elektronische Reiseinformations- und -genehmigungssysteme und hat damals das erste interaktive API-System, also Passdatensystem, aufgebaut. Heute sind wir in über 40 Ländern an Grenzsicherheitslösungen beteiligt, die unter anderem PNR- und API-Daten nutzen. Im April 2016 wurde die EU-Richtlinie zum Fluggastdatengesetz verabschiedet. Die Zweijahresfrist zur

Umsetzung in nationales Recht sowie den Systemaufbau hat damit bereits begonnen und wird mit dem vorliegenden Gesetzgebungsverfahren angestrebt.

Ein sorgfältiges Gesamtdesign des Projekts ist absolut notwendig, um ein gemeinsames Verständnis unter allen Beteiligten an dem System zu schaffen. Die technische Lösung ist auf die neuen Geschäftsprozesse anzupassen und nicht umgekehrt. Alle Nutzer des Systems sollen in diesem Prozess frühzeitig und regelmäßig einbezogen werden, sodass die Erwartungen und die Anforderungen entsprechend abgestimmt werden. Nachträgliche Änderungen am System sind extrem kostspielig und werden das Projekt verzögern. Der Erfolg eines Passagierdatensystems hängt maßgeblich von der Qualität der Passagierdaten ab. Wie zu Recht in der Begründung des Gesetzentwurfs bereits auch angemerkt wurde. Trotz aller Bemühungen um Standardisierung kann nicht von einem reibungslosen und einfachen Datenaustausch ausgegangen werden. So betreiben einige Fluggesellschaften immer noch sehr alte Reservierungssysteme und es können bei weitem noch nicht alle Fluglinien den sogenannten PNRGOV-Standard umsetzen oder benutzen dabei verschiedene Versionen oder Varianten. Das wird sich auch nicht in aller Kürze ändern lassen. Die Sicherstellung von qualitativen Datenlieferungen bzw. das Auffinden von Ursachen schlechter Datenqualität ist komplex und erfordert die Schaffung eines sogenannten Carrier Engagement Teams. Das sind die Ansprechpartner von Seiten der Regierung, welche aktiv mit den Fluggesellschaften zusammenarbeiten. Dies erfordert Kenntnisse und Erfahrungen mit den Systemen der Fluggesellschaften, auch auf Seiten der Regierung. Kollaborative Zusammenarbeit mit den Fluglinien und den Nutzern ist ein fortwährender Prozess über die gesamte Laufzeit und von immenser Wichtigkeit. Das wird oft unterschätzt. Technische Spezifikationsbeschreibungen sollten für die Fluglinien frühzeitig erstellt werden, um die Anforderungen der Regierungen eindeutig und umfassend zu beschreiben, damit die Fluglinien sich entsprechend rechtzeitig darauf einstellen können.

Unumgänglich bleibt eine Test- und Zertifizierungsphase mit den einzelnen Fluglinien, bevor die Daten in das Produktivsystem übernommen werden. Auch wenn Fluglinien bereits Daten im PNRGOV-Format senden, so ist trotzdem, wenn auch eine abgespeckte Zertifizierung, notwendig. Ein Pilotprojekt ist aus technischer und operationeller Sicht empfehlenswert und bietet die Möglichkeit, in kleinem Umfang das System, die Daten und den damit verbundenen Umgang zu testen, zu validieren und zu trainieren. Eine überschaubare Menge an Fluglinien, die Grundfunktionalität des Systems und daraus resultierend eine kleine Menge an Fällen, die zu bearbeiten sind, ermöglichen es, vorab und vor allem rechtzeitig Änderungen oder Tuningmaßnahmen durchzuführen.

In diesem Zusammenhang möchte ich auf den Gesetzesänderungsantrag kurz eingehen. Das Inkrafttreten des Gesetzes soll wie folgt geändert werden: Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach der Verkündung in Kraft. Also im Sommer 2017. Das schnellere Inkrafttreten des Gesetzes dient sicherlich dazu, die rechtliche Absicherung der technischen Testphase sicherzustellen. Und das ist auch sinnvoll. Jedoch auch, wenn für einen Verstoß gegen Datenübermittlungspflichten keine Sanktionen drohen, kann dies ein rechtliches Obligo der Fluglinien für eine Datenübermittlung schon in zwei bis drei Monaten bedeuten. Dies kann eine formale Rechtswidrigkeit im Falle der Nichtlieferung der Daten, Rechtfertigungszwang sowie Haftungskriterien bedeuten. Ich würde mir wünschen, dass dieser Punkt nochmal kritisch hinterfragt wird.

Es gilt zu berücksichtigen, dass nicht nur Deutschland, sondern auch die meisten anderen europäischen Mitgliedstaaten eine Umsetzung und Inbetriebnahme ihres jeweiligen Passagierdatensystems bis Mai 2018 anstreben. Somit sind Engpässe bei der Umsetzung der jeweiligen Regierungsanforderungen auf Seiten der Fluglinien zu erwarten. Jeder Mitgliedstaat muss mit jeder Fluglinie den Test- und Zertifizierungsprozess durchlaufen. Im Fall von Deutschland sind das also circa 150 Fluglinien, zumindest in weiterer Ausbaustufe, die es zu testen gilt, die parallel dazu auch von anderen Staaten bedient werden müssen. Unserer Erfahrung nach ist von circa 12 bis 24 Monaten für die technische Implementierung auszugehen. Es hängt jedoch sehr stark davon ab, inwieweit auf eigene Inhouse-Entwicklungen oder die Beschaffung von bereits bestehenden

Teilkomponenten von erfahrenen Zulieferern unter dem Aspekt „Sicherheit, Kosten und Zeit“ zurückgegriffen wird.

Zusammenfassend empfehlen wir, Risiken des Projektes von Anfang an bestmöglich zu minimieren, damit das System effektiv zur Bekämpfung von Terrorismus und schwerer Kriminalität beitragen kann und dennoch nicht aus dem zeitlichen und finanziellen Rahmen läuft. Berücksichtigung von Erfahrungen und Praxisbeispielen anderer Länder ist hier hilfreich. Enge Kooperation mit allen beteiligten Nutzern des Systems, also den Organisationen BKA, BPOL, Zoll usw. zur Erstellung eines nutzerorientierten effektiven Systems und die partnerschaftliche Zusammenarbeit mit den Fluglinien, den Lieferanten der Daten, um möglichst schnell und fortlaufend qualitativ hochwertige Daten zu erhalten. Die Einhaltung der etablierten Standards ist absolut wichtig für die Luftfahrtbranche. Die Durchführung eines Pilotprojektes zur Erprobung der technischen Lösung, aber vor allem die Einübung und Vereinfachung der neuen organisatorischen Prozesse zur Nutzung dieses neuen Instruments für Deutschland zur Bekämpfung von Terrorismus und schwerer Kriminalität. Vielen Dank für Ihre Aufmerksamkeit.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Knetsch. Und nun last but not least, zeitgerecht eingetroffen, ich hoffe, Sie haben einmal durchatmen können, Herr Prof. Dr. Arzt, Sie haben jetzt das Wort für Ihre fünfminütige Eingangsstellungnahme.

SV **Prof. Dr. Clemens Arzt** (Hochschule für Wirtschaft und Recht Berlin): Ganz herzlichen Dank. Ich muss mich hier vielmals entschuldigen. Seit vielen Wochen steht dieser Termin am 26.04. in meinem Kalender und ich habe mich gewundert, warum er zeitglich mit einer Einladung der CDU stattfindet, bis ich heute gegen 15.45 Uhr von Herrn Leopold gehört habe, dass der Termin jetzt ist. Glücklicherweise war meine Stellungnahme zwei Minuten vorher fertig und ich habe sie Ihnen auch bereits übersandt um 16.02 Uhr. Also da bitte ich nochmal um Nachsicht.

Worum geht es in diesem Gesetzentwurf? Zunächst, ich denke, das dürfte hinreichend klar sein, haben wir eine massive Erfassung von rund 170 Millionen Passagieren pro Jahr, die hier erfasst werden mit ihren Fluggastdaten. Das heißt in fünf Jahren, wenn wir einfach mal den Löschungszeitraum des § 13 ansetzen, haben wir bereits 850 Millionen Fluggastdatensätze gespeichert, die dem BKA dann zur Mustererkennung zur Verfügung stehen. Ob man dieses Gesetz zu diesem Zeitpunkt einführen sollte, abgesehen davon, dass man es nach meiner Sicht nicht einführen sollte, da muss man ein klares Fragezeichen machen mit Blick darauf, dass wir alle wissen, dass beim EuGH derzeit ein Verfahren anhängig ist, wo es um das PNR-Abkommen mit Kanada geht. Hier gibt es ein Gutachten des Generalanwaltes Paolo Mengozzi, der einige Fragezeichen in den Raum stellt. Es gibt aber dazu natürlich auch noch verfassungsrechtliche Gesichtspunkte aus deutscher Sicht.

Wenn wir mal kurz darüber nachdenken, wozu soll dieses Mittel dienen, dann haben wir dort nicht nur die Verfolgung von Straftaten, sondern auch deren Verhütung. Verhütung von Straftaten ist ein gängiges Instrument der Gefahrenabwehr im Polizeirecht. Der große Unterschied besteht allerdings darin, dass wir hier nicht irgendwo an einem Zusatz, sozusagen an Erkenntnissen ansetzen, wie an einem gefährlichen Ort oder ähnliches, wo die Polizei relativ beliebig jeden einer Identitätsfeststellung unterziehen darf, sondern alleine der Umstand, dass ich ein Flugzeug nutze, bringt mich entsprechend in die Datei und gestattet es dem Bundeskriminalamt und vielen vielen anderen Behörden, an die ja noch relativ frei übermittelt werden darf – es gibt Datenaustausch bis hin zu den Nachrichtendiensten im Ausland, nicht nur ins EU-Ausland. All dieses kann zur nicht näher definierten Verhütung von Straftaten gerastert werden. Man kann natürlich schauen, dass man in § 4 einige Straftaten aufgezählt hat, aber wenn wir über die Verhütung von Straftaten als Teil der Gefahrenabwehr sprechen, müssen wir natürlich auch immer darüber sprechen, dass es irgendwelche Wahrscheinlichkeitsgrade braucht und diese Wahrscheinlichkeitsgrade werden im Gesetz an keiner Stelle näher benannt, durchgängig. Die Polizei bekommt hier einen absoluten Freibrief mit dieser Maßnahme.

Abgesehen davon, dass es changiert, ob die Maßnahme der Bekämpfung des Terrorismus oder des internationalen Terrorismus dienen soll, auch das durchaus ein rechtlicher Unterschied. Da haben wir noch ein ziemliches

Bestimmtheitsproblem mit der Idee der schweren Kriminalität, die so zunächst mal, aus meiner Sicht, nicht so einfach zu verorten ist. Also die Maßnahme dient letztendlich einer anlasslosen Verdachts- und Verdächtigengewinnung gegen jede Person, die sich in Europa mit dem Flugzeug bewegt. Hier gehen wir auch gleich deutlich weiter als es unbedingt von der Richtlinie gefordert wird. Also wir erfassen nicht nur Flüge in Drittstaaten, sondern wir erfassen alle Flüge außerhalb Deutschlands.

Wir haben also letztendlich sozusagen eine Anschlussmaßnahme zur TK-Vorratsdatenspeicherung, die allerdings einen deutlich anderen Ansatz vertritt. In der TK-Vorratsdatenspeicherung, die ja durchaus verfassungsrechtlich, wie wir wissen, umstritten ist, vom EuGH gerade jüngst wiederrum beanstandet wurde, dennoch haben wir zumindest in der deutschen Ausformung der TK-Vorratsdatenspeicherung den konkreten Anlass, warum vorratsgespeicherte Daten von der Polizei im Einzelfall abgerufen werden können. Hier tun wir das Gegenteil, hier erheben wir nochmal alleine, weil ein Mensch vom Flugverkehr Gebrauch macht, dessen Daten und können diese Daten nach Mustern des BKA, die alleine das BKA zu verantworten hat, es also selbst ein Verdachtsmuster festlegen kann, dann entsprechend im breiten Raum rastern. Wir haben also eine völlig neue Dimension anlassloser Massenüberwachung, die hier eingeführt wird.

Wir haben eine Fülle in § 2 Absatz 3, eine Fülle von Daten dann, aber wir wissen eigentlich gar nicht, warum werden hier immerhin 20 Kategorien von unterschiedlichen Daten festgelegt. Also in welchem Bezug sollen jeweils diese Daten eigentlich zu der Zielsetzung aus § 1 Absatz 2 stehen? Das wird im Gesetz nicht weiter dargelegt und dazu haben wir noch ein Freitext-Feld in Nummer 16. Hier können Hinweise gespeichert werden, also „Hinweise“ ist nun in keiner Art und Weise mehr gesetzlich geregelt, was eigentlich hier gespeichert werden darf.

Wenn das Gesetz von dem Begriff in § 4, vom Begriff der Datenverarbeitung ausgeht, haben wir ein weiteres Novum, was sich natürlich ein Stück weit einreiht in die jetzige Novelle des Datenschutzrechtes und des BKA-Gesetzes. Während wir also früher ausgehend von der Volkszählungsentscheidung des Bundesverfassungsgerichts eine klare dezidierte Unterscheidung der verschiedenen Stufen und Etappen oder Formen der Datenverarbeitung hatten, ist diese Idee komplett aufgehoben. Dem BKA wird die Befugnis zur Datenverarbeitung gegeben, das heißt: Erheben, Erfassen, Organisation, Orten, Speichern, Anpassen, Verändern, Auslesen, Abfragen und so weiter und so fort. Also der Gesetzgeber hat komplett darauf verzichtet, normisch, spezifisch normenklar zu regeln, welche Varianten der Datenverarbeitung dem BKA hier zukommen sollen. Wir haben also faktisch, wenn wir dann weitergehen und uns diese Idee der Mustererkennung anschauen, eine neue Form der Rasterfahndung. Gerastert werden kann jeder anlässlich seiner Nutzung eines Fluges innerhalb Europas und darüber hinaus.

Schauen wir uns die Rechtsprechung des Bundesverfassungsgerichts zur Rasterfahndung an, sehen wir, dass die Anforderungen dort deutlich höher sind als hier im Gesetz. Eine Rasterfahndung ist nach der Entscheidung des Bundesverfassungsgerichtes zulässig zur Abwehr konkreter Gefahren für hochrangige Rechtsgüter. Achtung: konkrete Gefahren für hochrangige Rechtsgüter – auch wenn der Terrorismus sicherlich hochrangige Rechtsgüter gefährdet, fehlt es komplett an der konkreten Gefahr, es fehlt komplett an jeglicher Wahrscheinlichkeitsdefinition des Gesetzgebers. Er legt nirgendwo den Maßstab der Wahrscheinlichkeit in irgendeiner Art fest.

Wir werden daraus sicherlich, genau wie wir das bei der TK-Vorratsdatenspeicherung diskutiert haben, eine neue Form von Einschüchterung haben. Jeder weiß in Zukunft, dass seine Daten, wenn er sich irgendwo innerhalb Europas oder außerhalb Europas mit dem Flugzeug bewegt, für fünf Jahre gespeichert werden. Also das BKA hat über jede Flugbewegung, über jeden Fluggast für fünf Jahre die Daten über diese Flugbewegung – das erscheint mir verfassungsrechtlich in keiner Weise hinnehmbar und es ist natürlich und erst recht – ich versuche schnell zum Ende zu kommen, ich konnte mich jetzt leider nicht mehr vorbereiten auf die Hauptpunkte – es ist erst recht nicht vereinbar mit der Rechtsprechung des EuGH zur Vorratsdatenspeicherung. Also hier haben wir einen ganz klaren Bruch.

Lassen Sie mich ganz kurz hier durchblättern. Vielleicht ganz kurz zu § 5, zur sogenannten Depersonalisierung. Die Depersonalisierung verlässt die alte Idee von Anonymisierung und Pseudonymisierung. Also wir führen etwas Neues ein. Was es da an Schutzrecht nicht kennt. Nirgendwo dort werden Sie Depersonalisierung finden und diese Depersonalisierung kann jederzeit im Grunde aufgehoben werden. Dafür braucht es eine gerichtliche Entscheidung oder entsprechend eine „Gefahr im Verzug“, ohne dass die Maßstäbe, was „Gefahr im Verzug“ darstellt, sehr klar wären.

Letzter Punkt. Wir haben eine komplette Durchbrechung der Idee eines, früher Mal Trennungsgebotes oder auch nur der informationellen Trennung; die nimmt natürlich ihren Ausgang in der Antiterrordatei und im BKAG. Dennoch geht es hier aus meiner Sicht deutlich weiter, weil nunmehr beliebig ohne konkreten Bezug zu bestimmten Menschen Daten mit den Nachrichtendiensten frei gehandelt werden können und darüber hinaus auch noch ans Ausland und viele andere Dienste gegeben werden können. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Prof. Dr. Arzt. Wir kämen dann zur Runde der Fraktionen. Zunächst die CDU/CSU-Fraktion. Herr Kollege Schuster, bitte.

BE Abg. **Armin Schuster** (Weil am Rhein) (CDU/CSU): Vielen Dank die Herren Sachverständigen für Ihre Beiträge. Ich richte meine Fragen direkt an den Einzelsachverständigen Herr Prof. Dr. Wollenschläger. Handelt es sich um eine anlasslose Massenüberwachung oder habe ich Sie falsch verstanden, denn die Spannbreite der Meinungen war ja jetzt doch sehr groß? Sie hatte ich jetzt so verstanden, als dass der Entwurf dieses Gesetzes die EU-Richtlinie rechtlich vollständig und auch verfassungsgemäß umsetzt. Wie stehen Sie dann zu diesem Begriff „anlasslose Massenüberwachung“, die der Kollege von Ihnen, Prof. Dr. Arzt, jetzt gerade eben benannt hat? Und was mich interessieren würde ist: Das Niveau an Datenschutz und Datensicherheit in diesen beiden Gesetzen, BDSG und dann BKAG im Entwurf, ist das Niveau für Sie angemessen und verfassungsgemäß?

Frage an den BKA-Präsidenten Herrn Münch: Haben Sie einen Freibrief bekommen? Das habe ich gerade eben gelernt. Da wollte ich nochmal nachfragen, ob Sie einen polizeilichen Freibrief für alles bekommen haben? Und in dem Zusammenhang würde mich interessieren, Sie haben es jetzt sehr vage gesagt, es gibt ja Länder, die haben Erfahrungen gesammelt. Können Sie das näher sagen? Zu den Fallkonstellationen, zu konkreten Fallkonstellationen, um mal den Mehrwert fassbarer zu machen. Wir sprechen immer von terroristischen Gefahren usw. Aber ich glaube, man kann es vielleicht etwas präzisieren.

Und an den Herrn Knetsch habe ich die Frage: Sie haben jetzt sehr vornehm, glaube ich, etwas darum herum geredet, so habe ich es jedenfalls verstanden, dass wir unter enormem Zeitdruck leiden könnten, also das ist aber jetzt meine Deutung. Ich habe versucht, zwischen Ihren Zeilen zu lesen. Sie dürfen uns hier schon richtig sagen, weil Sie nämlich derjenige sind, der die Erfahrungen aus den anderen Ländern hat, die ja schon solche Dinge umgesetzt haben, was Methodik und Zeitansätze anbelangt. Womit müssen wir rechnen in Deutschland? Haben wir Zeit, haben wir Zeitdruck? Was sagen Ihnen jetzt konkret Ihre Erfahrungen aus den Ländern, die es schon geschafft haben? Und Sie haben auch darüber gesprochen, dass es problematisch werden könnte mit der Datenqualität der Fluggesellschaften, das würde mich auch noch mal interessieren. Wenn Sie das präzisieren könnten.

Eine Frage noch Herr Münch – Verstoß gegen das Trennungsgebot, das war jetzt auch gerade im Raum. Können Sie nochmal sagen, mit welchen rechtlichen Grundlagen und mit welchen praktischen Mechanismen diese Behörden versorgt werden, die nicht BKA sind? Und wie wird da das Trennungsgebot einhalten?

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Kollege Schuster. Frau Kollegin Renner, bitte.

BE Abg. **Martina Renner** (DIE LINKE.): Danke auch von mir an die Anzuhörenden. Ich würde gerne diese Frage nach der Effizienz der Systeme in den Ländern, wo entsprechend die Fluggastdaten schon erfasst werden, präzisieren. Herr Münch, Sie sprachen davon, es seien dort zum Beispiel Foreign Fighters an der Ausreise gehindert worden. Können Sie einfach mal schildern, in welchem Land das war, wann und ob das tatsächlich mit den Fluggastdaten zusammenhing oder ob es nicht

vielleicht sonstige Maßnahmen gab, unter denen diese Personen in den Blick geraten waren.

Diese Frage nach der Evaluation der Effizienz würde ich aber ganz gerne auch an Herrn Prof. Dr. Arzt richten. Ob Ihnen Untersuchungen, Erkenntnisse bekannt sind, inwieweit tatsächlich diese Systeme zur Gefahrenabwehr geeignet sind oder ob wir uns im Bereich der Kolportage bewegen?

Herr Münch würde von mir noch die Frage bekommen: 170 Millionen Fluggastdaten. Gehen wir davon aus, dass vielleicht bei einem Promille das System anschlägt. Das heißt, 170 Tausend Datensätze, die von 200 Mitarbeitern ausgewertet werden – ist das realistisch oder müssen wir erwarten, dass in den nächsten Haushaltsberatungen dort nachgefordert wird? Und wenn wir uns auch nochmal gerade die Fälle der letzten Terroranschläge und Terrorvorbereitungen anschauen, da meine ich auch insbesondere nicht nur den Fall „Amri“, sondern den Fall des Rechtsterrors, müsste die Personalentwicklung im BKA nicht in eine ganz andere Richtung gehen, als Leute, die Datensätze auswerten?

Herrn Sander würde ich gerne fragen: Sie haben ja eben diese Problematik des Freitext-Feldes sehr stark auch nochmal in Ihrer mündlichen Stellungnahme hervorgehoben. Wie würden Sie denn die Datenschutzproblematik dort einordnen? Es geht um 170 Millionen möglicherweise Freitext-Felder, die mit irgendwas beschrieben werden. Wer soll das denn prüfen?

Und an Sie auch meine letzte Frage: Es wird ja von den Befürwortern des PNR-Systems oft gesagt: Im Gegensatz zu einem Grenzbeamten, einer Grenzbeamtin, die möglicherweise subjektiv und auch vorurteilsbeladen/-belastet agiert, sei dieses System objektiv. Also zum Beispiel so etwas wie Racial Profiling käme da nicht vor. Ist das denn bei Algorithmen ausgeschlossen? Können Algorithmen auch Vorurteile transportieren? Das wäre meine abschließende Frage an Sie. Danke.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Frau Kollegin Renner. Herr Kollege Gunkel, bitte.

BE Abg. **Wolfgang Gunkel** (SPD): Schönen Dank an die Herren Sachverständigen. Für mich kommt nochmal der Blick auf das dazu, was wir bereits diskutiert haben in der 1. Lesung des Bundestages. Hier sind einige Eckpunkte genannt worden. Da der Herr Prof. Dr. Schwarz nicht da ist, muss ich meine Fragen jetzt so ein bisschen verteilen auf die anderen Herren.

Ich frage nochmal dazu nach, wie es mit den datenschutzrechtlichen Kontrollen aussieht, insbesondere im Hinblick auf die Weitergabe der Daten an Drittstaaten. Das hatte mich seiner Zeit schon bewegt. Herr Sander, Sie haben dazu schon anfänglich eine Aussage gemacht. Wie würden Sie das bewerten, ist die Kontrolle da in hinreichendem Maße durch das Gesetz, durch das Gesetzesvorhaben gewährleistet?

Ein weiterer größerer Komplex geht an Herrn Münch. Herr Münch, Sie haben vorhin erwähnt, dass die Zusammenarbeit zwischen den Behörden von großer Wichtigkeit ist und wir haben inzwischen gehört, dass da riesen Datensätze zu bewältigen sind. Und im Zusammenhang ist auch bekannt, dass die Bundespolizei mit den API-Daten bereits Erfahrungen hat, indem seit 2006 dort schon Kontrolldaten aus den Flugdaten herausgelesen werden und die entsprechend auch bearbeitet werden, und auch im Ordnungswidrigkeitenverfahren spricht die Bundespolizei dort Ordnungsgelder aus. Wäre es nicht besser gewesen, diese Aufgabe der Bundespolizei zu übertragen, anstatt mit dem Bundesverwaltungsamt eine weitere neue Behörde zu befassen, die damit keinerlei Erfahrung hat? Das Gleiche kann ich indirekt an Herrn Knetsch vielleicht auch fragen, der besonders abgehoben hat auf die enge Zusammenarbeit zwischen den Beteiligten, auch bei der Schwierigkeit der Datenübermittlung.

Dazu gleich das nächste, Herr Münch. Könnten Sie sich vorstellen, dass es bei diesen Datenübermittlungen zu Sicherheitslücken kommt und wie glauben Sie könne man diese Sicherheitslücken vermeiden?

Dann habe ich noch eine Frage, die zielt jetzt auf die anderweitigen Daten, die einbezogen werden sollen. Auf EU-Ebene haben wir ja schon die unterschiedlichsten Datenerhebungen. Sie sprachen das an – SIS II und INPOL national. Sie wissen auch, dass die Mitgliedstaaten gerade das SIS II nur unzureichend pflegen. Dadurch kommt es immer wieder zu Fahndungsnebentreffern, das heißt, man trifft nicht richtig, wenn nicht alle Staaten sich intensiv um die Pflege der Daten

bemühen. Sehen Sie ein ähnliches Schicksal für die PNR-Daten?

Und als letztes vielleicht. Sie haben auch schon – und die anderen Kollegen äquivalent – in Ihrem schriftlichen Bericht auf die Erfolge der PNR-Systeme in anderen Staaten hingewiesen: in Australien, Großbritannien, in den USA. Da würde mich interessieren, wie viele Treffer gab es da konkret und haben denn Vorgehen zu einer Verhaftung und zur Verhinderung von Straftaten oder ähnlichem geführt?

So, zum Schluss habe ich dann noch eine weitere Frage und zwar die Speicherdauer der PNR-Daten, die ja auf sechs Monate bis zum Bereich der Aufdeckung möglich sind und auf fünf Jahre generell. Dazu hätte ich Herrn Sander gerne nochmal gehört, wie er das sieht. Ob das so erforderlich ist oder ob das nicht etwas übers Ziel hinausschießt? Dankeschön.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Kollege Gunkel. Frau Kollegin Mihalic, bitte.

Abg. **Irene Mihalic** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank Herr Vorsitzender. Auch von meiner Seite herzlichen Dank an die Herren Sachverständigen. Ich habe zunächst zwei Fragen an Herrn Arzt. Sie haben ja schon und auch andere Sachverständige haben ja auf das anhängige Verfahren beim EuGH hingewiesen und auf die Probleme, die damit möglicherweise verbunden sind und auch Sie haben vorhin gesagt, dass es durchaus sein kann, dass eben auch das PNR-Abkommen zwischen der EU und Kanada für europarechtswidrig eingestuft wird. Und deswegen möchte ich Sie zunächst fragen, wie Sie die Möglichkeit einschätzen, dass die Richtlinie und insbesondere der Abgleich aller Passagierdaten mit sogenannten Mustern für europarechtswidrig erklärt wird.

Und meine zweite Frage ist, wie Sie die Folgen für den Fall abschätzen, dass die Fluggastdatenbank, wenn wir mal davon ausgehen, sie wird europa- und grundrechtswidrig errichtet, erst mal alle Daten sammelt. Also die Frage nach den Folgen einer solchen Datensammlung in einer europa- und grundrechtswidrigen Fluggastdatenbank wären für mich nochmal wichtig zu erfahren.

Dann habe ich noch eine Frage an Herrn Sander. Wie schätzen Sie die Eingriffsschwelle ein in Bezug auf den Abgleich der Daten unverdächtiger Personen eben mit sogenannten Mustern? Also, auch wenn wir mal davon ausgehen, so wie es die Bundesregierung auch in ihrem Gesetzentwurf schreibt, dass sie von einer Trefferquote von 0,1 Prozent ausgeht bei dem Abgleich der Daten Unverdächtiger, was ja einer faktischen Rasterfahndung entspricht. Ist da aus Ihrer Sicht die Eingriffsschwelle hinreichend genug, und ich will das nur nochmal vom Problem her eingrenzen, damit Sie da auch gezielt Stellung zu nehmen können. Es handelt sich dabei um eine Maßnahme der Verdachtsgenerierung. Also es werden ja keine Daten von bereits verdächtigen Personen abgeglichen oder auch aufgrund von ganz konkreten Gefahrensituationen, sondern erst über den Abgleich wird ja ein Verdacht generiert. Wenn Sie dazu noch etwas sagen könnten. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Frau Kollegin Mihalic. Dann beginnen wir nun auf dieser Seite. Herr Prof. Dr. Arzt. Kurze, knappe Antworten sind erwünscht.

SV **Prof. Dr. Clemens Arzt** (Hochschule für Wirtschaft und Recht Berlin): Ja, das wird diesmal relativ schnell gehen. Ich muss gestehen Frau Renner, Untersuchungen zur Eignung der Maßnahme kenne ich einfach nicht. Da hatte ich jetzt auch in der Vorbereitung nicht die Zeit, da intensiv zu recherchieren, Punkt.

Zu den Fragen oder zu einer Frage von Herrn Gunkel: Datenschutzrechtliche Kontrolle bei Weitergabe an Drittstaaten. Hier haben wir den § 10, der dann entsprechend nochmal auf die §§ 78 bis 80 Bundesdatenschutzgesetz verweist, die dann wiederrum möglicherweise ein Beschluss der Kommission verlangen und ähnliches. Aber wenn Sie sich den § 10 anschauen, dann reicht es, dann kann übermittelt werden, wenn diese Behörde im Drittland für die Verfolgung von Terroristen und die Verhütung von Straftaten und der schweren Kriminalität zuständig ist und die Datenübermittlung zu diesem Zweck erforderlich ist.

Ja, wo ist hier ernsthaft die Begrenzung einer Datenübermittlung, frage ich mich? Nochmal, die Verhütung von Straftaten beginnt jenseits der Gefahr. Sie beginnt jenseits des Anfangsverdachtes, sie beginnt da, wo die Fluggastdatenstelle, sprich BKA, meint, hier könnten irgendwann, in ferner Zukunft von irgendjemand Straftaten begangen

werden, die in diese Richtlinie fallen. Das scheint mir doch sehr sehr nebulös und eine völlige Entgrenzungsstrategie zu sein.

Zu den beiden Fragen von Frau Mihalic. Ich denke, der EuGH hat mit seiner Entscheidung zur TK-Vorratsdatenspeicherung, die ja deutlich abweicht von der Linie des Bundesverfassungsgerichtes, nämlich zugunsten der Menschenrechte und der europäischen Grundrechte abweicht, klare Eckpunkte gesetzt. Nun geht es in dem anstehenden Verfahren ja nur um das Abkommen mit Kanada, aber sicherlich wird auch die Fluggastdatenrichtlinie dort irgendwann zur Kontrolle landen und ich kann mir schwerlich vorstellen, dass sie nicht beanstandet wird. Also wenn man sich die Entscheidung zur TK-Vorratsdatenspeicherung anschaut und jetzt hier ja noch mehr Daten hat, deutlich mehr Daten und zwar sensible Daten und für fünf Jahre und nicht nur für ein paar Wochen oder Monate. Und der Regelfall sind eben fünf Jahre, weil alles, was depersonalisiert ist, kann ja auch wieder repersonalisiert werden und für alles was ich erstmal übermittelt habe, zum Beispiel an andere Behörden, gelten auch nicht mehr die fünf Jahre, sondern dann gilt die Regel-Speicherdauer von zehn Jahren. Und wenn ich also zum Ende der fünf Jahre was übermittle, also nach viereinhalb Jahren, dann kommen nochmal zehn Jahre möglicherweise dazu, weil eben die Frist von fünf Jahren nicht absolut ist, sondern durch eine schöne Anschlussüberweisung nochmal um zehn Jahre, bis zu zehn Jahre verlängert werden kann. Die Folgen im Falle einer Europa- oder Grundrechtswidrigkeit, ich denke, das ist ein bekanntes Muster der Gesetzgebung in Deutschland. Wir erlassen Gesetze, von denen wir bereits ahnen, dass sie verfassungs- oder europarechtswidrig sind und warten darauf, bis die zuständigen Gerichte darüber entscheiden. Dankeschön.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Prof. Dr. Arzt. Herr Knetsch, bitte.

SV **Matthias Knetsch** (Lufthansa Group and Government Services bei SITA, Eschborn): Herr Abgeordneter Schuster, Sie hatten zwei Fragen gestellt. Zum einen nach der Zeitplanung und zum zweiten nach der Datenqualität. Es geht in etwa ein Stück auch in die Richtung der Frage von Herrn Abgeordnetem Gunkel – Schwierigkeiten bei der Datenübermittlung. Zur Zeitplanung sieht es ja so aus, dass die EU bereits einen Implementierungsplan vorgegeben hat. Der sieht so aus, dass bereits im nächsten Monat die PIU, also die Passenger Information Unit, stehen sollten und im August 2017 das PNR-System fertig sein soll. Wo Deutschland derzeit steht, habe ich keinen Überblick, das entzieht sich meiner Kenntnis.

Was ich eben in meinen Ausführungen schon dargestellt habe, so ist die Erfahrung die, dass je nach Komplexität solch eines Projektes der Zeitaufwand schon zwischen 12 und 24 Monaten liegt. Hier ist die Frage: Wann ist denn ein Projekt fertig: Hier ist die Frage in der Tat: Wann ist das Projekt dann fertig: wenn 150 Fluglinien, wenn die Daten von 150 Fluglinien verarbeitet werden können oder fängt man zunächst, was auch unsere Empfehlung ist, erstmal klein an, testet das System und baut es dann weiter aus? Ein Testsystem kann durchaus in drei Monaten aufgebaut werden, das ist realistisch, das sind die Erfahrungen, die wir auch haben. Zur Zeitplanung nochmal ein ganz wichtiger Punkt: Deutschland ist nicht der einzige, der die Daten von den Fluglinien erheben möchte und auch die Zertifizierungen jeder einzelnen Fluglinie plant, sondern 26 andere EU-Staaten tun das gleiche, zur selben Zeit, vermutlich bis Mai nächsten Jahres. Hier wird es zu einer Konkurrenzsituation kommen mit den Fluglinien und darauf muss man sich einstellen.

Zum Thema „Datenqualität“. Datenqualität wird oftmals verwechselt mit dem Punkt „vollständige Datensätze“ Hier nochmal zur Erläuterung: Es werden keine neuen Daten erhoben, sondern es werden nur die Daten übermittelt, die die Reservierungssysteme, die Fluglinien eh schon haben. Es wird nichts Neues an Daten erhoben.

BE Abg. **Armin Schuster** (Weil am Rhein) (CDU/CSU): Wie lange speichern die das eigentlich?

SV **Matthias Knetsch** (Lufthansa Group and Government Services bei SITA, Eschborn): Die Fluglinien selber? Das entzieht sich meiner Kenntnis. Es sind auch nicht nur die Fluglinien, sondern auch Reservierungssysteme der sogenannten GDS-Systeme wie Amadeus selber, oder Sabre, die auch Flugdaten und Reservierungen vornehmen, dort wird sicherlich auch über längere Zeit gespeichert, aber der genaue Zeitraum entzieht sich meiner Kenntnis.

Also zum Thema „gute Datenqualität“ spricht man hier eher davon: sind die Daten lesbar und sind die Daten zeitgemäß übermittelt. „Formatfehler“ ist hier sicherlich ein schwieriges Thema, was zu prüfen ist und welche Versionen und Varianten werden geliefert. Ich sagte das eben schon: Nur davon auszugehen, wenn Fluglinien Daten im PNRGOV-Format zusenden, dann ist alles in Ordnung – hier gibt es verschiedene Versionen und Varianten und deshalb müssen auch die Zertifizierungen pro Fluglinie durchgeführt werden.

Zur Frage: Schwierigkeiten bei der Datenübermittlung. Dies betrifft sicherlich den Punkt in der Tat des Carrier Engagements, das heißt, was ich eben versuchte auszuführen. Es ist ganz wichtig ein Team zu haben seitens der Regierungen, die eng mit den Fluglinien zusammenarbeiten, die auch Kenntnisse und Verständnis für dieses Thema der Fluglinien haben. Dort sind entsprechend die Zertifizierungen vorzunehmen, vorgenommen zu werden, fortlaufende Kontrollen und Prüfungen müssen gemacht werden und die regelmäßige Kommunikation zwischen den Fluglinien, den Regierungen, ist absolut wichtig. Auf beiden Seiten müssen Zeitfenster definiert werden, falls Änderungen notwendig sind. Diese Komplexität ist nicht zu unterschätzen. Soweit meine Ausführungen dazu.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Knetsch. Dann Herr Münch, bitte.

SV **Präsident Holger Münch** (Bundeskriminalamt, Wiesbaden): Vielen Dank. Herr Schuster, einen Freibrief für alles haben wir Gott sei Dank nicht. Wir haben Wert darauf gelegt und wir sind auch froh, dass es so formuliert ist, dass nicht das BKA als Zentralstelle die Fluggastdaten verarbeitet, sondern die Fluggastdatenzentralstelle im BKA. Und ich habe das im Eingangsstatement schon gesagt, das bedeutet, dass auch BKA-Mitarbeiter keinen Zugriff auf diese Daten haben, sondern nur die Mitarbeiter der Fluggastdatenzentralstelle und von dort aus an das BKA weiter übermittelt wird. Das halten wir für einen Teil eines sinnvollen Datenschutzkonzeptes, genau wie die technische Trennung, dazu gleich nochmal mehr.

Sie hatten darum gebeten, mal praktische Fallkonstellationen zu benennen. Ich habe mal mitgebracht, wie zum Beispiel in Großbritannien und den USA versucht wird, Dschihad-ausreisende Minderjährige zu erkennen: Das Anlegen eines Musters im Datensatz und dann eine Kontrolle auszulösen, „bisher nicht alleinreisend, jetzt aber alleinreisend unter 18“ ist dann so ein Muster. Kurzfristige Buchung und Barzahlung nochmal als verdachtserhöhendes Moment und Zielflughafen, ist dann „aus der Erfahrung günstig zum Weiterflug oder in Nähe eines Zielgebietes“. Das sind so die Kriterien, die dort angelegt werden. Es wäre ein Muster, was es gilt herauszuarbeiten und das schwierige ist, die Muster so eng zu machen, dass man möglichst zielgenaue Treffer hat. Das ist ja hier schon gefallen.

Ein anderes ist zum Beispiel: Wie erkenne ich denn im Rauschgiftbereich den Schmuggler? Den Körperschmuggler? Die praktische Erfahrung ist häufig ein Barkauf von Tickets. Der Flug wird mehrfach umgebucht. Man hat wenig Gepäck und der Rückflug kommt schnell auf den Hinflug. Das wären so Muster, das man anlegt, um dann Treffer zu finden, jenseits der Fahndung, sondern als aktives Signal. Also Fahndung ist ja was anderes, das kann ich auch mit API-Daten machen, außer im Inner-Schengenflug, sondern hier geht es darum, wie kann ich einen möglichen Straftäter erkennen. Das mal als Beispiele für Muster.

Der Verstoß gegen das Trennungsgebot, der soll natürlich genauso verhindert werden, wie wir es ansonsten auch machen. Das heißt, wir würden dann Daten zum Beispiel an das BfV weitergeben, wenn wir Hinweise zu einer Person haben, bei der wir ausgehen können, dass auch bei den Aufgaben des BfV diese Information jetzt wichtig ist. Also wir haben einen Hinweis auf eine konkrete Person und einen Verdacht, dass jemand Mitglied einer terroristischen Vereinigung ist, dann würden wir auch im Fall, dass diese Daten nicht aus einem PNR kommen, sie weitergeben. Also das heißt, da gelten aus unserer Sicht die gleichen Maßstäbe wie für Daten, die aus anderen Gründen beim BKA anfallen.

Ich möchte vielleicht die Antwort zum „Zeitdruck“ noch ergänzen, die gerade kam. Wir planen den Aufbau des Echtbetriebes – so muss man es ja nennen, einen Pilotbetrieb kann man ja nicht machen, wenn wir mit echten Daten arbeiten, sondern dieses begrenzten Echtbetriebes – zum November dieses Jahres, wenn das Gesetz in Kraft tritt. Bis dahin, glauben wir, dass man sowohl auf

BVA-Seite als auch auf BKA-Seite die Voraussetzungen geschaffen hat. Und das Ganze soll passieren mit einem Flughafen, mit einer Fluggesellschaft und daran dann die Prozesse auch einzuüben, um erst dann auch in den weiteren Ausbau zu gehen.

Zur Effizienz der Systeme, Frau Renner, die Frage habe ich auch gestellt. Ich habe keine hinreichende Antwort bekommen von den Staaten, die ich vorhin genannt habe. Es sind immer Fallbeispiele, die man nennt, aber ich kann Ihnen nicht sagen, auf den Einsatz der Ressourcen, Verhältnis zum Output, wie groß sind die Effekte, sondern das sind Erfahrungswerte, die uns mündlich kommuniziert werden und Beispielfälle, die uns genannt worden sind. Im Bereich des Terrorismus tun sich dann die Partner auch immer schwer, komplette Daten offenzulegen. Da muss ich die definitive Antwort schuldig bleiben.

Auf die Frage, ob wir mit dem Personalansatz klar kommen? Ich weiß wie groß die entsprechenden Einheiten in den USA und in Großbritannien sind – wir sind darunter im Vergleich zu dem Volumen der Daten, die dort bewegt werden. Wir haben das sehr sorgfältig abgewogen, auch nach Besuchen in diesen Ländern und nach Rücksprachen mit dem Bundesverwaltungsamt. Es gibt eine Stelle, wo wir noch nicht genau wissen, ob unsere Berechnungen dann auch sehr treffgenau sind. Das betrifft die Auswertung mit Treffern im Schengener Informationssystem. Das liegt einfach daran, dass das Schengener Informationssystem gar nicht unter dem Aspekt gebaut ist. Also, Sie können die Katalogdaten dort nicht erkennen. Das heißt, jeder Schengen-Treffer wird erstmal dort auflaufen und wir können ihn nicht rausfiltern – oder fast jeder. Und auch dann wird es manuell so sein, dass wir immer nachfragen müssen, weil auch in den ausschreibungsbegründenden Unterlagen im Schengener Informationssystem wird nicht zweifelsfrei die Katalogtat zu erkennen sein. Also hier müssen wir einfach sehen und da sind wir auch noch im Gespräch mit den europäischen Partnern, die das Problem ja alle haben, wie kann man hier auch nachschärfen, sodass wir dort manuellen Aufwand vermeiden und möglichst wenig nicht notwendige Kontrollen am Ende noch auslösen. Also das ist die einzige Unschärfe, die ich momentan sehe, vorbehaltlich der Tatsache, dass wir natürlich da noch lernen müssen und erstmal auch aufbauen müssen.

Zur Frage des Personalaufbaus. Das Ganze soll ja schrittweise passieren. Sie haben ja gefragt, ob wir das Personal nicht an anderer Stelle einsetzen sollten/müssten? Wir werden starten zum November 2017 mit 34 Mitarbeitern, dann aufbauen nach einigen Monaten auf 40 und dann schrittweise weiter aufbauen mit der Zahl der Fluggesellschaften, die angeschlossen werden. Und das geht, weil es auch nicht alles Polizisten sind, das muss man jetzt auch sagen, sondern wir werden am Anfang 10 bis 15 Polizisten dort einsetzen, Vollzugsbeamte und dazu auch weitere, die wir dann auch zeitnah einkaufen können, so will ich es mal ausdrücken, einstellen können, sodass wir möglichst wenige aus anderen Bereichen verschieben, sondern parallel aufbauen, auch zu anderen Bereichen. Aber zweifelsohne ist das natürlich eine große Herausforderung bei all den vielen Herausforderungen, die das BKA zurzeit hat.

Herr Gunkel, zur Frage warum wir das mit dem BVA machen? Weil wir diese Prozesse dort auch eingeübt haben. Das BVA ist auch an anderer Stelle schon Datenhalter. Zum Beispiel bei biometrischen Daten und wir machen das fachliche Konzept und wir glauben, dass es auch wichtig ist, das so weiter auszubauen, auch wenn wir im Hinterkopf wieder all die Fragen und Konsolidierungen von IT-Systemen haben, glaube ich, ist das der richtige Schritt, auch hier so mit diesem Partner, den wir schon verlässlich haben, weiter zusammenzuarbeiten und darauf auch aufzubauen. Und das wir das dann auch selber machen liegt daran, dass die Nähe des Zwecks des Gesetzes natürlich bei den Aufgaben des BKA liegt: Terrorismusbekämpfung und schwere Kriminalität.

Wenn ich ehrlich bin, habe ich Ihre Frage zu den Sicherheitslücken bei der Datenübermittlung nicht richtig verstanden. Meinen Sie, dass zwischen BVA und BKA dann solche Lücken auftauchen könnten?

Abg. **Wolfgang Gunkel** (SPD): Ja. (genickt)

SV **Präsident Holger Münch** (Bundeskriminalamt, Wiesbaden): Das schließen wir nach jetzigem Stand aus, weil es so sein wird, dass das BVA quasi den Abgleich in die Fahndungsdateien anstößt und wenn es einen Treffer gibt, wir den erhalten. Das heißt, wir sehen die Daten nicht, aber das BVA

sieht die Treffer nicht. Und so soll es passieren, dass wir also dann beiderseitig den Datenschutz herstellen und gleichzeitig aber auch keine Datenverluste haben.

Zu Erfolgen in anderen Staaten und der Zahl der Treffer habe ich schon etwas gesagt. Ihre vierte Frage habe ich leider vergessen.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Münch. Herr Sander, bitte.

SV **Alexander Sander** (Digitale Gesellschaft e.V., Berlin): Vielen Dank. Zunächst mal zu diesem Freifeld, was Sie angesprochen haben. Also dabei handelt es sich um ein Feld, wo im Grunde zu jedem Zeitpunkt der Reise irgendjemand, der etwas mit dieser Reise zu tun hat, also Airline-Mitarbeiter zum Beispiel, etwas in dieses Feld eintragen können. Es gab so Datenanfragen, wo Leute ihre PNR-Daten angefragt haben und da stehen dann zum Beispiel so Sachen drin, dass jemand einen Apfel dabei gehabt hat oder es steht drin, dass jemand ein Buch dabei gehabt hat und dann steht der Titel des Buches dabei. Es steht dabei, dass jemandem seine Schuhe geputzt wurden oder allerlei dieser Informationen. Also es sind Informationen, wo man sich zum einen fragen muss: Inwieweit kann man die überhaupt nutzen, um gegen Terrorismus und schwere Kriminalität vorzugehen und es können eben auch sehr schnell sehr sensible Informationen da drin auftauchen in diesem Freifeld und es ist zu keinem Zeitpunkt nachvollziehbar, wer diese Informationen da rein geschrieben hat. Also im Grunde jeder, der Zugang hat zu diesen PNR-Daten kann da relativ leicht in diesen Datensätzen auch Sachen verändern, ohne dass nachvollziehbar ist, wer das gemacht hat. Das betrifft nicht nur das Freifeld, das betrifft alle Felder und letztens hat auch der CCC eindrucksvoll gezeigt, wie leicht man eben an Buchungsdaten herankommt, wie leicht man die dann auch entsprechend verändern kann und das betrifft natürlich dann eben auch dieses Freifeld und dann ist natürlich die Frage, wenn man sich das Gesetz genauer anschaut, dann steht ja da drin, dass sensible Daten nicht verarbeitet und gespeichert werden sollen. Das bedeutet, es muss jemand irgendwann vorher in dieses Freifeld da reinschauen und diese Daten da irgendwie rausholen, wenn sie denn sensibel sind und das bedeutet, dass bei diesen 170 Millionen Reisenden, wie wir jetzt schon gehört haben, in jeden Datensatz reingeschaut werden müsste, von einer Person, von einem Mensch, weil das funktioniert mit technischen Maßnahmen nicht, um diese Daten da raus zu holen. Warum das mit technischen Maßnahmen nicht funktioniert, dass zeigt der Blick nach Australien, wo eben diese Fluggastdaten ja von der EU auch hin übermittelt werden und die eben in ihrem Evaluierungsbericht auch klar das Problem benannt haben und gesagt haben: Es ist unmöglich, eine technische Filterung vorzunehmen dieser sensiblen Informationen. Es geht einfach nicht, es landen immer in dieser Datenbank dann auch sensible Daten und man muss diese händisch einfach rausholen, man muss da einfach reinschauen und gucken, was das ist, weil es eben ein Freifeld ist, es ist keine Kategorie. Im Vorfeld der Debatte im EU-Parlament gab es ja zum Beispiel auch noch die Felder mit Gesundheitsdaten oder den Essenswünschen. Die wurden nachher dann rausgenommen, weil man gesagt hat, dass der sensible Charakter zu groß ist, aber, wie wir jetzt eben wissen, stehen auch solche Daten in so einem Freifeld drin und die können eben nicht einfach rausgelöscht werden, sondern man muss die sich tatsächlich anschauen und das ist ein massives Problem bei diesem Freifeld. Also die Informationen, die drin sind, sind nicht nachvollziehbar, auch nicht, wer diese Informationen da rein gesetzt hat und diese Daten landen am Ende des Tages in dieser Datenbank.

Zu der zweiten Frage, bezüglich Profiling oder überhaupt Profiling-Maßnahmen. Also ich hatte es ja einleitend schon gesagt, in dem Gesetz steht ja drin, dass es eben verdachtsbegründende und verdachtsentlastende Prüfungsmerkmale geben soll. Und die muss sich ja irgendjemand ausdenken. Und das macht ja das BKA, die sitzen dann da und überlegen sich, was ist denn jetzt verdachtsentlastend und was ist eben verdachtsbegründend und da gehen natürlich auch immer irgendwelche Gedanken damit einher und ein Stück weit sicherlich auch Vorurteile, die da transportiert werden. Und diese Muster, die da entstehen, sind eben niemals vorurteilsfrei, weil es muss ja irgendeinen Moment geben, wo man sagt, das ist jetzt verdachtsentlastend und das ist jetzt verdachtsbegründend und das wird eben mit aller Wahrscheinlichkeit nicht dabei bleiben, dass es eben dieses eine Muster gibt, wie wir jetzt gehört haben, sondern dass es viele verschiedene Muster geben wird und das viele Leute an diesen Mustern

dran arbeiten und dass natürlich auch die Daten selbst genutzt werden, um diese Muster zu erstellen. Und hierbei werden natürlich dann durch die Daten selbst wieder, die sich dann in so einem Muster wiederfinden, diese Vorurteile mittransportiert. Also von daher glaube ich nicht, dass jetzt hier dadurch ein Mehrwert geschaffen wird, was eben nicht dazu führt, dass es kein Racial Profiling gibt, sondern es wird weiterhin eben Vorurteile in diesen Algorithmen geben.

Zur Weitergabe der Daten an Drittstaaten. Es ist so, dass es ja viele Drittstaaten gibt, die jetzt sich jenseits jeglicher rechtsstaatlicher Prinzipien, wie wir sie kennen, bewegen. Und das Problem ist relativ klar, weil es wird nur davon gesprochen, dass es ein angemessenes Datenschutzniveau in diesen Staaten geben muss. Das ist natürlich keinesfalls ausreichend und keinesfalls klar genug, um zu sagen: Das sind die Prinzipien, nach denen wir prüfen müssen, dass es eben ein angemessenes Datenschutzniveau ist, um die Daten weiterzugeben. Wir wissen ja auch zum Beispiel seit der Safe Harbor Entscheidung mit den USA, dass da auch staatliche Institutionen durchaus mal falsch liegen können bei diesen Beurteilungen. Und das Problem ist auch, was passiert dann, wenn die Daten einmal da sind? Also auch da gibt es keine Prüfungspflichten oder ähnliches, die dann eben das Ganze überprüfen, ob die Daten tatsächlich dann irgendwann mal wieder gelöscht wurden oder was mit den Daten dann passiert ist. Also, sind die dort von diesen Drittstaaten vielleicht nochmal weitergegeben worden an andere Drittstaaten oder auch in diesen Staaten, an welche Behörden gehen diese Daten überall? Also das bleibt alles vollkommen unklar und es gibt eben da überhaupt keine Garantien für einen entsprechenden Datenschutz und eigentlich kann man davon ausgehen, dass wenn die Daten einmal an Drittstaaten weitergegeben wurden, dass sie dann auch entsprechend nahezu verloren sind. Also von daher würde ich da sagen, dass hier auch die Vorgaben keinesfalls ausreichend im Gesetz sicherstellen, dass hier kein Schindluder mit diesen Daten getrieben wird.

Ich hatte es auch schon in meinem Eingangsstatement gesagt, dass ich auch ein großes Problem mit dieser Speicherdauer habe, weil mir auch vollkommen unklar ist, warum eben jetzt fünf Jahre vorgesehen sind. Es gibt ja zum Beispiel so ein Fluggastdaten-Abkommen mit den USA. Da ist man bei 15 Jahren. Bei Australien 5 ½ Jahren. Bei Kanada eben auch bei fünf Jahren. Dann ist es da auch völlig unterschiedlich, wann diese Daten depersonalisiert oder anonymisiert werden. Also ganz am Anfang im Entwurf der Kommission stand ja noch das Wort „anonymisieren“ und „deanonymisieren“, bis man dann herausgefunden hat, dass das gar nicht geht. Und auch hier sind in den Abkommen, die geschlossen worden sind, überall vollkommen unterschiedliche Speicherdauern vorgesehen. Es ist in allen Abkommen vollkommen unklar, wann die Daten jetzt eben depersonalisiert werden und wann nicht. Es wirkt eben schlichtweg willkürlich. Also die Speicherdauer an sich wirkt willkürlich. Es wirkt willkürlich, warum nach einem halben Jahr die Daten depersonalisiert werden müssen und nicht schon zum Beispiel nach einer Woche? Oder eben nach vier Jahren oder wann auch immer. Es gibt an keiner Stelle eine sinnvolle Begründung dafür, warum die Daten in dieser Form solange vorgehalten werden und von daher, wie gesagt, würde ich auch sagen, dass die Speicherdauer grundsätzlich einfach nicht angemessen und nicht verhältnismäßig ist, weil eben die Begründung dafür fehlt.

Und dann zur letzten Frage, zur Eingriffsschwelle für die Verdächtigen. Im Gesetzesvorschlag der EU-Kommission, also in dem Richtlinienvorschlag, stand damals in der Begründung drin, dass man mit dieser Maßnahme bisher unbekannte Verdächtige finden möchte und das zeigt ja eigentlich relativ klar, was passieren soll. Das ist eine Profiling-Maßnahme, mit der Verdächtige kreiert werden. Es handelt sich eben nicht darum, dass man jetzt nach Verdächtigen sucht, sondern dass man Verdächtige kreiert. Und wir haben ja auch von Herrn Münch gehört, dass das möglichst viel und genau passieren soll. Also mit anderen Worten, man wird auch Treffer haben, die eben unbescholtene Bürger betreffen. Es werden immer unverdächtige Personen bei dieser Maßnahme mit überwacht werden und das Problem ist ja nicht, dass dann eben festgestellt wird, das ist eine unverdächtige Person, sondern das muss ja dann auch überprüft werden. Also es gehen damit weitere Überwachungsmaßnahmen einher, die dann in der Folge diese Personen über sich ergehen lassen müssen und was daraus sich entwickeln kann, sieht man, glaube ich, ganz gut, wenn man

wieder in die USA schaut, die schon relativ lange mit diesen Systemen arbeiten, und dort auf diese No-Flight-List oder No-Flight-Orders schaut, wo dann eben immer wieder Journalisten, selbst Abgeordnete eben auf solchen Listen stehen, also schon EU-Abgeordnete haben auf den No-Flight-Listen der USA gestanden, die eben auf diesen PNR-Daten beruhen. Und dreijährige Kinder haben auf diesen Listen gestanden und wurden eben in Verbindung mit Terrorismus gebracht und da zeigt sich, dass diese Eingriffsschwelle immer dazu führt, dass Personen, die vollkommen unbescholten sind, in das Visier der Ermittlungsbehörden geraten und dann eben massive Einschränkungen ihrer Grundrecht in Kauf nehmen müssen, obwohl sie sich nichts haben zu Schulden kommen lassen. Vielen Dank.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Sander. Herr Prof. Dr. Wollenschläger, bitte.

SV **Prof. Dr. Ferdinand Wollenschläger** (Universität Augsburg): Vielen Dank. Ich antworte insbesondere auf die beiden Fragen von Herrn Schuster, wobei Ihre erste Frage nach der Anlasslosigkeit schon ein breites Spektrum umfasst. Die Frage hatten wir ja auch schon diskutiert hier bei der Anhörung über die Telekommunikationsverkehrsdatenspeicherung. Die Bewertung hängt davon ab, was Sie unter Anlasslosigkeit verstehen. Es wäre falsch, Anlasslosigkeit so verstehen, dass hier ein Gesetz auf den Weg gebracht wird, das zu Grundrechtseingriffen ohne Zwecksetzung ermächtigt; Anlass ist vielmehr der Beitrag, den man sich von diesen Eingriffen zur Verhütung bzw. zur Verfolgung von Straftaten erhofft. Insofern besteht keine Anlasslosigkeit. Anlasslosigkeit ist aber gegeben, wenn Sie die Anlasslosigkeit – wie bei der Vorratsdatenspeicherung – darauf beziehen, dass diese Eingriffe auch Personen treffen, die nicht in einem Bezug zu terroristischen Straftaten und schwerer Kriminalität stehen, weil eine breite Basis für den Abgleich, genauso bei der TK-Vorratsdatenspeicherung, benötigt wird.

Auf einen Punkt möchte ich nochmals hinweisen, damit keine falsche oder auch selektive Wahrnehmung besteht. Man kann nicht für gegeben annehmen, dass die Rechtsprechung des Europäischen Gerichtshofs zur Vorratsdatenspeicherung übertragbar ist – unabhängig von der ganz anderen Frage, wie man sie versteht, und darauf zwingende Prognosen stützen. In seinem Schlussantrag hat auch Generalanwalt Mengozzi klargestellt, dass dieser Eingriff weniger, wenn ich zitieren darf, weitreichend ist als die frühere Vorratsdatenspeicherung und sich auch weniger auf das tägliche Leben der Einzelnen auswirkt, was, wenn man die Art der gespeicherten Daten anschaut, auf der Hand liegt. Daher ist hinter die Übertragbarkeit ein Fragezeichen zu setzen, trotz der jüngeren strengeren Rechtsprechung des EuGH.

Wenn Sie Anlasslosigkeit so verstehen, wie das Vorredner in den Raum gestellt haben, nämlich dass das Bundeskriminalamt aufgrund völlig unspezifischer Rechtsgrundlagen Daten verarbeiten darf, möchte ich dem doch deutlich entgegentreten, sodass kein falscher Eindruck vom Gesetzentwurf entsteht. Zunächst wird hier keine General- oder Superbefugnis für das BKA geschaffen: vielmehr zeigt bereits ein Blick in den Gesetzentwurf, dass dieser konkrete Datenverarbeitungsvorgänge betrifft: im § 2 die Übermittlung, dann im § 4 Absatz 2 den Abgleich, im § 4 Absatz 5 die Möglichkeit des punktuellen Zugriffs und schließlich in § 6 die Übermittlung. Hier besteht keine Generalklausel.

Und noch ein weiterer Punkt, der meines Erachtens auch unscharf in den Raum gestellt wurde. Der Annahme, dass das Bundeskriminalamt zu präventiven Zwecken ohne eine Eingriffsschwelle tätig werden darf, möchte ich entgegentreten. Vielmehr findet sich im Gesetzentwurf die Formulierung, dass eine gewisse Wahrscheinlichkeit bestehen muss, indem hier von „innerhalb eines übersehbaren Zeitraums“ gesprochen wird, eine Formulierung, die sich auch im Entwurf des aktuellen BKA-Gesetzes findet. Ich würde vielleicht in Ergänzung meiner Vorschläge insoweit noch empfehlen: Das BKA-Gesetz konkretisiert diese Schwelle noch weiter durch Zusätze wie ihrer Art nach feststellbaren Straftaten etc. Mas sollte prüfen, inwieweit diese Begrifflichkeiten aus dem BKA-Gesetz übernommen und weiter konkretisiert werden können. Ein Blick in das Gesetz widerlegt jedenfalls, dass keinerlei Schwelle im präventiven Bereich besteht.

Letzter Punkt. Sie hatten mich noch auf die Datensicherheit angesprochen. Es ist richtig, dass der Gesetzentwurf auf den ersten Blick keine Anforderungen an die Datensicherheit enthält. Bei diesem Einwand denkt man sofort an die

Rechtsprechung des Bundesverfassungsgerichts, die hohe Anforderungen an die Datensicherheit aufgestellt hat im Kontext der Vorratsdatenspeicherung – allerdings wegen deren sehr großer Eingriffsintensität und der Speicherung nicht bei staatlichen Stellen, sondern bei privaten Unternehmen, was einen gewissen Unterschied rechtfertigt. Datensicherheit wird in unserem Kontext zudem so sichergestellt, dass diejenigen Regelungen des Bundesdatenschutzgesetzes, die für das Bundeskriminalamt gelten, um Datensicherheit zu gewährleisten, die ja letztlich auch auf den europäischen Rahmenbeschluss, jetzt dann die neue Richtlinie, zurückzuführen sind, Anwendung finden und dieses Mindestmaß, das dafür erforderlich erachtet wird, sicherstellen. Vielleicht darf ich noch zwei kleine Anmerkungen machen. Erstens zur Objektivität von Profilen. Sowohl der Datenschutzbeauftragte der Zentralstelle als auch die Bundesdatenschutzbeauftragte sind einbezogen in die Erstellung und Anwendung dieser Profile. Zweitens: Die Garantie für Übermittlungen in Drittstaaten kann und muss man im Einzelnen diskutieren und genau anschauen, aber hier gelten auch die allgemeinen Regeln: Gemäß §§ 78 ff. Bundesdatenschutzgesetzentwurf ist es auch jetzt nicht so, dass Sie ohne Weiteres Daten in Drittstaaten übermitteln können, wobei, und insofern sind wir uns einig, diese elementaren Garantien, die verfassungsrechtlich, europarechtlich, aber auch nach einem Bundesdatenschutzgesetz notwendig sind, im Einzelfall sicherzustellen sind. Danke.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Prof. Dr. Wollenschläger. Wir hätten dann noch Zeit für eine kurze weitere Fragerunde. Ich bitte dann aber, die Fragen auf ein oder zwei Fragen zu limitieren. Herr Kollege Mayer, bitte.

Abg. **Stephan Mayer** (Altötting) (CDU/CSU): Vielen Dank Herr Vorsitzender. Ich habe eine Frage, die ich an Herrn Prof. Dr. Wollenschläger und an den BKA-Präsidenten Münch richten möchte. Und zwar, wie aus Ihrer Sicht, sowohl in rechtlicher als auch in praktischer Hinsicht, folgende Fallkonstellationen zu behandeln sind nach dem neuen PNR-Umsetzungsgesetz. Es wird ein INPOL-gesuchter Räuber festgestellt, der einen Inner-Schengenflug plant. Er möchte von Frankfurt nach Palma de Mallorca fliegen. Das taucht dann natürlich auf, wird festgestellt vom BKA. Nun gehört der Raub § 249 StGB nicht zu den Katalogstraftaten des § 4 Absatz 1 des Gesetzentwurfes. Demnach verbietet es sich für das BKA diese Information beispielsweise der Bundespolizei am Frankfurter Flughafen mitzuteilen, um den geplanten Abflug des gesuchten Verdächtigen wegen Raubes zu verhindern.

Zweite Fallkonstellation: Es gibt den Hinweis, dass ein auch im INPOL zur Fahndung ausgeschriebenes minderjähriges Kind, dem aufgrund eines familiengerichtlichen Beschlusses die Ausreise aus Deutschland verboten ist, plant Deutschland zu verlassen, auch im Rahmen eines Inner-Schengenfluges. Auch dieser Umstand, auch die Straftat § 235 StGB, die widerrechtliche Verbringung von Minderjährigen außer Landes, gehört nicht zu den Katalogstraftaten des § 4 Absatz 1 des Gesetzentwurfes. Hier gleiche Fragestellung. Es ist dem BKA nach dem jetzt vorliegenden Gesetzentwurf untersagt, der Bundespolizei am Frankfurter Flughafen diese Mitteilung zu machen. Wie wird aus Ihrer Sicht, sowohl in praktischer als auch rechtlicher Hinsicht, mit diesen beiden Fallkonstellationen umzugehen sein?

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Kollege Mayer. Frau Kollegin Renner, bitte.

BE Abg. **Martina Renner** (DIE LINKE.): Ich habe auch nur noch zwei Fragen. Eine an Herrn Münch. Sie konnten die Frage nach der Effizienz nicht beantworten. Haben uns aber Ausführungen dazu gegeben, wie zum Beispiel in Großbritannien solche Muster aussehen, um Dschihadisten bzw. Drogenhändler zu schnappen. Da frage ich mich natürlich, ob man über solche Muster reden sollte, öffentlich, wenn man dann in Zukunft als Krimineller weiß, dass ich besser nicht nur mit Handgepäck, Barzahlung und kurzer Ein- und Ausreise fliege. Egal. Aber das konnte Großbritannien mitteilen, wie die Muster aussehen, aber sie konnten nicht mitteilen, in welchem Fall zum Beispiel ein Drogenhändler geschnappt wurde. Das ist dann geheim. Das wirkt komisch, ja. Und ich glaube, die Frage ist ja von vielen Kolleginnen und Kollegen hier gestellt worden. Die Frage tatsächlich nach der Wirksamkeit einer Maßnahme hängt ja auch sehr eng mit der Frage der Verhältnismäßigkeit zusammen und die muss man, glaube ich, in einem Gesetzgebungsverfahren

beantworten können. Und da kann man nicht sagen: Das ist geheim.

Ich finde, das ist eines der großen Mankos hier heute in der Anhörung. Länder, die seit Jahren diese Praxis üben, Großbritannien, USA, Mexiko, China, Australien, Kanada, da muss es doch valide Aussagen zu geben, was die Effizienz angeht. Und bei Drogenhändlern kann auch nicht gelten, dass es im Bereich des Terrorismus liegt und damit möglicherweise schützenswerte Inhalte betrifft. Also nur mal als Vorabbemerkung. Ist es wirklich so, dass es nichts gibt? Dass wir hier über eine Black-Box reden?

Und die zweite Frage, die geht an Herrn Sander. Der ganze Bereich der Überwachungs- und Kontrollmaßnahmen bei Reisebewegungen ist ja einer, der in den letzten Jahren eine große Bedeutung gewonnen hat. Also sogenannte Nacktscanner oder die Diskussion, dass man sogar Bahnreisende in Zukunft registrieren sollte und ähnliches mehr. Sind es alleine Sicherheitsinteressen, die hier die Diskussion führen oder sind dahinter nicht auch vielleicht Sicherheitsfirmen, Softwarehersteller und ähnliches, die da ein gewisses ökonomisches Interesse daran haben? Weil millionenfache Datensätze zu verwalten ist auch eine Industrie und da gibt es vielleicht auch Interessen und befördern die vielleicht jenseits der Effizienz auch bestimmte Diskussionen?

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Frau Kollegin Renner. Herr Kollege Gunkel, möchten Sie noch? Nein – dann Frau Kollegin Mihalic, bitte.

Abg. **Irene Mihalic** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank Herr Vorsitzender. Ich habe auch nur noch eine Frage an Herrn Arzt und Herrn Wollenschläger. Die Kollegin Renner hat ja vorhin schon auf eine gewisse Problematik hingewiesen, was die Muster betriff. Und das Verfahren zur Rasterung der Fluggastdaten unverdächtiger Personen eben zur Verdachtsgenerierung mit solchen Mustern ist ja etwas, was wir, sozusagen, auch in unserem gesetzlichen System bisher noch nicht kennen. Also das ist ja auch rechtlich für uns etwas völlig neues, weil es gibt ja kein vergleichbares Gesetz, wo so etwas schon irgendwie geregelt ist. Und jetzt haben wir natürlich das Problem, dass das oder die Muster in diesem Gesetz ja auch nicht genau bestimmt ist/sind und deswegen wäre meine Frage: Wie müsste denn aus Ihrer Sicht eine rechtstaatliche Regelung im Gesetz aussehen, die eben allen von der Datenrasterung betroffenen Personen hinreichend transparent macht; in welcher Weise bzw. womit genau die Daten eigentlich abgeglichen bzw. gerastert werden? Denn von solch einem Eingriff betroffene Personen müssten ja auch die Möglichkeit haben, die Maßnahme auf dem Rechtsweg irgendwie überprüfen zu lassen, wenn sie davon betroffen sind und dazu müssten die Betroffenen ja eben auch, sozusagen über das Gesetz nachvollziehen können, was genau im Rahmen eines solchen Abgleichs mit ihren Daten passiert.

Und Herr Wollenschläger, Sie haben ja auch auf die nachzubessernde oder aus Ihrer Sicht nachzubessernden Überprüfungsmöglichkeiten der Datenschutzbeauftragten hingewiesen und auch die Datenschutzbeauftragte bräuchte ja eine Art Prüfschema, dass sich ja auch irgendwie aus den gesetzlichen Regelungen ergeben muss, um eben auch das, was da im Rahmen des Datenabgleichs oder im Rahmen des Musterabgleichs passiert, auch irgendwie nachvollziehen zu können.

Also nochmal zusammengefasst: Wie genau müsste eine gesetzliche Regelung aussehen, die all diesen Anforderungen, die ich gerade beschrieben habe, genügt? An Sie beide gerichtet.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Frau Mihalic. Das waren jetzt nun Fragen an Herrn Arzt, Herrn Münch, Herrn Sander und Herrn Wollenschläger. Dann beginnen wir diesmal auf dieser Seite. Herr Wollenschläger, bitte.

SV **Prof. Dr. Ferdinand Wollenschläger** (Universität Augsburg): Vielen Dank. Zunächst also zur Prüfungsfrage von Herrn Mayer: Wie würde man konkret Sachverhalte unter dieses Gesetz subsumieren? Sie haben auf Probleme bei der Anwendung hingewiesen: Würden etwa der Raub und die Kindesentziehung – jedenfalls dem Wortlaut nach nicht erfasst – darunter fallen? Das Problem ist, dass die Europäische Richtlinie keine konkreten Tatbestände nennt, sondern strafbare Handlungen in Kombination mit einer Mindesthöchststrafe, und dies wegen der Heterogenität der Straftatbestände in den Mitgliedstaaten. Daher ist die Konkretisierung letztlich eine Umsetzungsfrage. Meines Erachtens

stellt sich hier die Frage, inwieweit die weitgefassten Tatbestände der Entführung in Nummer 14, was die Kindesentziehung betrifft, oder der Tatbestand des Diebstahls in organisierter Form oder mit Waffen gewisse Konkretisierungsspielräume für den Gesetzgeber eröffnen. Die Frage ist, inwieweit sich dies über einen Katalog auf nationaler Ebene erfassen ließe. Das ist ein Punkt.

Ein zweiter Punkt, den man sich auch fragen könnte: Wäre eine überschießende Richtlinienumsetzung denkbar? Entfaltet die Richtlinie aus Grundrechtsschutzgründen eine abschließende Wirkung, oder wäre es dem deutschen Gesetzgeber möglich, über einen Katalog hier weitere Straftatbestände aufzunehmen, solange er gewisse Mindestschwellen – wir sind hier im Bereich der schweren Kriminalität – einführt, vielleicht unter Anknüpfung an Tatbestände, die genannt sind – Diebstahl in organisierter Form mit Waffen, was in Richtung Raub geht, und die Entführung, die genannt ist? Aufgrund der unvollständigen Synchronisierung von nationalen Straftatbeständen mit strafbaren Handlungsweisen, die eben notgedrungen so sein müssen in einer Richtlinie, die für 28 Strafrechtssysteme gilt, stellen sich in der Tat die Umsetzungsfragen, auf die Sie hingewiesen haben.

Beim Betrug ist, wie ich angedeutet habe, die Strafbarkeitsschwelle sicher zu niedrig angesetzt, weil jede Betrugsstraftat erfasst wäre. Das wäre eine Frage, die man im Rahmen der Umsetzung klären müsste.

Dann die Frage von Ihnen, Frau Mihalic. Sie hatten ja im Wesentlichen die Frage des Abgleichs mit Profilen angesprochen. Das ist in der Tat eine neue Maßnahme, die grundrechtlich, das ist auch bei Herrn Arzt angeklungen, Fragen aufwirft: Ist das rechtfertigungsfähig? Auch hier kann man wieder auf den Generalanwalt verweisen, der diese Möglichkeit der Profilbildung im Grundsatz für zulässig erachtet hat. Wie muss so ein Gesetz ausschauen? Wenn man gesetzlich die Muster schon verankerte, wäre das zweckfrei, weil – das hat ja auch Ihre Kollegin angesprochen – das Betroffenen ein Einstellen auf diese Muster ermöglicht. Ich denke, hier enthält in besonderer Weise das deutsche Fluggastdatengesetz im Entwurf mit der Kombination „verdachtsbegründend“, „verdachtsentlastend“ schon Kriterien, die dem Erfordernis gerecht werden, dass die Profilbildung auf Tatsachen beruhen muss, die nicht aus der Luft gegriffen sein dürfen, sondern die sich auf Muster mit Blick auf die Begehung konkreter Straftaten beziehen.

Ich hatte auch darauf hingewiesen, dass die Datenschutzbeauftragten eingebunden sind in die Erstellung und in die Kontrolle; insoweit, da will ich nicht falsch verstanden sein, besteht die Kontrolle. Das ist der einzige Punkt, für den die Datenschutzkontrolle durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ausdrücklich vorgesehen ist, auch im deutschen Gesetz. Ich hatte für eine Klarstellung plädiert, was der Tätigkeit der Überwachung insgesamt unterliegt. Dabei wird man darauf achten müssen, dass natürlich diese gesetzlichen Tatbestände, die man viel konkreter nicht fassen können wird, in der Umsetzung durch das Bundeskriminalamt anhand der gesetzlichen Vorgaben – Tatsachenbezug, hinreichende Validität, Verdachtsbegründung, Verdachtsentlastung – formuliert werden und dann in Kombination mit der Datenschutzkontrolle, die vorgesehen ist, dafür gesorgt wird, dass das diesem rechtlichen Rahmen entspricht. Hierauf ist zu setzen. Ich denke, das Gesetz enthält zumindest Tatbestandsmerkmale, anhand derer eine entsprechende Kontrolle möglich ist. Damit ende ich. Dankeschön.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Wollenschläger. Herr Sander, bitte.

SV **Alexander Sander** (Digitale Gesellschaft e.V., Berlin): Zu den ökonomischen Interessen, die da dahinter stehen. Also grundsätzlich, klar sind solche Datenbanken Millionenprojekte. Also es ist jetzt nicht nur damit getan, dass man mal 5.000 Euro auf den Tisch legt und dann hat man so eine Datenbank, sondern hier werden Millionen investiert und auch, wenn man sich allgemein mal diesen weltweiten Sicherheitsmarkt anschaut, dann hat er sich, laut Zahlen der EU-Kommission, in den letzten Jahren, in den letzten 10 Jahren, verzehnfacht. Also auch eine relativ krisensichere Branche, die auch eine gewisse Lobby macht, auch in Brüssel vor allen Dingen hat, wo ja diese Gesetze zum großen Teil auch herkommen. Sie hatten es ja auch schon angesprochen mit den Nacktscannern zum Beispiel. Und wenn man sich dieses gesamte Konzept „Airport-Security“ oder die

Sicherheitskonzepte in der Luftfahrtbranche anschaut, dann geht das ganz klar in diese Richtung, dass immer mehr Datenauswertungen zu vermeintlich mehr Sicherheit führen sollen. Es gibt dann so Konzepte von der IATA, also diesem Internationalen Luftfahrtverband, über den Checkpoint der Zukunft, wo es dann eben so zum Beispiel drei solche Sicherheitslanes geben soll, also grob unterteilt einmal für Vielflieger, einmal für normale Reisende und einmal für Verdächtige und diese Leute werden vorher durch Datenermittlung zum Beispiel dann in diese verschiedenen Lanes reingestopft und auch insbesondere in diesem Bereich gibt es eine sehr intransparente Lobby in Brüssel, die da sehr aktiv ist. Und wenn man auf diese Bahnreisen guckt, also es gibt natürlich auch eben nicht nur die Forderung, jetzt PNR-Daten für Flugreisen zu sammeln. PNR-Daten werden überall gesammelt. Alles was mit Reisen zu tun hat, wir haben es vorhin schon gehört, es gibt Datenverarbeiter wie Amadeus, die dann sowas komplett verarbeiten, also alles was mit Reisen zu tun hat, Mietwagen, Hotelbuchung, eben Flugreisen, all so was wird als PNR-Daten gesammelt. Da gibt es diese Datenbanken und man sieht, dass der Antiterrorbeauftragte der EU und viele Sicherheitspolitiker auch schon im Zuge der Verhandlung um das EU-PNR schon immer wieder gefordert haben, diese Maßnahmen auszuweiten. Eben zum Beispiel auf Bahnreisen, auf Schiffsreisen, sowie wie man das jetzt eben in Belgien vorhat. Dort gibt es einen entsprechenden Gesetzesvorschlag, wo dann nicht nur diese Flüge überwacht werden sollen, sondern eben auch Bahn- und Schiffsreisen von Belgien, also internationale Züge von Belgien raus und nach Belgien rein. Und da zeigt sich der Weg, wo das hingeht. Also wenn man hier einmal dieses Fass mit dieser Vorratsdatenspeicherung von Reisedaten aufmacht, kommt eben am Ende des Tages so eine Totalüberwachung des Reiseverkehrs dabei heraus, weil man dann zügig, wie jetzt auch schon, wenn man sich die EU-Richtlinie anguckt, gesagt hat: Alle Flüge in die EU herein und alle Flüge aus der EU heraus. Jetzt setzen sich dann zwei Tage später die Innenminister zusammen und sagen: Ja innereuropäische Flüge müssen auch mit überwacht werden. Also wo man hier eben klar diesen Druck sieht, dass diese Maßnahmen immer ausgeweitet werden und da stehen natürlich auch immer ökonomische Interesse dahinter, weil diese Datenbanken Geld kosten. Da müssen Leute eingestellt werden, da müssen Firmen mit irgendwas beauftragt werden, die dann diese verschiedenen Standards, die jetzt zum Beispiel noch vorherrschen, in irgendeiner Art und Weise so zusammenbringen, dass dann hier auch die Sicherheitsbehörden darauf zugreifen können. Und da gibt es natürlich entsprechend auch weniger Anbieter, die dann überhaupt die Kompetenz haben, in diesem Bereich tätig zu werden. Auch das hat man zum Beispiel bei den Nacktscannern gesehen, wo es dann am Ende des Tages eigentlich nur zwei Anbieter weltweit gibt, die diesen Nacktscanner überhaupt an Flughäfen zur Verfügung stellen können. Ähnlich ist es bei anderen Sicherheitskonzepten eben auch immer, dass nur eine Handvoll Anbieter überhaupt auf dem Markt ist, die dann natürlich auch ein berechtigtes Interesse aus ihrer Sicht daran haben, sich einen ökonomischen Vorteil zu verschaffen und dann sich immer wieder darüber freuen, wenn solche Datenbanken auch angelegt werden.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Sander. Herr Münch, bitte.

SV **Präsident Holger Münch** (Bundeskriminalamt, Wiesbaden): Herr Mayer, Sie haben eine Stelle angesprochen, wo wir uns auch sehr viel Gedanken machen, nämlich die Tatsache, dass, wenn wir als Fluggastdaten-Zentralstelle von einer Ausschreibung Kenntnis erreichen – im Inner-Schengenraum, die ja dann so ohne weiteres in der Regel der Bundespolizei nicht zugänglich wird – dann haben wir zu prüfen, ob wir die Vorsetzung des § 4 Absatz 1 Katalogtat erfüllt sehen und wenn nicht, dann können wir nach diesem Stand jetzt nicht weitergeben. Weil ja in den zwei Fallbeispielen – bei dem siebenjährigen Kind würde ich jetzt mal davon ausgehen, dass auch, nachdem wir noch weiter natürlich die Fallkonstellation ausgeschärft haben, wir eher bei einer Weitergabe sind – ja auch noch die mittelbare Täterschaft ein Thema ist, was man diskutieren kann. Bei dem Räuber muss man allerdings ganz genau hinschauen, sind jetzt die Voraussetzungen erfüllt oder sind sie nicht erfüllt? Das macht uns insofern auch noch Kopfzerbrechen, aber ich glaube, wir müssen in den nächsten Monaten hier auch noch sehr genau ausschärfen, was fällt denn nun unter diesen Katalog der EU-Richtlinie, die ja

hier genannt ist und was nicht? Das ist der eine Punkt.

Der zweite Punkt ist, wir werden auch in der Verifizierung hier und da noch Schwierigkeiten haben, weil nicht bei allen Ausschreibungen wir eben auch genau auf den Katalog stoßen werden. Das gilt auch für Ausschreibungen zur Einreiseverweigerung. Auch diese können ja auftauchen im Inner-Schengenverkehr, wenn eine Person sich in der EU aufhält, die sich eigentlich nicht hier aufhalten sollte. Auch hier ist dann wieder die Frage: Können wir den Ausschreibungsgrund erkennen und erfüllt er eine Katalogtat und sind wir in der Lage, dann diese Information weiterzugeben. Das ist natürlich etwas, was einem als Polizei schon Gedanken macht. Ja. Sie haben eine Information, die es wert ist, weiter bearbeitet zu werden, in der Hand, aber Sie können sie nicht weitergeben. Aber so lesen wir zurzeit den Gesetzentwurf und wir werden natürlich auch bis zum Inkrafttreten dann auch weiter ausschärfen müssen, wo sind die Grenzen, wo ist die Katalogtat erfüllt und wo nicht.

Frau Renner, dann zu Ihrer Frage. Ich habe natürlich hier nur mal zwei Beispiele genannt und einige, die noch aktiv sind, nicht. Es ist so, dass uns die Amerikaner insbesondere sagen, das Muster, das man einstellt – und es gibt da nur lebende Prinzipien – auf Basis des Täterverhaltens, das man erkennt aus Hinweisen, aus Verfahren, natürlich auch immer von den Tätern bemerkt werden, weil damit Kontrollen ausgelöst werden und das Verhalten sich wieder ändert und dann muss man die Muster wieder anpassen. Also insofern ist das ein lebendes Prinzip, um die Wahrscheinlichkeit eines Erfolges bei der Kontrolle zu erhöhen. Aber am Ende war es dann so bei den Fragen, die wir gestellt haben, die gingen ja immer um die Punkte: Wie sind die Prozesse zu gestalten? Welche Ressourcen muss ich einplanen und wie macht ihr das ganz praktisch? Da haben wir aus den Staaten keine Daten, wo wir am Ende sagen können: Für x Euro haben wir soundsoviel Treffer bei der Kontrolle. Das muss ich leider schuldig bleiben, aber am Ende muss man auch sagen: Wir sind dann ins Spiel gekommen und haben unsere Fragen gestellt, als es darum ging, eine EU-Richtlinie hier in Deutschland umzusetzen. Insofern ging es für uns darum, wie können wir das möglichst treffgenau und ressourcenschonend machen und da glauben wir schon, können wir von den Erfahrungen dieser Drittstaaten profitieren, weil das ja auch bei der Musterbildung dann darum geht, möglichst keine unnötigen Kontrollen am Ende auszulösen. Es muss ja auch unser Ziel sein. Soweit von mir dazu.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Münch. Herr Prof. Dr. Arzt, bitte.

SV **Prof. Dr. Clemens Arzt** (Hochschule für Wirtschaft und Recht Berlin): Vielen Dank. Jetzt muss ich Herrn Schuster und Frau Mihalic leider kurz stören, um auf die Frage antworten zu können. Ja, die Frage von Frau Mihalic ging dahin: Wie müsste eine gesetzliche Regelung aussehen, die bestimmt genug ist? Ja, dazu werde ich gerne mal ein paar Bachelor-Arbeiten bei mir im Fachbereich ausgeben.

Wenn ich die jetzige Regelung mir anschaue, dann heißt es im § 4 Absatz 3: Die Muster enthalten verdachtsbekundende und verdachtsentlastende Prüfungsmerkmale. Das ist natürlich eine spannende Formulierung, weil der Begriff des Verdachts aus der Strafprozessordnung kommt, wir hier aber Gefahrenabwehr ja betreiben sollen, nicht die Verhütung von Straftaten. Da passt der Begriff des Verdachtes schon gar nicht. Also wir haben schon, zumindest im geltenden Gesetz, keine hinreichende Bestimmtheit und Klarheit. Ich glaube, offen gestanden, Sie können sowas nicht beschreiben oder Sie müssten wirklich einen langen Katalog über irgendwie Verwaltungsvorschriften machen, die dann aber noch veröffentlicht werden müssen und das würden Sie gar nicht veröffentlichen wollen, weil Sie ja nicht wollen, dass die Außenwelt es weiß. Also wird man, glaube ich, andersrum da ran gehen müssen. Es war jetzt kein Petitum dafür, das alles geheim zu halten. Sondern man wird anders daran gehen müssen. Das Bundesverfassungsgericht stellt zur Rasterfahndung fest, Sie erlauben mir ein ganz kurzes Zitat? „Eine präventiv-polizeiliche Rasterfahndung“ und das ist das, was wir hier unter anderem haben, „ist mit dem Grundrecht auf informationelle Selbstbestimmung nur vereinbar, wenn eine konkrete Gefahr für hochrangige Rechtsgüter, wie Bestand oder Sicherheit des Bundes oder Landes oder Leib, Leben oder Freiheit einer Person gegeben ist. Im Vorfeld der Gefahrenabwehr scheidet eine solche Rasterfahndung aus. Im Vorfeld der

Gefahrenabwehr scheidet eine solche Rasterfahndung aus. Eine allgemeine Betreuungslage, wie sie im Hinblick auf terroristische Anschläge seit dem 11. September 2001 bestanden hat usw. reicht nicht aus. Vorausgesetzt ist vielmehr das Vorliegen weiterer Tatsachen, aus denen sich eine konkrete Gefahr, etwa für die Vorbereitung und Durchführung terroristischer Anschläge ergibt.“ Warum trage ich Ihnen das vor? Weil man aus meiner Sicht hieraus eindeutig erkennen kann: Wir können das nur über die Tatbestandsvoraussetzung letztendlich regeln. Also wir müssen oder man müsste sehr deutlich nachsteuern bei den Tatbestandsvoraussetzungen. Wann überhaupt hält man eine solche Maßnahme für zulässig? Da wird man dann, Herr Wollenschläger und ich, wahrscheinlich zu unterschiedlichen Ergebnissen kommen, zunächst mal bei der Betrachtung. Aber ich glaube, das wird eigentlich die einzige Variante sein, so machen wir das sonst auch. Also wir definieren über den Tatbestand, wann, in welchem Stadium darf der Staat hier eingreifen. Anders geht es, aus meiner Sicht nicht und das ist hier, aus meiner Sicht, bei weitem nicht gelungen. Die Tatbestandshürde ist soweit wie der Himmel über Berlin. Dankeschön.

Vors. **Ansgar Heveling** (CDU/CSU): Vielen Dank Herr Prof. Dr. Arzt. Mit diesem Schlusswort sind wir am Ende der Anhörung. Ich darf mich ganz herzlich bei den Herren Sachverständigen bedanken, dass Sie Ihre Einführungsstatements gehalten haben und Rede und Antwort gestanden haben. Vielen Dank an die Kolleginnen und Kollegen für Ihre Fragen. Ich schließe damit die 114. Sitzung des Innenausschusses und wünsche noch einen schönen Abend.

Schluss der Sitzung: 17:56 Uhr

Ansgar Heveling, MdB

Vorsitzender

STEPHAN MAYER
MITGLIED DES DEUTSCHEN BUNDESTAGES
INNENPOLITISCHER SPRECHER

CDU CSU Fraktion im Deutschen Bundestag

BURKHARD LISCHKA
MITGLIED DES DEUTSCHEN BUNDESTAGES
INNENPOLITISCHER SPRECHER

SPD BUNDESTAGS FRAKTION

An den Vorsitzenden des Innenausschusses
Herrn Ansgar Heveling MdB

Per E-Mail: INNENAUSSCHUSS@BUNDESTAG.DE

Berlin, 28. März 2017

Sehr geehrter Herr Vorsitzender,

für die Sitzung des Innenausschusses am 26. April 2017 übersenden wir zum „Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz - FlugDaG)" (Drucksache 18/11501) den anliegenden Änderungsantrag und bitten, diesen zur Beschlussfassung auf die Tagesordnung zu setzen.

Mit freundlichen Grüßen

Stephan Mayer MdB

Burkhard Lischka MdB

(7861)

Innenausschuss

Eingang mit Anl. am 28.3.2017
1. Vors. m.d.B. um Kenntnisnahme/Rücksprache
2. Mehrfertigungen mit/ohne Anschreiben an Abg. BE, Obl. Sekr.

an

3. Wv
4. z.d.A. [a]phab.-Gesetz- BMI)

POSTANSCHRIFT PLATZ DER REPUBLIK 1 11011 BERLIN WWW.CDUCSU.DE
BÜROANSCHRIFT WILHELMSTRASSE 60 10117 BERLIN
TELEFON (030) 227-74932 **TELEFAX** (030) 227-76781 **E-MAIL** STEPHAN.MAYER@BUNDESTAG.DE

POSTANSCHRIFT PLATZ DER REPUBLIK 1 11011 BERLIN WWW.SPDFRAKTION.DE
BÜROANSCHRIFT: JAKOB-KAISER-HAUS 10117 BERLIN
TELEFON (030) 227-71908 **TELEFAX** (030) 227-76908 **E-MAIL** BURKHARD.LISCHKA@BUNDESTAG.DE

Änderungsantrag

der Fraktionen CDU/CSU und SPD

für den Innenausschuss des Deutschen Bundestages

Zusammenstellung

des Entwurfs eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/681

– Drucksache 18/11501

mit den Beschlüssen des Innenausschusses (4. Ausschuss)

Entwurf	Beschlüsse des 4. Ausschusses
Gesetzentwurf der Bundesregierung	**Gesetzentwurf der Bundesregierung**
Entwurf eines Gesetzes *über die Verarbeitung von Fluggastdaten* zur Umsetzung der Richtlinie (EU) 2016/681	**Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/681**
(Fluggastdatengesetz – FlugDaG)[1)]	**entfällt**
Vom ...	**Vom ...**
Der Bundestag hat das folgende Gesetz beschlossen:	Der Bundestag hat das folgende Gesetz beschlossen:
	Artikel 1
	Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681
	(Fluggastdatengesetz – FlugDaG)[1)]

1) Dieses Gesetz dient der Umsetzung der Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (ABl. L 119 vom 4.5.2016, S. 132)

Entwurf	Beschlüsse des 4. Ausschusses
Abschnitt 1	**Abschnitt 1**
Fluggastdatenzentralstelle und Zweck des Fluggastdaten-Informationssystems	**unverändert**
§ 1	
Fluggastdatenzentralstelle und Zweck des Fluggastdaten-Informationssystems	
(1) Das Bundeskriminalamt ist nationale zentrale Stelle für die Verarbeitung von Fluggastdaten (Fluggastdatenzentralstelle). Die Fluggastdatenzentralstelle unterhält ein Fluggastdaten-Informationssystem nach Maßgabe dieses Gesetzes.	
(2) Das Fluggastdaten-Informationssystem dient der Verhütung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität.	
(3) Das Bundesverwaltungsamt verarbeitet Fluggastdaten im Auftrag und nach Weisung der Fluggastdatenzentralstelle.	

Entwurf	Beschlüsse des 4. Ausschusses
Abschnitt 2	**Abschnitt 2**
Übermittlung von Fluggastdaten an die Fluggastdatenzentralstelle	**unverändert**
§ 2	
Datenübermittlung durch Luftfahrtunternehmen	
(1) Luftfahrtunternehmen übermitteln nach Maßgabe des Absatzes 3 im Rahmen ihrer Geschäftstätigkeit erhobene Fluggastdaten von Fluggästen, einschließlich von Transfer- und Transitfluggästen, die von ihnen in einem Luftfahrzeug befördert werden oder befördert werden sollen, an die Fluggastdatenzentralstelle.	
(2) Fluggastdaten sind folgende Daten:	
1. Familienname, Geburtsname, Vornamen und Doktorgrad des Fluggastes,	
2. Angaben zum Fluggastdaten-Buchungscode,	
3. Datum der Buchung und der Flugscheinausstellung,	
4. planmäßiges Abflugdatum oder planmäßige Abflugdaten,	
5. Anschrift und Kontaktangaben, einschließlich Telefonnummer und E-Mail-Adresse,	
6. Flugscheindaten, einschließlich Flugscheinnummer, Ausstellungsdatum, einfacher Flug und automatische Tarifanzeige,	
7. vollständige Gepäckangaben,	

Entwurf	Beschlüsse des 4. Ausschusses
8. etwaige erhobene erweiterte Fluggastdaten (Advance Passenger Information-Daten), einschließlich Art, Nummer, Ausstellungsland und Ablaufdatum von Identitätsdokumenten, Staatsangehörigkeit, Familienname, Vorname, Geschlecht, Geburtsdatum, Luftfahrtunternehmen, Flugnummer, Tag des Abflugs und der Ankunft, Flughafen des Abflugs und der Ankunft, Uhrzeit des Abflugs und der Ankunft,	
9. sonstige Namensangaben,	
10. alle Arten von Zahlungsinformationen, einschließlich der Rechnungsanschrift,	
11. gesamter Reiseverlauf für bestimmte Fluggastdaten,	
12. Angaben zum Vielflieger-Eintrag,	
13. Angaben zum Reisebüro und zur Sachbearbeiterin oder zum Sachbearbeiter,	
14. Reisestatus des Fluggastes mit Angaben über Reisebestätigungen, Eincheckstatus, nicht angetretene Flüge und Fluggäste mit Flugschein, aber ohne Reservierung,	
15. Angaben über gesplittete und geteilte Fluggastdaten,	
16. allgemeine Hinweise, einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen unter 18 Jahren, wie beispielsweise Namensangaben, Geschlecht, Alter und Sprachen der oder des Minderjährigen, Namensangaben und Kontaktdaten der Begleitperson beim Abflug und Angabe, in welcher Beziehung diese Person zu der oder dem Minderjährigen steht, Namensangaben und Kontaktdaten der abholenden Person und Angabe, in welcher Beziehung diese Person zu der oder dem Minderjährigen steht, begleitende Flughafenmitarbeiterin oder begleitender Flughafenmitarbeiter bei Abflug und Ankunft,	

Entwurf	Beschlüsse des 4. Ausschusses
17. Sitzplatznummer und sonstige Sitzplatzinformationen,	
18. Angaben zum Code-Sharing,	
19. Anzahl und Namensangaben von Mitreisenden im Rahmen der Fluggastdaten und	
20. alle vormaligen Änderungen der unter den Nummern 1 bis 19 aufgeführten Fluggastdaten.	
(3) Fluggastdaten sind für alle Flüge des Linien-, Charter- und Taxiverkehrs zu übermitteln, die nicht militärischen Zwecken dienen und die	
1. von der Bundesrepublik Deutschland aus starten und in einem anderen Staat landen oder	
2. von einem anderen Staat aus starten und in der Bundesrepublik Deutschland landen oder zwischenlanden.	
(4) Bei Flügen mit Code-Sharing zwischen mehreren Luftfahrtunternehmen übermittelt dasjenige Luftfahrtunternehmen, das den Flug durchführt, die Fluggastdaten aller Fluggäste des Fluges an die Fluggastdatenzentralstelle.	
(5) Die Luftfahrtunternehmen haben die Fluggastdaten der Fluggastdatenzentralstelle nach Absatz 7 Satz 1 zu übermitteln:	
1. 48 bis 24 Stunden vor der planmäßigen Abflugzeit und	
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.	

Entwurf	Beschlüsse des 4. Ausschusses
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; 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.	
(6) Zusätzlich zu den in Absatz 5 genannten Zeitpunkten sind in Einzelfällen die Fluggastdaten auf Anforderung der Fluggastdatenzentralstelle unverzüglich zu übermitteln, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Begehung einer Straftat nach § 4 Absatz 1 unmittelbar bevorsteht, und dies zur Erfüllung der in § 6 Absatz 1 Satz 1 und Absatz 2 Satz 1 genannten Aufgaben erforderlich ist. Satz 1 gilt bei Ersuchen nach § 7 Absatz 3 Satz 1 Nummer 3 entsprechend.	
(7) Die Fluggastdaten werden elektronisch übermittelt. Bei der Übermittlung zu verwenden sind die gemeinsamen Protokolle und die unterstützten Datenformate, die jeweils festgelegt worden sind durch Durchführungsrechtsakte der Europäischen Kommission nach Artikel 16 Absatz 3 der Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (ABl. L 119 vom 4.5.2016, S. 132). Die Luftfahrtunternehmen teilen der Fluggastdatenzentralstelle mit, welches konkrete Protokoll und Datenformat für die Übermittlung der Fluggastdaten verwendet wird. Bei technischen Störungen erfolgt die Übermittlung der Fluggastdaten in Abstimmung mit der Fluggastdatenzentralstelle ausnahmsweise auf andere geeignete Weise, die ein angemessenes Datensicherheitsniveau gewährleistet.	

Entwurf	Beschlüsse des 4. Ausschusses
§ 3	
Datenübermittlung der durch andere Unternehmen erhobenen Fluggastdaten	
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.	

Entwurf	Beschlüsse des 4. Ausschusses
Abschnitt 3	**Abschnitt 3**
Verarbeitung von Fluggastdaten durch die Fluggastdatenzentralstelle	**unverändert**
§ 4	
Voraussetzungen für die Datenverarbeitung	
(1) Die Fluggastdatenzentralstelle verarbeitet die von den Luftfahrtunternehmen übermittelten Fluggastdaten und gleicht sie mit Datenbeständen und Mustern nach Maßgabe der Absätze 2 und 5 ab, um Personen zu identifizieren, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie eine der folgenden Straftaten begangen haben oder innerhalb eines übersehbaren Zeitraumes begehen werden:	
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,	

Entwurf	Beschlüsse des 4. Ausschusses
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 (EU) 2016/681 aufgeführten strafbaren Handlung entspricht und die mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht ist.	
(2) Ein automatisierter Abgleich von Fluggastdaten durch die Fluggastdatenzentralstelle ist vor der Ankunft eines Luftfahrzeuges auf einem Flughafen in der Bundesrepublik Deutschland oder vor dem Abflug eines Luftfahrzeuges von einem Flughafen der Bundesrepublik Deutschland zulässig	
1. mit Datenbeständen, die der Fahndung oder Ausschreibung von Personen oder Sachen dienen und	
2. mit Mustern	
(vorzeitiger Abgleich). Treffer, die aus einem vorzeitigen Abgleich resultieren, werden von der Fluggastdatenzentralstelle individuell überprüft.	

Entwurf	Beschlüsse des 4. Ausschusses
(3) Die Muster für den Abgleich nach Absatz 2 Satz 1 Nummer 2 werden von der Fluggastdatenzentralstelle unter Einbeziehung der oder des Datenschutzbeauftragten der Fluggastdatenzentralstelle erstellt und in Zusammenarbeit mit den in § 6 Absatz 1 Satz 1 und Absatz 2 Satz 1 genannten Behörden sowie mit der oder dem Datenschutzbeauftragten der Fluggastdatenzentralstelle regelmäßig, mindestens alle sechs Monate, überprüft. Die Muster enthalten verdachtsbegründende und verdachtsentlastende Prüfungsmerkmale. Verdachtsbegründende Prüfungsmerkmale beruhen auf den Tatsachen zu bestimmten Straftaten, die den in § 6 Absatz 1 Satz 1 oder Absatz 2 Satz 1 genannten Behörden vorliegen. Sie müssen geeignet sein, Personen zu identifizieren, die für die Verhütung oder Verfolgung der in Absatz 1 genannten Straftaten bedeutsame Prüfungsmerkmale erfüllen. Verdachtsentlastende Prüfungsmerkmale dienen dazu, Personen, die unter verdachtsbegründende Prüfungsmerkmale fallen, als Nichtverdächtige auszuschließen. Bei den Mustern sind verdachtsbegründende Prüfungsmerkmale mit verdachtsentlastenden Prüfungsmerkmalen so zu kombinieren, dass die Zahl der unter ein Muster fallenden Personen möglichst gering ist. Angaben zur rassischen oder ethnischen Herkunft, zu den politischen Meinungen, zu den religiösen oder weltanschaulichen Überzeugungen, zur Mitgliedschaft in einer Gewerkschaft, zum Gesundheitszustand, zum Sexualleben oder zur sexuellen Orientierung einer Person dürfen nicht Gegenstand eines Prüfungsmerkmals sein. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert die Erstellung und Anwendung der Muster mindestens alle zwei Jahre. Sie oder er erstattet der Bundesregierung alle zwei Jahre Bericht.	
(4) Die Fluggastdatenzentralstelle kann Fluggastdaten analysieren, um Muster für den vorzeitigen Abgleich zu erstellen oder zu aktualisieren.	

Entwurf	Beschlüsse des 4. Ausschusses
(5) 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.	
§ 5	
Depersonalisierung von Daten	
(1) Nach Ablauf von sechs Monaten ab Übermittlung der Fluggastdaten an die Fluggastdatenzentralstelle werden die Fluggastdaten durch Unkenntlichmachung der folgenden Datenelemente, mit denen die Identität einer Person nach § 2 Absatz 1 festgestellt werden könnte, von der Fluggastdatenzentralstelle depersonalisiert:	
1. Namensangaben nach § 2 Absatz 2 Nummer 1 und 9 sowie die Anzahl und die Namensangaben der erfassten Mitreisenden nach § 2 Absatz 2 Nummer 19,	
2. Anschrift und Kontaktangaben nach § 2 Absatz 2 Nummer 5,	
3. alle Arten von Zahlungsinformationen, einschließlich der Rechnungsanschrift, nach § 2 Absatz 2 Nummer 10, die zur Feststellung der Identität des Fluggastes oder anderer Personen beitragen könnten,	
4. Angaben zum Vielflieger-Eintrag nach § 2 Absatz 2 Nummer 12,	
5. allgemeine Hinweise nach § 2 Absatz 2 Nummer 16, die zur Feststellung der Identität des Fluggastes beitragen könnten und	

Entwurf	Beschlüsse des 4. Ausschusses
6. Daten nach § 2 Absatz 2 Nummer 8.	
(2) Die Aufhebung der Depersonalisierung von Fluggastdaten durch die Fluggastdatenzentralstelle ist nur zulässig, wenn die Aufhebung	
1. im Fall eines Abgleichs nach § 4 Absatz 5 Satz 1 zur Verhütung oder Verfolgung von Straftaten nach § 4 Absatz 1 erforderlich ist und	
2. auf Antrag der Leitung der Fluggastdatenzentralstelle oder deren Vertretung gerichtlich genehmigt worden ist.	
Bei Gefahr im Verzug kann die Präsidentin oder der Präsident des Bundeskriminalamtes oder ihre oder seine Vertretung die Genehmigung erteilen. Die gerichtliche Entscheidung ist unverzüglich nachzuholen. Die Sätze 1 bis 3 gelten mit Blick auf die in § 6 Absatz 2 Satz 1 genannten Behörden entsprechend mit der Maßgabe, dass die Aufhebung im Fall eines Abgleichs nach § 4 Absatz 5 Satz 2 zur Erfüllung von deren Aufgaben im Zusammenhang mit Straftaten nach § 4 Absatz 1 erforderlich ist.	
Abschnitt 4	**Abschnitt 4**
Übermittlung von Fluggastdaten durch die Fluggastdatenzentralstelle	**unverändert**
§ 6	
Datenübermittlung an die zuständigen Behörden im Inland	
(1) Soweit dies zur Erfüllung von deren Aufgaben zur Verhütung oder Verfolgung von Straftaten nach § 4 Absatz 1 erforderlich ist, kann die Fluggastdatenzentralstelle die aus einem Abgleich nach § 4 Absatz 2 oder Absatz 5 resultierenden Fluggastdaten und die Ergebnisse der Verarbeitung dieser Daten zur weiteren Überprüfung oder zur Veranlassung geeigneter Maßnahmen übermitteln an	

Entwurf	Beschlüsse des 4. Ausschusses
1. das Bundeskriminalamt,	
2. die Landeskriminalämter,	
3. die Zollverwaltung sowie	
4. die Bundespolizei.	
Die Übermittlung von Daten, die aus einem Abgleich nach § 4 Absatz 5 resultieren, an eine andere als an die ersuchende Behörde erfolgt nur im Einvernehmen mit der ersuchenden Behörde.	
(2) Soweit dies zur Erfüllung von deren Aufgaben im Zusammenhang mit Straftaten nach § 4 Absatz 1 erforderlich ist, kann die Fluggastdatenzentralstelle die aus einem Abgleich nach § 4 Absatz 2 oder Absatz 5 resultierenden Fluggastdaten und die Ergebnisse der Verarbeitung dieser Daten zudem übermitteln an	
1. das Bundesamt für Verfassungsschutz und die Verfassungsschutzbehörden der Länder,	
2. den Militärischen Abschirmdienst sowie	
3. den Bundesnachrichtendienst.	
Absatz 1 Satz 2 gilt entsprechend.	
(3) Die in Absatz 1 Satz 1 und Absatz 2 Satz 1 genannten Behörden dürfen die übermittelten Daten nur zu den Zwecken, zu denen sie ihnen übermittelt worden sind, verarbeiten.	
(4) 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.	

Entwurf	Beschlüsse des 4. Ausschusses
§ 7	
Datenaustausch zwischen den Mitgliedstaaten der Europäischen Union	
(1) Der Fluggastdatenzentralstelle obliegt der Austausch von Fluggastdaten und von Ergebnissen der Verarbeitung dieser Daten mit den Fluggastdatenzentralstellen anderer Mitgliedstaaten der Europäischen Union (Mitgliedstaat).	
(2) Die Fluggastdatenzentralstelle kann die Fluggastdatenzentralstelle eines anderen Mitgliedstaates aufgrund eines begründeten Ersuchens einer in § 6 Absatz 1 Satz 1 genannten Behörde ersuchen um	
1. Übermittlung von Fluggastdaten und von Ergebnissen der Verarbeitung dieser Daten, soweit dies zur Verhütung oder Verfolgung von Straftaten nach § 4 Absatz 1 erforderlich ist, oder	
2. Anforderung von Fluggastdaten bei Luftfahrtunternehmen und Übermittlung dieser Daten, soweit dies zur Verhütung einer unmittelbar bevorstehenden Straftat nach § 4 Absatz 1 erforderlich ist.	
Ein begründetes Ersuchen nach Satz 1 Nummer 1 kann bei Gefahr im Verzug auch durch eine Behörde nach § 6 Absatz 1 Satz 1 gestellt werden. Die Fluggastdatenzentralstelle ist nachrichtlich zu beteiligen. Die Sätze 1 bis 3 gelten mit Blick auf die in § 6 Absatz 2 Satz 1 genannten Behörden entsprechend mit der Maßgabe, dass	
1. die Übermittlung zur Erfüllung von deren Aufgaben im Zusammenhang mit Straftaten nach § 4 Absatz 1 erforderlich ist, und	
2. im Fall des Satzes 1 Nummer 2 die Begehung einer Straftat nach § 4 Absatz 1 unmittelbar bevorsteht.	

Entwurf	Beschlüsse des 4. Ausschusses
(3) Die Fluggastdatenzentralstelle kann Fluggastdaten und die Ergebnisse der Verarbeitung dieser Daten an die Fluggastdatenzentralstellen anderer Mitgliedstaaten übermitteln, wenn	
1. sich durch einen Abgleich nach § 4 Absatz 2 oder Absatz 5 oder durch eine Analyse von Fluggastdaten nach § 4 Absatz 4 herausstellt, dass die Daten zur Erfüllung der Aufgaben von Behörden anderer Mitgliedstaaten zur Verhütung oder Verfolgung von terroristischen Straftaten oder schwerer Kriminalität erforderlich sind,	
2. ein Ersuchen der Fluggastdatenzentralstelle eines anderen Mitgliedstaates vorliegt, aus dem sich tatsächliche Anhaltspunkte dafür ergeben, dass die Übermittlung zur Verhütung oder Verfolgung von terroristischen Straftaten oder schwerer Kriminalität erforderlich ist, oder	
3. ein Ersuchen der Fluggastdatenzentralstelle eines anderen Mitgliedstaates vorliegt, das auf Anforderung von Fluggastdaten bei Luftfahrtunternehmen und Übermittlung dieser Daten gerichtet ist und sich aus dem Ersuchen tatsächliche Anhaltspunkte dafür ergeben, dass die Übermittlung der Daten zur Verhütung einer unmittelbar bevorstehenden terroristischen Straftat oder einer unmittelbar bevorstehenden Straftat der schweren Kriminalität erforderlich ist.	

Entwurf	Beschlüsse des 4. Ausschusses
Die Übermittlung von Daten nach Satz 1 Nummer 1, die aus einem Abgleich nach § 4 Absatz 5 resultieren, erfolgt nur im Einvernehmen mit der um den Abgleich ersuchenden Behörde. In den Fällen des Satzes 1 Nummer 2 kann bei Gefahr im Verzug das Ersuchen auch durch eine zuständige Behörde eines anderen Mitgliedstaates gestellt werden, sofern sie nach Artikel 7 Absatz 3 der Richtlinie (EU) 2016/681 gegenüber der Europäischen Kommission benannt worden ist und diese Mitteilung durch die Europäische Kommission im Amtsblatt der Europäischen Union veröffentlicht wurde. Bei der Übermittlung von Daten aufgrund eines Ersuchens nach Satz 1 Nummer 2 gilt § 5 Absatz 2 entsprechend.	
(4) Die Fluggastdatenzentralstelle kann Fluggastdaten und die Ergebnisse der Verarbeitung dieser Daten, die ihr von den Fluggastdatenzentralstellen anderer Mitgliedstaaten übermittelt werden, verarbeiten und an die in § 6 Absatz 1 Satz 1 genannten Behörden übermitteln, wenn	
1. sich nach einer individuellen Überprüfung herausstellt, dass die Daten zur Erfüllung der Aufgaben dieser Behörden zur Verhütung oder Verfolgung von Straftaten nach § 4 Absatz 1 erforderlich sind, oder	
2. die Daten mittels eines begründeten Ersuchens nach Absatz 2 Satz 1 oder Satz 2 angefordert wurden und zur Erfüllung der Aufgaben dieser Behörden erforderlich sind.	
Die Übermittlung von Daten nach Satz 1 Nummer 2 an eine andere als an die ersuchende Behörde erfolgt nur im Einvernehmen mit der ersuchenden Behörde. Die Sätze 1 und 2 gelten mit Blick auf die in § 6 Absatz 2 Satz 1 genannten Behörden entsprechend mit der Maßgabe, dass die Übermittlung der Daten zur Erfüllung von deren Aufgaben im Zusammenhang mit Straftaten nach § 4 Absatz 1 erforderlich ist.	

Entwurf	Beschlüsse des 4. Ausschusses
(5) Die Vorschriften über die internationale Rechtshilfe in strafrechtlichen Angelegenheiten bleiben unberührt.	
§ 8	
Teilnahme an gemeinsamen Verfahren der Zusammenarbeit	
Die Fluggastdatenzentralstelle kann an gemeinsamen Verfahren der systematischen Zusammenarbeit mit anderen Fluggastdatenzentralstellen der Mitgliedstaaten der Europäischen Union zur Verhütung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität nach Maßgabe dieses Gesetzes teilnehmen. § 7 bleibt unberührt.	
§ 9	
Datenübermittlung an Europol	
Die Fluggastdatenzentralstelle kann Fluggastdaten und die Ergebnisse der Verarbeitung dieser Daten an Europol übermitteln, wenn ein Ersuchen von Europol vorliegt, aus dem sich tatsächliche Anhaltspunkte dafür ergeben, dass die Übermittlung zur Verhütung oder Verfolgung von terroristischen Straftaten oder schwerer Kriminalität durch Europol erforderlich ist. § 5 Absatz 2 gilt entsprechend.	
§ 10	
Datenübermittlung an Drittstaaten	
(1) Unter Beachtung der §§ 78 bis 80 des Bundesdatenschutzgesetzes kann die Fluggastdatenzentralstelle Fluggastdaten und die Ergebnisse der Verarbeitung dieser Daten im Einzelfall auf Ersuchen an die Behörden von Staaten, die nicht Mitgliedstaaten der Europäischen Union sind (Drittstaaten) übermitteln, wenn	

Entwurf	Beschlüsse des 4. Ausschusses
1. diese Behörden für die Verhütung oder Verfolgung von terroristischen Straftaten oder schwerer Kriminalität zuständig sind und die Datenübermittlung zu diesem Zweck erforderlich ist und	
2. sich diese Behörden verpflichten, die Daten nur dann an die Behörden eines anderen Drittstaates zu übermitteln, wenn dies zur Verhütung oder Verfolgung von terroristischen Straftaten oder schwerer Kriminalität erforderlich ist, und vor der Weiterübermittlung die Einwilligung der Fluggastdatenzentralstelle eingeholt wird.	
§ 5 Absatz 2 gilt entsprechend. Die Vorschriften über die internationale Rechtshilfe in strafrechtlichen Angelegenheiten bleiben unberührt.	
(2) Die Fluggastdatenzentralstelle kann die Fluggastdaten eines anderen Mitgliedstaates unter den Voraussetzungen des Absatzes 1 an die Behörden von Drittstaaten übermitteln, wenn die Fluggastdatenzentralstelle dieses Mitgliedstaates in die Übermittlung einwilligt. Liegt keine Einwilligung vor, ist die Übermittlung nur dann zulässig, wenn	
1. die Übermittlung erforderlich ist, um eine gegenwärtige Gefahr durch terroristische Straftaten oder schwere Kriminalität in einem Mitgliedstaat oder einem Drittstaat abzuwehren, und	
2. die Einwilligung nicht rechtzeitig eingeholt werden kann.	
Die für die Einwilligung nach Satz 2 zuständige Fluggastdatenzentralstelle ist unverzüglich zu unterrichten.	
(3) Die Fluggastdatenzentralstelle unterrichtet die Datenschutzbeauftragte oder den Datenschutzbeauftragten der Fluggastdatenzentralstelle über jede Datenübermittlung nach den Absätzen 1 und 2. Die Datenübermittlung nach Absatz 2 Satz 2 ist nachträglich durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten der Fluggastdatenzentralstelle zu überprüfen.	

Entwurf	Beschlüsse des 4. Ausschusses
Abschnitt 5	**Abschnitt 5**
Datenschutzrechtliche Bestimmungen	**Datenschutzrechtliche Bestimmungen**
§ 11	§ 11
Nationale Kontrollstelle	**unverändert**
Die Aufgaben der nationalen Kontrollstelle für den Datenschutz nimmt die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wahr.	
§ 12	§ 12
Die oder der Datenschutzbeauftragte der Fluggastdatenzentralstelle	**Die oder der Datenschutzbeauftragte der Fluggastdatenzentralstelle**
(1) Die Aufgaben der oder des Datenschutzbeauftragten der Fluggastdatenzentralstelle nimmt die oder der Datenschutzbeauftragte des Bundeskriminalamtes wahr.	(1) unverändert
(2) *Abweichend von § 72 Absatz 2 des Bundeskriminalamtgesetzes kann die* oder der Datenschutzbeauftragte der Fluggastdatenzentralstelle eine Angelegenheit an die nationale Kontrollstelle verweisen, wenn sie oder er eine Verarbeitung von Fluggastdaten für rechtswidrig hält.	(2) **Die** oder der Datenschutzbeauftragte der Fluggastdatenzentralstelle **kann** eine Angelegenheit an die nationale Kontrollstelle verweisen, wenn sie oder er eine Verarbeitung von Fluggastdaten für rechtswidrig hält.
§ 13	§ 13
Löschung von Daten	**unverändert**
(1) Fluggastdaten sind nach Ablauf von fünf Jahren ab ihrer Übermittlung an die Fluggastdatenzentralstelle durch die Fluggastdatenzentralstelle aus dem Fluggastdaten-Informationssystem zu löschen. Die Löschung von Fluggastdaten, die den in § 6 Absatz 1 Satz 1 oder Absatz 2 Satz 1 genannten Behörden übermittelt wurden, richtet sich nach den jeweiligen für diese Behörden geltenden Vorschriften.	

Entwurf	Beschlüsse des 4. Ausschusses
(2) Daten, die der Fluggastdatenzentralstelle von den Luftfahrtunternehmen übermittelt wurden und die nicht Fluggastdaten nach § 2 Absatz 2 sind, werden unverzüglich nach ihrem Eingang bei der Fluggastdatenzentralstelle durch die Fluggastdatenzentralstelle gelöscht.	
(3) Fluggastdaten nach § 2 Absatz 2, die Angaben zur rassischen oder ethnischen Herkunft, zu den politischen Meinungen, zu den religiösen oder weltanschaulichen Überzeugungen, zur Mitgliedschaft in einer Gewerkschaft, zum Gesundheitszustand, zum Sexualleben oder zur sexuellen Orientierung einer Person beinhalten, werden unverzüglich nach ihrem Eingang bei der Fluggastdatenzentralstelle durch die Fluggastdatenzentralstelle gelöscht.	
(4) Die Ergebnisse der Verarbeitung von Fluggastdaten sind durch die Fluggastdatenzentralstelle zu löschen, sobald sie nicht mehr erforderlich sind, um die in § 6 Absatz 1 Satz 1 oder Absatz 2 Satz 1 genannten Behörden, die Fluggastdatenzentralstellen anderer Mitgliedstaaten, Europol oder die Behörden von Drittstaaten zu informieren. Verarbeitungsergebnisse, die aus Analysen von Fluggastdaten resultieren, sind von der Fluggastdatenzentralstelle zu löschen, sobald sie nicht mehr für die Erstellung oder Aktualisierung von Mustern für den vorzeitigen Abgleich oder zur Information der Fluggastdatenzentralstellen anderer Mitgliedstaaten benötigt werden. Die Löschung von Ergebnissen der Verarbeitung von Fluggastdaten, die den in § 6 Absatz 1 Satz 1 oder Absatz 2 Satz 1 genannten Behörden übermittelt wurden, richtet sich nach den jeweiligen für diese Behörden geltenden Vorschriften.	
(5) Ergibt die individuelle Überprüfung nach § 4 Absatz 2 Satz 2 nach einem vorzeitigen Abgleich, dass kein Treffer vorliegt, so ist dieses Ergebnis spätestens dann zu löschen, wenn die dazugehörigen Daten nach Absatz 1 Satz 1 gelöscht werden.	

Entwurf	Beschlüsse des 4. Ausschusses
§ 14	§ 14
Protokollierung	**Protokollierung**
(1) *§ 76 des Bundesdatenschutzgesetzes gilt mit der Maßgabe, dass die Protokolle der oder dem Datenschutzbeauftragten der* Fluggastdatenzentralstelle *oder der nationalen Kontrollstelle in elektronisch auswertbarer Form für* die *Überprüfung der Rechtmäßigkeit der Datenverarbeitung zur Verfügung stehen.*	(1) **Die** Fluggastdatenzentralstelle **hat mindestens** die **folgenden Verarbeitungsvorgänge zu protokollieren:**
	1. Erhebung,
	2. Veränderung,
	3. Abfrage,
	4. Übermittlung und
	5. Löschung.
(2) *Abweichend von § 76 Absatz 3 des Bundesdatenschutzgesetzes dürfen die* Protokolle *ausschließlich für* die *Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch* die *Datenschutzbeauftragte oder den Datenschutzbeauftragten* der *Fluggastdatenzentralstelle sowie* die *nationale Kontrollstelle sowie für* die *Eigenüberwachung, für* die *Sicherstellung* der *Integrität und Sicherheit der personenbezogenen* Daten *und für Audits verwendet werden.*	(2) **Die** Protokolle **über Abfragen und Übermittlungen müssen es ermöglichen,** die **Begründung, das Datum** und die **Uhrzeit dieser Vorgänge und so weit wie möglich die Identität** der **Person,** die die **personenbezogenen Daten abgefragt oder übermittelt hat, und** die **Identität des Empfängers** der Daten **festzustellen.**
(3) Die *Protokolldaten sind fünf Jahre lang aufzubewahren* und *anschließend zu löschen.*	(3) Die **Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten der Fluggastdatenzentralstelle sowie die nationale Kontrollstelle sowie für die Eigenüberwachung, für die Gewährleistung der Integrität** und **Sicherheit der personenbezogenen Daten und für Audits verwendet werden.**
	(4) Die Protokolldaten sind fünf Jahre lang aufzubewahren und anschließend zu löschen.

Entwurf	Beschlüsse des 4. Ausschusses
	(5) Die Fluggastdatenzentralstelle hat die Protokolle der nationalen Kontrollstelle auf Anforderung zur Verfügung zu stellen.
	(6) Die Protokollierung erfolgt in einer Weise, dass die Protokolle der oder dem Datenschutzbeauftragten der Fluggastdatenzentralstelle oder der nationalen Kontrollstelle in elektronisch auswertbarer Form für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung zur Verfügung stehen.
§ 15	§ 15
Dokumentationspflicht	**unverändert**
(1) Die Fluggastdatenzentralstelle dokumentiert alle Verarbeitungssysteme und Verarbeitungsverfahren, die in ihre Zuständigkeit fallen.	
(2) Die Dokumentation enthält zumindest folgende Angaben:	
1. den 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,	
2. die Ersuchen von	
a) in § 6 Absatz 1 Satz 1 und Absatz 2 Satz 1 genannten Behörden,	
b) nach Artikel 7 Absatz 3 der Richtlinie (EU) 2016/681 benannten Behörden anderer Mitgliedstaaten,	
c) Fluggastdatenzentralstellen anderer Mitgliedstaaten und	
d) Europol sowie	

Entwurf	Beschlüsse des 4. Ausschusses
3. die Ersuchen von Behörden von Drittstaaten und jede Übermittlung von Fluggastdaten an Behörden von Drittstaaten.	
(3) Die Fluggastdatenzentralstelle stellt der nationalen Kontrollstelle auf Anfrage alle verfügbaren Dokumentationen zur Verfügung.	
Abschnitt 6	**Abschnitt 6**
Geltung des Bundeskriminalamtgesetzes	**unverändert**
§ 16	
Geltung des Bundeskriminalamtgesetzes	
Das Bundeskriminalamtgesetz findet entsprechende Anwendung, soweit in diesem Gesetz keine spezielleren Regelungen enthalten sind.	
Abschnitt 7	**Abschnitt 7**
Schlussvorschriften	**Schlussvorschriften**
§ 17	§ 17
Gerichtliche Zuständigkeit, Verfahren	**unverändert**
Für gerichtliche Entscheidungen nach diesem Gesetz ist das Amtsgericht zuständig, in dessen Bezirk das Bundeskriminalamt seinen Sitz hat. Für das Verfahren gelten die Bestimmungen des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.	

Entwurf	Beschlüsse des 4. Ausschusses
§ 18	§ 18
Bußgeldvorschriften	**unverändert**
(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.	
§ 19	§ 19
Inkrafttreten	**entfällt**
Dieses Gesetz tritt am 25. Mai 2018 in Kraft.	
	Artikel 2
	Änderung des Fluggastdatengesetzes
	§ 14 des Fluggastdatengesetzes vom ... [einsetzen: Datum der Ausfertigung sowie Fundstelle dieses Gesetzes] wird wie folgt gefasst:

Entwurf	Beschlüsse des 4. Ausschusses
	„§ 14
	Protokollierung
	(1) § 76 des Bundesdatenschutzgesetzes gilt mit der Maßgabe, dass die Protokolle der oder dem Datenschutzbeauftragten der Fluggastdatenzentralstelle oder der nationalen Kontrollstelle in elektronisch auswertbarer Form für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung zur Verfügung stehen.
	(2) Abweichend von § 76 Absatz 3 des Bundesdatenschutzgesetzes dürfen die Protokolle ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten der Fluggastdatenzentralstelle sowie die nationale Kontrollstelle sowie für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten und für Audits verwendet werden.
	(3) Die Protokolldaten sind fünf Jahre lang aufzubewahren und anschließend zu löschen.“
	Artikel 3
	Inkrafttreten
	(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach der Verkündung in Kraft.
	(2) Artikel 1 §§ 7 bis 10 und 18 sowie Artikel 2 treten am 25. Mai 2018 in Kraft.

Begründung

Zur Gesetzesbezeichnung (Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/681)

Aufgrund der Untergliederung des Gesetzentwurfs in insgesamt drei Artikel ist die Schaffung einer neuen Gesetzesbezeichnung aus rechtsförmlichen Gründen erforderlich.

Zu Artikel 1 (Fluggastdatengesetz)

Zu § 12 Absatz 2 (Die oder der Datenschutzbeauftragte der Fluggastdatenzentralstelle)

Mit der Änderung wird ein Redaktionsversehen korrigiert. Aufgrund der subsidiären Geltung des Bundeskriminalamtgesetzes nach § 16 ist der Verweis überflüssig. Zugleich wird ein Verweis auf das künftige Bundeskriminalamtgesetz, das erst am 25. Mai 2018 in Kraft treten wird, vermieden.

Zu § 14 (Protokollierung)

Durch die Änderung wird eine Regelung zur Protokollierung geschaffen, durch die ein Verweis auf das künftige Bundesdatenschutzgesetz, das erst am 25. Mai 2018 in Kraft treten wird, vermieden wird und zugleich die dortigen Vorgaben berücksichtigt. Die aktuelle Entwurfsfassung des § 14 soll dagegen am 25. Mai 2018 zeitgleich mit dem künftigen Bundesdatenschutzgesetz in Kraft treten (s. unten zu Artikel 2).

Zu § 19 (Inkrafttreten)

Die Regelung ist aufgrund des neu aufzunehmenden Artikels 3 überflüssig.

Zu Artikel 2 (Änderung des Fluggastdatengesetzes)

Die Aufnahme von Artikel 2 sowie die Änderung des § 14 (Protokollierung) sind erforderlich, um eine Anpassung des § 14 an das künftige Bundesdatenschutzgesetz, das am 25. Mai 2018 in Kraft treten wird, zu ermöglichen.

Zu Artikel 3 (Inkrafttreten)

Durch die Einfügung von Artikel 3 soll eine sukzessive Inbetriebnahme des Fluggastdaten-Informationssystems sowie eine stufenweise Anbindung der Luftfahrtunternehmen ab Inkrafttreten des Gesetzes ermöglicht werden. Die Regelungen zum europäischen und internationalen Datenaustausch sowie die Bußgeldvorschriften treten mit Blick auf die in der Richtlinie (EU) 2016/681 genannten Umsetzungsfrist am 25. Mai 2018 in Kraft. Gleiches gilt für Artikel 2, da das künftige Bundesdatenschutzgesetz ebenfalls zu diesem Zeitpunkt in Kraft treten wird.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)869 A

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Andrea Voßhoff
Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

POSTANSCHRIFT Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Postfach 1468, 53004 Bonn

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-100
TELEFAX (0228) 997799-550
E-MAIL arbeitsgruppe22@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 13.04.2017
GESCHÄFTSZ. **22-660/060#1688**

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

Vorsitzenden des Innenausschusses
des Deutschen Bundestages

Herrn Ansgar Heveling, MdB
ansgar.heveling@bundestag.de

Mitglied des Deutschen Bundestages
Herrn Stephan Mayer
stephan.mayer@bundestag.de

Mitglied des Deutschen Bundestages
Herrn Burkhard Lischka
burkhard.lischka@bundestag.de

Mitglied des Deutschen Bundestages
Frau Ulla Jelpke
ulla.jelpke@bundestag.de

Mitglied des Deutschen Bundestages
Frau Irene Mihalic
irene.mihalic@bundestag.de

Mitglied des Deutschen Bundestages
Herrn Clemens Binninger
clemens.binninger@bundestag.de

Mitglied des Deutschen Bundestages
Herrn Wolfgang Gunkel
wolfgang.gunkel@bundestag.de

17190/2017

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Mitglied des Deutschen Bundestages
Frau Martina Renner
martina.renner@bundestag.de

Mitglied des Deutschen Bundestages
Herrn Dr. Konstantin von Notz
konstantin.notz@bundestag.de

nachrichtlich:
innenausschuss@bundestag.de

11011 Berlin

BETREFF **Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz-FlugDaG)**

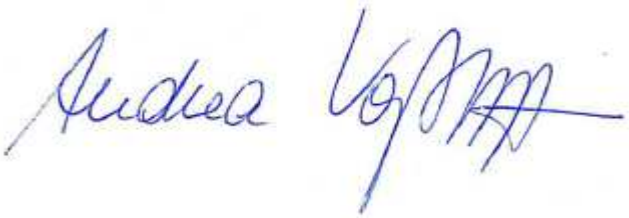
Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

anliegend sende ich Ihnen anlässlich der Anhörung des Innenausschusses zum Fluggastdatengesetz meine Stellungnahme zum Gesetzentwurf.

Ich wäre Ihnen und Ihren Kolleginnen und Kollegen im Ausschuss dankbar, wenn Sie die Stellungnahme bei Ihren Beratungen des Gesetzentwurfs berücksichtigten.

Meine Mitarbeiter und ich stehen gern für weitere Gespräche zur Verfügung.

Mit freundlichen Grüßen



Andrea Voßhoff

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 13.04.2017

Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Innenausschusses am 24. April 2017

zum

Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG)

BT-Drs 18/11501

Husarenstraße 30
53117 Bonn
Fon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de

Die Verarbeitung von sog. PNR-Daten zu Sicherheitszwecken kombiniert zwei grundsätzliche Probleme im Bereich des Datenschutzes im Sicherheitsbereich: PNR-Daten werden so genutzt, dass sämtliche Flugreisende mit abstrakt formulierten Gefährderprofilen („Mustern“) abgeglichen werden. Denn PNR-Daten sind nicht erforderlich, um bekannte Gefährder oder Straftäter bei der Grenzkontrolle zu fassen. Sie dienen dem **Generieren von Verdächtigen**, also dem Aufspüren von Reisenden, die eine **Gefahr darstellen könnten** und den Sicherheitsbehörden noch nicht bekannt sind. Gleichzeitig schafft die PNR-Richtlinie eine weitere Vorratsspeicherung von Daten, weil die Sicherheitsbehörden PNR-Daten verdachtslos über Jahre speichern.

Die Bewertung des Fluggastdatengesetzes darf zudem nicht isoliert von anderen Vorratsspeicherungen von Daten erfolgen. Das Bundesverfassungsgericht hat hierzu entschieden, dass „durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten […] der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer [wird]“ (Bundesverfassungsgericht, Urteil des Ersten Senats vom 2. März 2010, u.a.1 BvR 256/08 - Rn. 218).

Das Inkrafttreten des Fluggastdatengesetzes würde bedeuten, dass jährlich Fluggastdaten zu etwa 170 Millionen Passagieren in Deutschland unterschiedslos abgeglichen und über 5 Jahre gespeichert würden.

Im Hinblick auf den Gesetzentwurf begrüße ich, dass während der Ressortberatung verschiedene meiner Hinweise zur Umsetzung im Detail aufgenommen worden sind.

Auf der anderen Seite halte ich gerade mit Blick auf die wesentlichen Fragestellungen die abschließende Beratung des Fluggastdatengesetzes zum gegenwärtigen Zeitpunkt für verfrüht. Denn mit Spannung erwarten die Regierungen, das Europäische Parlament und die europäischen Datenschutzbehörden das **Gutachten des EuGH** zu einem **Abkommen mit Kanada**, das die Übermittlung von PNR-Fluggastdaten nach Kanada regelt und aller Voraussicht nach grundsätzliche Aussagen zur Vereinbarkeit der Verarbeitung von PNR-Daten mit der europäischen Grundrechtecharta treffen wird. Hieraus können sich erhebliche Auswirkungen auf die PNR-Richtlinie und ihre Umsetzung in deutsches Recht ergeben.

Das Fluggastdatengesetz sollte daher vor Veröffentlichung und Auswertung des EuGH-Gutachtens nicht verabschiedet werden.

1. In Erwartung des Gutachtens des EuGH zum PNR-Abkommen mit Kanada

Der Bundestag sollte das Fluggastdatengesetz nicht vor dem unmittelbar bevorstehenden Gutachten des EuGH zum PNR-Abkommen mit Kanada annehmen.

Die Umsetzungsfrist bis zum 25. Mai 2018 gibt dem deutschen Gesetzgeber die Zeit, das Gutachten des EuGH abzuwarten, das täglich erwartet wird.

Darin wird der EuGH seine Rechtsprechung zur Vorratsspeicherung von Daten und zur Anwendung dieser Rechtsprechung auf PNR-Daten konkretisieren. Nach den Schlussanträgen des Generalanwalts in dieser Rechtssache und nach dem Urteil des EuGH vom 21.12.2016 in der Rechtssache Tele2/Watson könnte der EuGH die Verarbeitung von PNR-Daten für Sicherheitszwecke nur dann mit der Grundrechtecharta für vereinbar halten, wenn sie weitergehende Beschränkungen enthält, als sie in der PNR-Richtlinie und dem Fluggastdatengesetz vorgesehen sind. So hat der EuGH eine Vorratsspeicherung von Daten nur dann für zulässig gehalten, wenn diese „gezielt" („targeted") erfolgt (EuGH, Urteil der Großen Kammer vom 21.12.2016, C-203/15, Rn. 108). Es bleibt abzuwarten, ob die Erfassung aller Flugpassagiere diesem Erfordernis gerecht wird.

In seiner Stellungnahme zum PNR-Abkommen macht Generalanwalt Mengozzi deutlich, dass die Vorgaben des EuGH aus „Digital Rights Ireland" und „Schrems" auch für die Speicherung von PNR-Daten gelten[1]. Folgt der EuGH der Stellungnahme des Generalanwalts, wird er das PNR-Abkommen mit Kanada in seiner jetzigen Form für rechtswidrig erachten, aller Wahrscheinlichkeit nach mit Auswirkungen auf die PNR-Richtlinie und deren Umsetzung in nationales Recht (etwa im Hinblick auf die generelle Erforderlichkeit, den PNR-Datensatz, die Speicherdauer oder den Abgleich mit „Mustern").

Vor diesem Hintergrund sehe ich auch den Änderungsantrag der Koalitionsfraktionen vom 28. März 2017 (A-Drs. 18(4)855) kritisch, das Inkrafttreten der wesentlichen Teile des Gesetzes vorzuziehen. Aus den dargestellten Gründen hielte ich es für vorzugswürdig, die Verabschiedung des Gesetzes zu verschieben, um eine Auswertung des EuGH-Gutachtens vor Verabschiedung zu ermöglichen.

2. Einbeziehung des innereuropäischen Flugverkehrs

Aus Verhältnismäßigkeitserwägungen ist es mindestens geboten, substantiiert darzulegen, warum intra-EU-Flüge einbezogen werden sollen und warum die Anwendbarkeit des Gesetzes nicht auf bestimmte EU-Flüge beschränkt werden kann.

Der nach langen Verhandlungen zur PNR-Richtlinie erreichte Kompromiss sieht vor, dass die Mitgliedstaaten nicht dazu verpflichtet sind, sämtliche innereuropäischen

[1] Schlussanträge des Generalanwalts Paolo Mengozzi vom 8. September 2016, Gutachten 1/15, Rn. 7.

Flüge in den nationalen PNR-Systemen zu erfassen. Die PNR-Richtlinie räumt den Mitgliedstaaten allerdings die Möglichkeit hierzu ein. Daneben eröffnet sie die Möglichkeit, nur näher zu bestimmende innereuropäische Flüge zu erfassen (Art. 2 Abs. 1 und 3 PNR-Richtlinie).

Mit diesem Umsetzungsspielraum setzt sich der Gesetzentwurf nicht hinreichend auseinander. Nach dem Fluggastdatengesetz sollen alle innereuropäischen Flüge einbezogen werden. In seiner Begründung beschränkt sich der Entwurf dabei auf den Hinweis, dass Sicherheitslücken zu schließen seien und dass eine effektive Bekämpfung von Terrorismus und schwerer Kriminalität die Einbeziehung erforderlich mache. Es wird nicht begründet, warum eine Beschränkung auf ausgewählte EU-Flüge aus Sicht der Bundesregierung unzureichend wäre.

Dabei weise ich darauf hin, dass die Einbeziehung von innereuropäischen Flügen die Anzahl der erfassten Passagiere um über 100 Millionen von 68 Millionen auf 170 Millionen anhebt (basierend auf den Zahlen von Eurostat für das Jahr 2015)[2].

3. Kontrolle der Muster

Ob vorgesehene Abgleiche mit den Mustern mit der Grundrechtecharta vereinbar sind, ist noch nicht geklärt. Darin sehe ich einen weiteren Grund, das EuGH-Gutachten abzuwarten. Außerdem sollte die Möglichkeit der Berichterstattung der BfDI auch an den Bundestag in dem Gesetz klargestellt werden.

Wesentliche Neuerung im Instrumentarium der Sicherheitsbehörden ist durch das Fluggastdatengesetz der Abgleich aller Passagierdaten mit sog. „Mustern“ gem. § 4 Abs. 3 FlugDaG-E, also nicht mit bestehenden Dateien der Sicherheitsbehörden, sondern mit abstrakten, für diesen Zweck erstellten **„Gefährderprofilen“**. Die Konferenz der Datenschutzbeauftragten von Bund und Ländern hat in ihrer Entschließung vom 16./17. März 2011 deutlich gemacht, dass sie diesem Konzept skeptisch gegenübersteht[3].

Ungeachtet dessen hat der deutsche Gesetzgeber die Vorgaben der PNR-Richtlinie gänzlich umzusetzen, soweit sie nicht gegen höherrangiges EU-Recht verstoßen. Ob dies der Fall ist bzw. unter welchen Voraussetzungen dies mit Art. 8 EU-Grundrechtecharta vereinbar ist, wird der EuGH aller Voraussicht nach in seinem Gutachten zum PNR-Abkommen mit Kanada entscheiden. Auch dies spricht dafür, das Gesetz noch nicht zu verabschieden.

[2] http://ec.europa.eu/eurostat/statistics-explained/index.php/Air_transport_statistics

[3] Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2011

Der Gesetzentwurf sieht darüber hinaus eine Verpflichtung der BfDI vor, die Erstellung und Anwendung der Muster, also der abstrakten Gefährderprofile, mindestens alle zwei Jahre zu überprüfen und einen **Bericht** hierüber **an die Bundesregierung** zu erstatten. Meines Erachtens folgt aus den allgemeinen Regelungen für die BfDI, dass der Bericht zusätzlich auch an den **Bundestag** gerichtet werden kann. Ich rege an, eine entsprechende **Klarstellung** zumindest in die Begründung aufzunehmen.

4. Nutzung der PNR-Daten bleibt zu unbestimmt

Ich halte es aus Gründen der Bestimmtheit für erforderlich, in einem Straftatenkatalog konkret und abschließend zu formulieren, für welche Straftaten die PNR-Daten genutzt werden dürfen. Insbesondere § 4 Abs. 1 Nr. 6 FlugDaG-E genügt diesen Anforderungen nicht.

Im Fluggastdatengesetz sollte festgelegt werden, zur Verhütung und Verfolgung welcher Straftaten PNR-Daten genutzt werden dürfen. Insbesondere in § 4 Abs. 1 Nr. 6 zieht sich das Gesetz auf die Benennung abstrakter Straftaten zurück, wie sie im Anhang zur PNR-Richtlinie aufgeführt sind. Damit konkretisiert das Gesetz die Vorgaben des europäischen Gesetzgebers auf nationaler Ebene nicht. Diese Unbestimmtheit halte ich rechtstaatlich für zweifelhaft. Die erforderliche **Konkretisierung** ist Aufgabe des Gesetzgebers.

5. Keine Rechtssicherheit für die Fluggesellschaften hinsichtlich der Rechtsgrundlage

Der Gesetzgeber sollte aus Gründen der Rechtssicherheit für Luftverkehrsunternehmen eine ausdrückliche Rechtsgrundlage für die Übermittlung von PNR-Daten an andere PNR-Zentralstellen in der EU schaffen.

Die Datenschutzbehörden haben in der Vergangenheit eine Übermittlung von PNR-Daten an andere Staaten, vornehmlich Drittstaaten, aber auch das Vereinigte Königreich für unzulässig erachtet. Es fehle für diese Übermittlungen an einer Rechtsgrundlage.

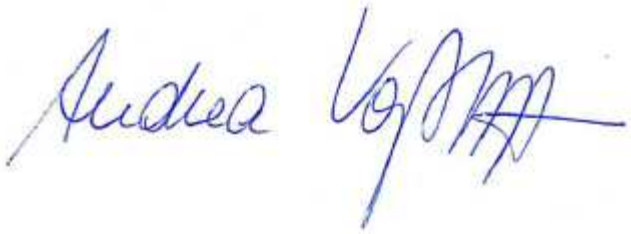
Da sämtliche Mitgliedstaaten, soweit bekannt, von der in der PNR-Richtlinie eingeräumten Möglichkeit Gebrauch machen, PNR-Daten auch von Flügen innerhalb der EU zu erheben, stellt sich die Frage, ob für die Übermittlung von PNR-Daten durch ein deutsches Luftverkehrsunternehmen an die Fluggastdatenzentrale eines anderen Mitgliedstaats eine spezifische Rechtsgrundlage erforderlich ist. Beispiel: Ein deut-

sches Luftverkehrsunternehmen wird ersucht, PNR-Daten an die französische Fluggastdatenzentrale zu übermitteln.

Das Fluggastdatengesetz schafft keine spezifische Rechtsgrundlage für die genannten Übermittlungen. In der Begründung des Gesetzes weist die Bundesregierung darauf hin, die Europäische Kommission halte eine Schaffung nicht für erforderlich. Sie gefährde gar eine einheitliche Umsetzung der PNR-Richtlinie in den Mitgliedstaaten.

Diese Auffassung teile ich nicht. Das Gesetz schafft in § 2 eine Rechtsgrundlage für Übermittlungen an die deutsche Fluggastdatenzentrale, nicht aber für die **Übermittlung an Fluggastdatenzentralen anderer Mitgliedstaaten**. Sofern keine ausdrückliche Vorschrift für diesen Fall geschaffen wird, kommt daher nur die die PNR-Richtlinie umsetzende Rechtsvorschrift des anderen Mitgliedstaates als Rechtsgrundlage in Betracht oder eine allgemeine Vorschrift der Datenschutz-Grundverordnung. Beides halte ich für rechtlich problematisch: Die erste Variante würde bedeuten, dass eine Rechtsvorschrift eines anderen Mitgliedstaates die Rechtsgrundlage für die Übermittlung an eine Fluggastzentrale eines anderen Mitgliedstaates wäre. Zweifel sind auch angebracht, ob die Vorschriften des § 6 Datenschutz-Grundverordnung eine hinreichende Rechtsgrundlage darstellt. Daher schafft das Gesetz nicht die erforderliche Rechtssicherheit für die Luftverkehrsunternehmen.

Bonn, April 2017



Andrea Voßhoff

DIGITALE GESELLSCHAFT.DE

Digitale Gesellschaft e.V.
Singerstraße 109
10179 Berlin

+49 30 97894230

info@digitalegesellschaft.de
www.digitalegesellschaft.de
@digiges

Berlin, den 20.04.17

Stellungnahme des Digitale Gesellschaft e.V. zum Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681

(Fluggastdatengesetz – FlugDaG)

Zu dem vorliegenden Entwurf nehmen wir wie folgt Stellung:

Vorbemerkung:

Als Reaktion auf terroristische Anschläge und organisierte, grenzüberschreitende Kriminalität wurde die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität auf den Weg gebracht.

Ziel ist es, durch die Einführung einer Vorratsdatenspeicherung von Fluggastdaten, nicht nur bekannte, sondern auch „bisher unbekannte Verdächtige“[1] zu identifizieren. Hierfür wird eine Fluggastdatenzentralstelle die von den Luftfahrtunternehmen übermittelten PNR-Daten mit bestehenden Datenbeständen und Mustern abgleichen. Jene Muster werden auch aus den zuvor übermittelten PNR-Daten erstellt und aktualisiert. Sowohl die PNR-Daten als auch die Ergebnisse der Verarbeitung dieser Daten können an das Bundeskriminalamt, die Landeskriminalämter, die Zollverwaltung, die Bundespolizei, das Bundesamt für Verfassungsschutz sowie die Verfassungsschutzbehörden der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst weitergeleitet werden. Zudem können die PNR-Daten als auch die Ergebnisse an andere Mitgliedstaaten der Europäischen Union, Europol sowie Drittstaaten übermittelt werden.

Die Speicherung und Auswertung von PNR-Daten erfolgt mittlerweile in einigen Staaten. Nationale PNR-Systeme gibt es etwa in Großbritannien, Schweden und Frankreich. Zudem bestehen Abkommen zur Übermittlung von Fluggastdaten zwischen der EU und den USA sowie Australien. Obwohl diese Staaten seit mehreren Jahren PNR-Daten im Kampf gegen Terrorismus und organisierte Kriminalität nutzen, gibt es keinen konkreten Nachweis dafür, dass eine Fluggastdatenspeicherung für die Bekämpfung von organisierter Kriminalität und Terrorismus ein taugliches Mittel wäre. Zugleich ist der Eingriff in die Grundrechte der Reisenden massiv: Die PNR-Daten von allen Reisenden auf Flügen, die zwischen den Mitgliedstaaten der EU durchgeführt werden als auch die von einem Mitgliedstaat der Europäischen Union aus in einen Drittstaat oder von einem Drittstaat aus in einen Mitgliedstaat der Europäischen Union starten, werden für fünf Jahre auf Vorrat gespeichert und verarbeitet, ohne das ein konkreter Tatverdacht vorliegt. Die PNR-Daten berühren zudem in ihrer Gesamtheit den Bereich des Privatlebens und lassen Rückschlüsse auf das Intimleben der Reisenden zu. Die Speicherung und Verarbeitung von PNR-Daten widerspricht damit Europäischen Grundrechten (Art. 7 und Art. 8 Charta).

Im Einzelnen:

Datenübermittlung

Zunächst ist anzumerken, dass im Entwurf des FlugDaG vorgesehen ist, dass die Fluggastdaten für alle Flüge, die von der Bundesrepublik Deutschland aus starten und

1 KOM(2011) 32 endgültig, S.4

in einem anderen Staat landen oder von einem anderen Staat aus starten und in der Bundesrepublik Deutschland landen oder zwischenlanden, gespeichert und ausgewertet werden. Die Anwendung der Richtlinie auf innereuropäische Flüge ist in der Richtlinie nicht verpflichtend vorgeschrieben. Das Ausdehnen der Richtlinie auf innereuropäische Flüge wird in der Begründung des Gesetzes damit erklärt, dass Täter und Tätergruppierungen im Bereich schwere Kriminalität und internationalem Terrorismus häufig Reiserouten innerhalb der Europäischen Union nutzen würden. Inwieweit Flugreisen dabei eine Rolle spielen und inwieweit die Erhebung und Auswertung von PNR-Daten nützlich sein kann, bleibt jedoch offen. Seitens der Europäischen Institutionen wird die Auswertung von Reisedaten innereuropäischer Flüge als nicht notwendig betrachtet, da diese nicht vorgeschrieben ist. Die lapidare Begründung, dass die angesprochenen Täter und Tätergruppierungen innereuropäische Reiserouten nutzen, erfüllt die Anforderungen an ein evidenzbasiertes Sicherheitskonzept nicht.

Unklar bleibt darüber hinaus, warum die in §2 (2) angeführten Daten, die durch die Luftfahrtunternehmen zu übermitteln sind, nötig sind, um den Zielen der Richtlinie gerecht zu werden. Die Daten berühren in ihrer Gesamtheit den Bereich des Privatlebens und lassen Rückschlüsse auf das Intimleben der Reisenden zu. Neben Informationen zu Kontaktdaten wie E-Mail-Adresse, Telefonnummer und Anschrift finden sich etwa auch Informationen über Mitreisende oder Zahlungsinformationen in den PNR-Daten. Unklar ist, welche Informationen in dem Datenfeld 16 „allgemeine Hinweise" gespeichert und verarbeitet werden. In diesem Freifeld können umfassende, darunter auch sensible Informationen, über die Reisenden gespeichert werden. Da es sich um ein Freifeld handelt, können diese Informationen auch nicht automatisiert gelöscht werden, sodass im Vorfeld der Speicherung und Auswertung der Daten sensible Informationen händisch gelöscht werden müssen. Die Erfahrungen[2] der australischen Behörden bei dem automatisierten Filtern und Löschen sensibler Daten in Bezug auf das Freifeld zeigen, dass hier ein enormer Arbeitsaufwand droht. Die Vorgaben aus §13 (3) FlugDaG dürften daher nur schwer zu erfüllen sein, zumindest fehlt jedoch ein Hinweis im Gesetz oder der Begründung, wie dieses Problem gelöst werden soll. Eine Begründung, warum diese Informationen notwendig sind und nicht etwa die

2 SWD(2014) 236 final, S.9

Auswertung und Speicherung von API-Daten ausreichend wäre, bleibt der Gesetzgeber schuldig. Ebenso bleibt unklar, wie die übermittelten Daten verifiziert werden können. Luftfahrtunternehmen sammeln und speichern PNR-Daten, um den reibungslosen Ablauf der Reise gewährleisten zu können. Neben verschiedenen internen Fehlerquellen, die zu falschen Angaben in einem PNR-Datensatz führen können, besteht zudem die Möglichkeit, durch Angriffe auf das System oder Hacks die Daten zu manipulieren und zu verfälschen. Sollten dabei Fehler auftreten, ist dies zwar ärgerlich für die Reisenden, jedoch drohen keine ernsthaften Konsequenzen. Wenn jedoch ein PNR-Datensatz mit falschen Informationen den Ermittlungsbehörden zur Verfügung gestellt wird, können daraus massive Einschnitte in die Grundrechte für die Betroffenen resultieren.

Datenverarbeitung

Die Fluggastdatenzentralstelle kann die Fluggastdaten automatisch mit Datenbeständen, die der Fahndung oder Ausschreibung von Personen oder Sachen dient, abgleichen. Hinzu kommt der Abgleich mit Mustern. Jene Muster werden von der Fluggastdatenzentrale aus den zuvor übermittelten Fluggastdaten selbst erstellt. Durch diese Profiling-Maßnahme sollen verdachtsbegründende und verdachtsentlastende Prüfungsmerkmale so miteinander kombiniert werden, „dass die Zahl der unter ein Muster fallenden Personen möglichst gering ist". Schon durch diese Formulierung wird ein massives Problem offensichtlich: Unbescholtene Bürgerinnen und Bürger können durch diese Profiling-Maßnahme in das Visier von Ermittlungsbehörden geraten. Im Rahmen der CeBIT wurde das technische System vorgestellt, mit dem die Datenanalyse durchgeführt werden soll. Am Ende der Analyse sollen 0,07% der Datensätze an die Ermittlungsbehörden weitergeleitet werden. Pro Jahr ist demnach mit über 100.000 Datensätzen zu rechnen, die durch die Profiling-Maßnahme entstehen. Zwar ist vorgesehen, dass die Treffer, die aus dieser Maßnahme resultieren, durch die Fluggastdatenzentrale individuell überprüft werden, jedoch gehen damit weitere Überwachungsmaßnahmen und Eingriffe in die Grundrechte der Betroffenen einher. Auch an dieser Stelle findet sich keine Begründung, warum nicht mehr oder weniger Datensätze überprüft werden müssen. Die Maßnahme, als auch ihr Ausmaß, werden allein auf Anekdoten gestützt, wirken willkürlich und entbehren jeder fachlichen Begründung.

Ein Blick in andere Staaten zeigt zudem, dass durch die Analyse von Reisedaten mit dem Ziel der Bekämpfung von schwerer Kriminalität und Terrorismus auch immer

wieder unbescholtene Bürger massive Einschränkungen ihrer Grundrechte in Kauf nehmen müssen. Die No Fly List der USA verdeutlicht die Problematik: Senatoren, Journalisten, Künstler aber auch Kinder landen immer wieder auf diesen Listen und werden an ihrer Reisefreiheit gehindert und mit massiven Überwachungsmaßnahmen konfrontiert. Mit solchen „false postive alerts" ist bei jeder Profiling-Maßnahme, wie sie auch im FlugDaG vorgesehen ist, zu rechnen. Problematisch bei einer algorithmischen Auswertung der PNR-Daten ist zudem, dass die Muster selbst diskriminierend sind, da verdachtsbegründende und verdachtsentlastende Prüfungsmerkmale vorgegeben werden. Ebenso muss davon ausgegangen werden, dass Personen, die tatsächlich in Verbindung mit schweren Straftaten oder Terrorismus stehen, durch die Datenanalyse nicht gefunden werden können.

Speicherdauer

Erst nach fünf Jahren werden die PNR-Daten gelöscht. In dieser Zeit können sie, teilweise mit Einschränkungen, vollständig abgerufen und ausgewertet werden. Zudem werden sie in dieser Zeit auch für die Erstellung der Muster genutzt. Unklar ist bis zum heutigen Tag warum die Speicherdauer auf fünf Jahre festgeschrieben wurde. Erneut fehlt jegliche Grundlage, die eine Speicherdauer von fünf Jahren rechtfertigen würde. Die Speicherdauer kann damit weder als verhältnismäßig noch als angemessen bezeichnet werden.

Weitergabe

Die PNR-Daten als auch die gewonnenen Erkenntnisse können im Inland an das Bundeskriminalamt, die Landeskriminalämter, die Zollverwaltung, die Bundespolizei, das Bundesamt für Verfassungsschutz sowie die Verfassungsschutzbehörden der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst weitergeleitet werden. Zudem können die PNR-Daten als auch die Ergebnisse an andere Mitgliedstaaten der Europäischen Union, Europol sowie Drittstaaten übermittelt werden. Durch die Weitergabe der Daten ist es nahezu unmöglich zu überprüfen, wie die entgegennehmenden Behörden

und Einrichtungen im folgenden mit den Daten umgehen und inwiefern sich diese an die Vorgaben aus dem FlugDaG halten. Es droht ein unübersichtliches und unkontrollierbares Netz von Datensilos zu entstehen.

Missbrauchspotential

Über 170 Millionen Passagiere reisen jährlich in Deutschland im Luftverkehr, Tendenz steigend. Die Daten von all jenen Passagieren werden für fünf Jahre in einer Datenbank gespeichert und mit anderen Behörden und Einrichtungen weltweit geteilt, auf die eine unbestimmte Anzahl von Personen Zugriff hat. Auch hier zeigt ein Blick auf das EU-USA Fluggastdatenabkommen, dass der Kreis der Zugriffsberechtigten schnell unüberschaubar werden kann. Über 14.000 DHS-Officers haben dort Zugriff auf die Datensätze.[3] Allein die Datensätze, die in der Bundesrepublik Deutschland zu speichern sind, werden in kürzester Zeit die Milliardengrenze sprengen. Zwar soll ein „modernes Zugriffs- und Berechtigungsmanagement" vor Missbrauch sowie ein „angemessenes Datensicherheitsniveau" vor unbefugten Zugriffen schützen, jedoch dürfte die Datensammlung große Begehrlichkeiten erwecken. Wer Zugriff auf die Daten hat, kann sich über das Intimleben von Millionen Reisenden informieren. Zudem können die Daten leicht für andere als im FlugDaG vorgeschriebene Anwendungsbereiche, wie etwa Wirtschaftsspionage, missbraucht werden.

Fazit:

Das FlugDaG schreibt eine verdachtsunabhängige und anlasslose Vorratsdatenspeicherung von Reisedaten ohne Beweis für den Nutzen der Datensammlung vor. Ziel der geplanten Massenüberwachung des europäischen Reiseverkehrs ist vorgeblich die Bekämpfung von Terrorismus und schwerer Kriminalität. Bislang fehlt es aber an jeglichen konkreten Nachweisen dafür, dass eine Fluggastdatenspeicherung für diesen Zweck ein taugliches Mittel wäre. Ganz im Gegenteil konnten sich beispielsweise die Mordanschläge von Paris im Januar und November 2015 ereignen, obwohl Frankreich bereits seit 2006 über Überwachungsinstrumente wie die Vorratsdatenspeicherung von Kommunikations- und Fluggastdaten verfügt. Die Attentäter befanden sich sogar schon lange vor den Anschlägen fast allesamt auf dem Radar der Behörden und konnten trotzdem ungehindert kreuz und quer durch Europa und in den Nahen Osten reisen. Gerade angesichts dieser behördlichen Versäumnisse leuchtet es nicht ein, die bereits

3 SWD(2017) 14 final, S.13

vorhandenen Datenberge weiter zu vergrößern und die Suche nach der Nadel im Heuhaufen damit noch schwieriger zu gestalten. Durch die Architektur des dezentralen Systems mit Passenger Information Units in jedem Mitgliedstaat der EU – in Deutschland in Form der Fluggastdatenzentralstelle – droht das bisherige Kommunikationsproblem zwischen den europäischen Ermittlungsbehörden weiter verschärft zu werden.

Mit der Richtlinie EU 2004/82 besteht bereits eine Maßnahme zur Übermittlung von Fluggastdaten. Eine Begründung, warum diese nicht ausreicht bzw. warum eine Reform dieser Richtlinie nicht geeigneter sein könnte, um die in dem FlugDaG genannten Ziele zu erreichen, bleibt der Gesetzgeber schuldig.

Zudem droht bereits jetzt die Ausweitung des Systems. Ein Blick nach Belgien zeigt, dass die heute zur Debatte stehende Fluggastdatenspeicherung schon morgen auch auf andere Verkehrsmittel ausgeweitet werden könnte. Es droht damit eine Total-Überwachung des Reiseverkehrs. Die Räume, in denen sich Menschen unbeobachtet vom Staat bewegen und entfalten können, werden zunehmend enger.

Die Urteile des Europäischen Gerichtshofs zur Vorratsdatenspeicherung von Kommunikationsdaten lassen zudem den Schluss zu, dass es sich bei dieser Maßnahme ebenfalls um eine grundrechtswidrige Überwachung handelt. Zur Zeit überprüft der EuGH zudem das EU-Kanada-PNR Abkommen. Die Entscheidung des EuGH sollte zumindest abgewartet werden, um nicht erneut Gesetze zu verabschieden, die die Grundrechte der Bürgerinnen und Bürger missachten.

SITA

SITA Information Networking Computing B.V.
Zweigniederlassung Eschborn
Ludwig-Erhard-Strasse 30-34
65760 Eschborn
Germany

Matthias Knetsch
Direktor SITA
Government and Lufthansa Group

matthias.knetsch@sita.aero

Telephone
+49 (0) 6196 970 400

Fax
+49 (0) 6196 970 444

An den Vorsitzenden des Innenausschusses
des Deutschen Bundestages

Herrn Ansgar Heveling, MdB

Deutscher Bundestag
Platz der Republik 1
11011 Berlin

21.04.2017

SITA Stellungnahme
Zum Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtline (EU) 2016/681 (Fluggastdatengesetz – FlugDaG)

Im April 2016 wurde die EU-Richtlinie 2016/681 (Fluggastdatengesetz - FlugDaG) zur Verwendung von PNR (*Passenger Name Record*) Daten verabschiedet, die 2-Jahres-Frist zur Umsetzung in nationales Recht hat bereits begonnen und wird mit dem vorliegendem Gesetzgebungsvorhaben angestrebt. Bis Mai 2018 soll sichergestellt werden, dass ein komplexes System erfolgreich implementiert wird, welches ermöglicht, Reisebewegungen von Terroristen und Schwerkriminellen mittels Erfassung von Daten nachzuvollziehen und damit Sicherheitsbehörden besser in die Lage zu versetzen, terroristische Straftaten aufzudecken und präventiv zu verhindern.

Neben einer technischen Lösung zur Erfassung und Verarbeitung der Daten (z.B. Risikoanalyse, Weiterleitung der Daten an EU Mitgliedsstaaten oder interne Behörden und Organisationen etc.) gilt es auch gerade die Organisation der geforderten PIU (Passenger Information Unit) vorab zu planen und zu strukturieren, als auch im ersten Schritt die rechtlichen Rahmenbedingungen so zu formulieren, dass heutige Möglichkeiten und zukünftige Entwicklungen effizient und zeitgemäß umgesetzt werden können.

Bei allen Bemühungen um die genannten Standards kann nicht von einem reibungslosen und einfachen Datenaustausch ausgegangen werden. So können bei weitem noch nicht alle Fluglinien den PNRGOV Standard umsetzen, oder benutzen dabei verschiedene Versionen und Varianten. Das wird sich auch nicht in Kürze ändern lassen. Deutschland sollte daher in Betracht ziehen, zumindest vorübergehend, weitere Formate zuzulassen.

In jedem Fall ist aus technischer Sicht von Änderungen am Datenumfang abzuraten. Dies würde zu erheblichen Verzögerungen des Projektes führen.

Die Erfahrung aus derart globalen Großprojekten hat SITA gelehrt, das Projektrisiko jeweils frühzeitig und bestmöglich zu minimieren.

Bereits bei der Datenanforderung ist es wichtig, internationale Standards für den Datentransfer und das Datenformat einzuhalten. Bleiben die Anforderungen im Rahmen der von der Weltzollorganisation (WZO), Internationalen Zivilluftfahrtorganisation (ICAO) und Internationalen Luftverkehrs-Vereinigung (IATA) vorgegebenen optimalen Verfahren (*„best practices"*), erleichtert und beschleunigt dieses die Datenlieferung durch die Fluggesellschaften erheblich.

Die harmonisierten Standards für das Datenformat und die Transportprotokolle ermöglichen ein robustes System zur Überprüfung und Überwachung der Datenqualität und der zeitgemäßen Lieferung der Daten.

Die Einführung eines Fluggastdatensystems ist weit mehr als nur ein IT-System. Es ist vielmehr die Einführung neuer Geschäftsprozesse für Regierungen und die nachgelagerten Organisationen.

Der Aufbau eines automatisierten Risikoanalysesystems bedarf einer guten Steuerung und eines entsprechenden Projektmanagements. Es sollte mit einem Gesamtdesign beginnen, um das IT-System und die neuen Arbeitsprozesse sowie die Abgrenzungen der Verantwortungsbereiche aufeinander abzustimmen.

Unserer Erfahrung nach ist ein solcher Designprozess absolut notwendig, um ein gemeinsames Verständnis unter allen Beteiligten an dem System zu schaffen und die technische Lösung auf die neuen Geschäftsprozesse anzupassen und entwickeln zu können. Alle Nutzer des Systems sollten in diesen Prozess frühzeitig einbezogen werden, sodass die Erwartungen und die Anforderungen entsprechend kommuniziert, abgestimmt und realisiert werden können. Nachträgliche Änderungen sind extrem kostspielig und verzögern das Projekt erheblich.

Datenqualität

Der Erfolg eines Passagierdatensystems hängt maßgeblich von der Qualität und der Quantität der Passagierdaten ab, die empfangen, verarbeitet und analysiert werden müssen.

Die Datenqualität ist sowohl für die Regierungen als auch die Fluggesellschaften von hoher Bedeutung, um die Effektivität des Systems zu gewährleisten und letztlich vermeintliche Gefährder zu identifizieren und bestenfalls von den Flugzeugen fernzuhalten.

Mangelnde Datenqualität kann auf mehreren Ursachen beruhen:

Die Sicherstellung von qualitativen Datenlieferungen bzw. das Auffinden von Ursachen schlechter Datenqualität erfordert die Schaffung eines entsprechenden „Carrier Engagement Teams" (Ansprechpartner von Seiten der Regierungen), welches aktiv mit den Fluggesellschaften zusammenarbeitet.

Die Größe eines solchen Teams ist proportional zur Anzahl der involvierten Fluglinien. Für ein System mit über 150 Fluglinien – von denen man in Deutschland derzeit ausgeht – ist von >30 Mitarbeitern auszugehen. Kollaborative Zusammenarbeit mit den Fluglinien, den Nutzern/Behörden sowie weiteren Beteiligten ist ein fortwährender Prozess über die gesamte Laufzeit und von immenser Wichtigkeit.

Technische Spezifikationsbeschreibung und Trainingsunterlagen sollten für die Fluglinien entwickelt werden, um die Anforderungen der Regierung eindeutig und umfassend zu beschreiben. Nur ein klares Verständnis der zu liefernden Informationen (Inhalt, Art und Weise) ermöglicht eine schnellstmögliche Anpassung der Systeme auf Seiten der Fluglinien zur Einhaltung der Gesetzesvorgaben. Die Dokumentation ist auch im laufenden Betrieb für die Fluglinien und ihre Mitarbeiter hilfreich, insbesondere bei Änderungen an ihren Systemen, neuem Personal etc.

Unumgänglich bleibt eine **Test- und Zertifizierungsphase** mit den einzelnen Fluglinien, um die Konformität zu überprüfen, bevor die Daten in das Produktivsystem übernommen werden. Auch wenn Fluglinien bereits Daten im PNRGOV-Format senden können, ist eine Zertifizierung notwendig – wenn auch in reduziertem Umfang.

Fluglinien haben unterschiedliche Systeme und Betriebskonzepte für den Umgang mit Passagierdaten. Einige Fluglinien betreiben noch heute sehr veraltete (Reservierungs-) Systeme, andere nutzen bereits moderne Plattformen. Dies erfordert Kenntnisse und Erfahrung mit den Systemen der Fluggesellschaften – auch auf Seiten der Regierung. Es müssen verschiedene Konzepte erarbeitet werden, um schnellstmöglich und gemeinschaftlich die notwendigen Lösungen/Anpassungen zu vereinbaren.

Implementierungszeitplanung

Es gilt zu berücksichtigen, dass nicht nur Deutschland, sondern eine Vielzahl der europäischen Mitgliedstaaten eine Umsetzung und Inbetriebnahme ihres Passagierdatensystems bis Mai 2018 anstreben.

Somit sind Engpässe bei der Umsetzung der jeweiligen Regierungsanforderungen auf Seiten der Fluglinien zu erwarten. Dies gilt trotz der Standards wie PNRGOV, da jeder Mitgliedsstaat mit jeder Fluglinie den oben beschriebenen Test- und Zertifizierungsprozess durchlaufen sollte.

Im Falle von Deutschland sind das ca. 180 Fluglinien die es zu testen gilt. Zudem muss vorher das Regierungssystem installiert, getestet und in Betrieb genommen werden. Unserer Erfahrung nach ist somit von ca. 12-24 Monaten für die technische Implementierung auszugehen.

Interoperabilität und Risikoanalyse

Ein umfassendes Verständnis der nationalen Infrastruktur und deren Integration, sowie die Anbindung an die externen (internationalen) Systeme sind die Grundvoraussetzung für ein effektives Risikoanalysesystem. Passagierdaten bzw. PNR im speziellen sind nur ein Teil eines mehrschichtigen Ansatzes zur Verbesserung der nationalen Sicherheit und muss daher integriert werden – es ist kein „*Stand-Alone-System*".

Kooperation mit den jeweiligen autorisierten Institutionen einer Regierung wie z.B. Europol sind dabei notwendig und beschleunigen die Anbindung an bereits bestehende Schnittstellen und Kommunikationswege.

Passagierdaten – PNR oder auch API – sind nur denjenigen Sicherheitsinstitutionen bzw. ihren Mitarbeitern, zugänglich zu machen, die diese für ihre jeweiligen Arbeiten benötigen und dazu befugt sind. Hierzu ist ein striktes, individuelles Nutzerprofil für jeden Mitarbeiter der PIU bzw. der nachgelagerten Institutionen zu erstellen, der Zugriff auf die Daten und auf das System (z.B. für Systemadministration) haben soll. Nur so ist die Protokollierung und Dokumentierung sicher zu stellen, um die Anforderungen an den Datenschutz erfüllen zu können.

Pilotprojekt zur Risikominimierung

Ein Pilotprojekt bietet die Möglichkeit, im kleinen Umfang das System, die Daten und den damit verbundenen Umgang zu testen, validieren und zu trainieren. Eine überschaubare Menge an Fluglinien, die Grundfunktionalitäten des Systems und daraus resultierend, eine kleine Menge an Fällen die zu bearbeiten sind, ermöglichen es, vorab und vor allem rechtzeitig Änderungen und Tuningmaßnahmen durchzuführen.

Hierbei wird u.a. sichtbar, ob die Anforderungen der einzelnen Nutzer des Systems erfüllt werden. An diesem Punkt wird deutlich, wie gut und detailliert die ursprüngliche Planung (Designphase) unter Einbeziehung der jeweiligen Nutzer tatsächlich umgesetzt werden konnte.

Zusammenfassend raten wir dazu, die Erfahrungen und Beispiele aus anderen Ländern zu berücksichtigen. Dies betrifft z.B. die Frage, welche Komponenten des Systems aus Sicherheits-, Kosten- und Zeitgründen sinnvollerweise selbst zu entwickeln sind und welche von erfahrenen Unternehmen beschaffen und angepasst werden sollten.

Die Anzahl der PNR-Systeme weltweit sind zum heutigen Zeitpunkt gering, aber die Vorgehensweise und Umsetzung bei komplexen Passagierdatensystemen sind hilfreich und geben Aufschluss auf die zu erwartenden Schwierigkeiten und deren Vermeidung.

Eine gute Vorbereitung, ein frühzeitiges und klares Verständnis der Anforderungen und Abhängigkeiten unter den Nutzern und Beteiligten sind die Voraussetzung, um ein solch komplexes Projekt in der vorgegebenen Zeit und im Rahmen des Budgets zu realisieren.

Risikominimierung steht an erster Stelle; durch die Nutzung von „Best-Practice-Beispielen" anderer Länder, unter Einbeziehung bereits erfahrener PNR-Nutzer (z.B. bei der Zollbehörde) und in Zusammenarbeit mit bewährten und in dem Bereich Fluglinien und Passagierdaten erfahrenen Unternehmen kann dieses unserer Erfahrung nach bestmöglich erreicht werden.

SITA ist spezialisiert auf die internationale Datenkommunikation der Luftfahrtindustrie und unterstützt seine Mitglieder und Anteilseigner durch Service und Technologien zur Vereinfachung des Passagier- und Frachtverkehrs.

Die Eigentümer bzw. Mitglieder und ihre Partner sind Fluggesellschaften, Flughäfen, Flugsicherheitsorganisationen sowie Regierungen und internationale Organisationen (wie z. B. die Vereinten Nationen, Weltgesundheitsorganisation und Weltbank). Dies macht SITA einzigartig in der Industrie und für seine etwa 500 Eigentümer weltweit.

SITA ist bereits seit den 1960-er Jahren an der Entwicklung von Standards in der Luftverkehrskommunikation beteiligt und war auch schon vor dem 11. September 2001 an dem freiwilligen Austausch von Passagierdaten einiger Fluglinien mit Regierungen zur Verbesserung der Sicherheit involviert.

Seit über 20 Jahren entwickelt SITA sowohl Risikoanalysesysteme für Regierungen zur Verbesserung der Grenzsicherheit als auch elektronische Reiseinformations- und Genehmigungssysteme und stellt sie Regierungen zur Verfügung. SITA hat das erste interaktive Advanced Passenger Information (API) System aufgebaut. SITA ist heute in über 40 Ländern an (Grenz-)Sicherheitslösungen beteiligt die u.a. zur Risikoanalyse, Passenger Name Record (PNR) und API Daten nutzen.

SITA hat mehrfach die Europäische Kommission zum Thema PNR beraten und unterstützt aktiv die Weltzollorganisation (WZO), die Internationale Zivilluftfahrtorganisation (ICAO) und die Internationale Luftverkehrs-Vereinigung (IATA) bei der Harmonisierung der internationalen Standards für API und PNR – worum es sich im Wesentlichen in dem vorliegenden Gesetzentwurf zur Fluggastdatenübermittlung handelt.

Anhörung des Präsidenten des Bundeskriminalamtes

Holger Münch

vor dem Innenausschuss des Bundestages

am 24. April 2017

zum Entwurf eines Fluggastdatengesetzes (FlugDaG)

(Drs. 18/11501)

1. Einleitung

Die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität trat zum 25. Mai 2016 in Kraft. Mit Umsetzung dieser Richtlinie soll der bereits bestehende europaweite Austausch von Erkenntnissen zwischen den Mitgliedstaaten der Europäischen Union im gemeinsamen Kampf gegen Terrorismus und schwere Kriminalität durch ein neues Instrument ergänzt werden.

Alle EU-Mitgliedsstaaten haben bis Mai 2018 den durch die EU vorgegebenen Rahmen in nationales Recht umzusetzen. Zudem müssen alle organisatorischen und technischen Maßnahmen ergriffen werden, damit das neu zu schaffende Fluggastdaten-Informationssystem rechtzeitig aufgebaut und in Betrieb genommen werden kann.

Der Aufbau des Fluggastdaten-Informationssystems stellt unter technischen Gesichtspunkten eine große Herausforderung für Deutschland und alle EU-Mitgliedstaaten dar, bietet aber zugleich in fachlicher Hinsicht einen großen Mehrwert. Dieser fachliche Mehrwehrt ist hierbei nicht auf einen speziellen Phänomenbereich oder aber ein Aufgabenfeld des Bundeskriminalamtes bzw. der Sicherheitsbehörden Deutschlands (präventiv oder strafprozessual) beschränkt. Das BKA sieht hier die Chance, durch ein neu-

es Instrumentarium der kriminalpolizeilichen Auswertung, einen weiteren Beitrag zu einer Verbesserung der Sicherheitslage in Deutschland leisten zu können.

2. Positive Erfahrungen anderer Staaten

Dies zeigen die Erfahrungen anderer Staaten wie Australien, USA und Großbritannien, die bereits über etablierte Systeme zur Erhebung und Verwendung von PNR-Daten verfügen. So konnten in Ländern mit Fluggastdaten-Informationssystemen Terrorverdächtige schon vor der Einreise im jeweiligen Abflugland identifiziert werden, oder aber in den Jihad ausreisende Teenager wurden rechtzeitig an ihrer Ausreise nach Syrien gehindert und den Sorgeberechtigten übergeben. Auch in anderen Deliktsbereichen wie z.B. dem international organisierten Rauschgiftschmuggel sind die Erfahrungen der Länder mit Fluggastdaten-Informationssystemen positiv und auch aus Sicht Deutschlands als vielversprechend zu bewerten.

Die Einbeziehung der Intra-Schengen-Flüge in das Fluggastdatengesetz durch den deutschen Gesetzgeber ist aus Sicht des Bundeskriminalamtes sowohl sinnvoll als notwendig. So haben Erfahrungen, insbesondere aus dem Phänomenbereich des islamistischen Terrorismus gezeigt, dass sich islamistische Gefährder sehr wohl des Schengenraumes und seiner Herausforderungen für die Sicherheitsbehörden bewusst sind. So werden Ein- und Ausreisen nach bzw. aus Europa über den Luftweg, zur Umgehung nationaler Sicherheitsmaßnahmen, einfach aus einem anderen europäischen Mitgliedsstaat angetreten. Der hierfür genutzte Intra-Schengen-Transitflug bleibt mangels fehlender Grenzkontrollen unerkannt. Gleiches gilt auch für viele zur Fahndung ausgeschriebene Straftäter. Die Nutzung von Fluggastdaten auch für Intra-Schengen-Flüge stellt daher ein wichtiges Element zur weiteren Stärkung des europäischen Raumes der Freiheit, der Sicherheit und des Rechts dar, soweit und wenn Abgleichstreffer Katalogtatenbezug aufweisen.

3. Neue Aufgabe des Bundeskriminalamts als Fluggastdatenzentralstelle

Die Verarbeitung von Fluggastdaten erfordert hierbei auf der einen Seite strenge Vorgaben an den Datenschutz und die Datensicherheit, auf der anderen Seite sind hohe Anforderungen an die Verarbeitungsgeschwindigkeit zu beachten, das Verfahren muss „in Echtzeit" funktionieren, um mit dem Luftverkehr Schritt zu halten.

Für die Verarbeitung von Fluggastdaten wird das Bundeskriminalamt als nationale Fluggastdatenzentralstelle zuständig sein. Hierzu unterhält das Bundeskriminalamt ein Fluggastdaten-Informationssystem nach Maßgabe des Fluggastdatengesetzes.

Unter engen rechtlichen Voraussetzungen dürfen die von den Luftfahrtunternehmen übermittelten Daten mit Datenbeständen, die der Fahndung oder Ausschreibung von Personen oder Sachen dienen, abgeglichen werden. Hierbei kommt insbesondere ein Abgleich mit den Datenbeständen des „Schengener Informationssystems" (SIS) als europäisches Fahndungssystem und von „INPOL-zentral" (INPOL-Z) als nationales Auskunfts- und Fahndungssystem in Betracht. Nur durch einen Abgleich mit beiden Datenbanken kann sichergestellt werden, dass die Fluggastdaten mit allen wichtigen Fahndungsdaten abgeglichen werden.

Zusätzlich besteht die Möglichkeit, die Fluggastdaten mit sogenannten Mustern abzugleichen, um so Personen zu identifizieren, die im Zusammenhang mit terroristischen Straftaten oder einer Straftat der schweren Kriminalität stehen könnten, aber den Behörden bislang nicht namentlich bekannt sind.

Die aus dem Abgleich resultierenden Treffer können - stets nach einer technischen und individuellen Trefferverifikation durch die Fluggastdatenzentralstelle - unter den engen Voraussetzungen des § 6 FlugDaG-E an das Bundeskriminalamt (außerhalb seiner Funktion als Fluggastdatenzentralstelle) weitergegeben sowie an die Landeskriminalämter, die Zollverwaltung und die Bundespolizei übermittelt werden. Darüber hinaus ist eine Übermittlung an das Bundesamt für Verfassungsschutz und die Verfassungsschutzbehörden der Länder, den Militärischen Abschirmdienst sowie an den Bundesnachrichtendienst grundsätzlich möglich, soweit dies zur Erfüllung von deren Aufgaben im Zusammenhang mit Katalogtaten nach § 4 Abs. 1 FlugDaG-E erforderlich ist.

Unter engen Voraussetzungen ist ein Datenaustausch mit den Fluggastdatenzentralstellen anderer EU-Mitgliedsstaaten und Europol möglich, ebenso – unter Beachtung der Vorgaben des (Entwurfs zum) Bundesdatenschutzgesetz – mit den zur Verhütung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität zuständigen Behörden von Drittstaaten.

4. Stärkung des Datenschutzes durch institutionelle Trennung

Die Fluggesellschaften übermitteln die Fluggastdaten aller Passagiere nach § 2 Abs. 2 FlugDaG-E zur Speicherung im Fluggastdaten-Informationssystem. Eine Vorselektie-

rung der zu erhebenden Fluggastdaten erfolgt zu diesem Zeitpunkt weder nach objektiven oder noch nach subjektiven Gesichtspunkten. Die Fluggastdaten werden also diskriminierungsfrei erhoben.

Der deutsche Gesetzgeber hat zudem auch aus datenschutzrechtlichen Gründen entschieden, dass die Erhebung und Speicherung der Fluggastdaten – technisch getrennt von der polizeilichen Verarbeitung – außerhalb des Bundeskriminalamts erfolgen soll. Die technische Realisierung des Fluggastdateninformationssystems wurde im Bundesverwaltungsamt angesiedelt, das die Fluggastdaten im Auftrag und nach Weisung des Bundeskriminalamts verarbeitet. Die Gesamtverantwortung verbleibt also im Bundeskriminalamt.

Im Wirkbetrieb nimmt demnach das Bundesverwaltungsamt die Fluggastdaten von den Luftfahrtunternehmen entgegen. Die Betreuung der Fluggesellschaften während und nach der Anbindung an das Fluggastdaten-Informationssystem wird ebenfalls durch das Bundesverwaltungsamt sichergestellt. Das Bundeskriminalamt übernimmt insgesamt die fachliche Verantwortung als Fluggastdatenzentralstelle und somit auch die Gesamtverantwortung für den operativen Betrieb.

Grundsätzlich wird erst im Falle eines technischen Treffers ein Vorgang mit den relevanten Daten durch das Bundesverwaltungsamt an die Fluggastdatenzentralstelle im Bundeskriminalamt übermittelt. Hierdurch wird sichergestellt, dass in der Fluggastdatenzentralstelle nur solche Treffer zu Personen angezeigt werden, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie eine Straftat nach § 4 Abs. 1 FlugDaG-E begangen haben oder innerhalb eines übersehbaren Zeitraumes begehen werden. Innerhalb der Fluggastdatenzentralstelle erfolgt eine individuelle Trefferverifikation durch einen kriminalpolizeilichen Sachbearbeiter. Erst wenn dies zu dem Ergebnis führt, dass eine hohe Wahrscheinlichkeit besteht, dass sich eine gesuchte Person unter den Passagieren befindet, werden polizeiliche Folgemaßnahmen beispielsweise über die an den Flughäfen zuständige Bundespolizei eingeleitet.

Die durch die Luftfahrtunternehmen übermittelten Klarpersonalien dürfen lediglich sechs Monate im Fluggastdaten-Informationssystem gespeichert werden, ehe diese für eine weitere Aufbewahrung von maximal viereinhalb Jahren depersonalisiert werden. Nach Ablauf von fünf Jahren ab ihrer Übermittlung an die Fluggastdatenzentralstelle sind die Fluggastdaten durch die Fluggastdatenzentralstelle aus dem Fluggastdaten-Informationssystem zu löschen. Eine Aufhebung der Depersonalisierung ist nur dann

zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Aufhebung zur Verhütung oder Verfolgung von terroristischen Straftaten oder schwerer Kriminalität erforderlich ist und die Aufhebung auf Antrag der Leitung der Fluggastdatenzentralstelle oder deren Vertretung gerichtlich genehmigt worden ist.

5. Sukzessiv aufwachsender Wirkbetrieb und stufenweise Anbindung der Luftfahrtunternehmen

Um der Komplexität des Aufbaues eines Fluggastdatensystems gerecht zu werden, ist es unabdingbar, die IT-Systeme und die fachlichen Prozesse sukzessive aufzubauen und zu stabilisieren, damit am Ende ein ausgereiftes, sicheres und allen Datenschutzanforderungen entsprechendes Gesamtsystem entsteht. Aufgrund der hohen Zahl der an das System anzubindenden Fluggesellschaften, der Vielzahl der zu erwartenden Passagierdaten sowie unter Berücksichtigung der zu etablierenden vielschichtigen und behördenübergreifenden Prozesse ist eine vollumfängliche Aufnahme des Wirkbetriebs des Fluggastdaten-Informationssystems unmittelbar mit Inkrafttreten des FlugDaG (Big Bang-Szenario) zu risikobehaftet.

Die dem Entwurf des Fluggastdatengesetzes beigefügte Begründung zu Artikel 3 zeigt, dass der Gesetzgeber sowohl die sukzessive Inbetriebnahme des Fluggastdaten-Informationssystems als auch eine stufenweise Anbindung der Luftfahrtunternehmen unterstellt und eine entsprechende Anlaufphase berücksichtigt hat. Die technische Anbindung der Luftfahrtunternehmen an das Fluggastdaten-Informationssystem wird demzufolge ab dem Zeitpunkt des Inkrafttretens des Gesetzes sukzessive in kooperativer Zusammenarbeit mit den Luftfahrtunternehmen erfolgen. Die enge Kooperation zwischen den Luftfahrtunternehmen und den Behörden wird momentan schon gelebt; seit dem Frühjahr 2016 ist das BVA aktives Mitglied der PNRGOV Working Group des internationalen Luftfahrtverbandes IATA und hat im Herbst 2016 den Vorsitz einer Subgroup (Unterarbeitsgruppe) unter der Federführung der IATA übernommen.

FAZIT

Der Europäische Gesetzgeber hat durch Verabschiedung der Richtlinie einen wichtigen Grundstein gelegt, auf dem der Entwurf des Fluggastdatengesetzes als künftig elementarer Baustein der Sicherheitsarchitektur Europas und Deutschlands fußt. Die Ausgestaltung der EU-Richtlinie durch den deutschen Gesetzgeber im Entwurf des Fluggastdatengesetzes erfolgte hierbei unter Achtung der Grundrechte und der Regelungen des

Datenschutzes. Gleichzeitig eröffnet es dem Bundeskriminalamt durch die operative Auswertung von gespeicherten Fluggastdaten als Deutschlands nationale Fluggastdaten-Zentralstelle ein weiteres Werkzeug für eine effektive Gefahrenabwehr und Strafverfolgung.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)869 E

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 ... 4
II. Hintergrund ... 7
III. Umsetzung durch den deutschen Gesetzgeber ... 7
1. Umsetzungspflicht ... 7
2. Anwendbares Grundrechtsregime: nationale oder EU-Grundrechte ... 8
3. Weitgehende 1:1-Umsetzung des deutschen Gesetzgebers ... 9
IV. Grundrechtliche Bewertung der Pflicht zur Speicherung von Fluggastdaten ... 10
1. Anhaltspunkte in der Rechtsprechung ... 10
2. Kein unionsgrundrechtliches Verbot einer anlasslosen Fluggastdatenverarbeitung ... 14
3. Wahrung des Wesensgehalts (Art. 52 Abs. 1 S. 1 GRC) ... 17
4. Legitimer Zweck ... 18
5. Eignung ... 18
6. Erforderlichkeit ... 19
7. Angemessenheit ... 19
a) Verwendungszwecke ... 19
b) Automatisierter Abgleich mit Mustern ... 21
c) Speicherdauer ... 22
d) Kategorien von Fluggastdatensätzen ... 22
8. Materiell- und verfahrensrechtliche Anforderungen für den Zugang zu Datenbeständen ... 25
a) Vorabkontrolle ... 25
b) Beschränkung des Zugangs ... 26
c) Benachrichtigungspflichten ... 28
d) Überwachung durch unabhängige Stelle ... 29
9. Datensicherheit ... 29
10. Weiterleitung an Drittstaaten ... 30
11. Berufsgeheimnisträger ... 31
12. Unternehmerische Freiheit ... 31
V. Umsetzungsfragen ... 33
1. Einbeziehung auch innereuropäischer Flüge ... 33
a) Kein generelles Verbot der anlasslosen Fluggastdatenverarbeitung ... 34
b) Eignung ... 35
c) Erforderlichkeit ... 36
d) Umfang der Speicherpflicht ... 37

e) Datensicherheit ... 37
f) Datenlöschung ... 37
g) Verwendungszwecke ... 38
h) Berufsgeheimnisträger ... 40
i) Datenzugang ... 40
j) Transparenz ... 42
2. Einbeziehung anderer Unternehmen als Fluggesellschaften ... 47
3. Übermittlungszeitpunkt ... 47
4. Straftatenkatalog ... 48
a) Erfasste Straftaten ... 48
b) Bestimmtheit ... 48
5. Datensicherheit ... 49
6. Weitere Datenschutzregelungen ... 50
7. Fluggastdatenzentralstelle und Auftragsdatenverarbeitung ... 51
8. Speicherort im Hoheitsgebiet der Mitgliedstaaten ... 52
9. Aufgabe der Zweckbindung im Kontext der Strafverfolgung (§ 6 Abs. 4 FlugDaG-E) ... 53
10. Anordnungsbefugnis bei Gefahr im Verzug ... 54
11. Benachrichtigungspflichten bei Rechtsverletzungen ... 55
12. Sanktionen ... 56
13. Abgleich mit Mustern und Datenbanken ... 56
14. Weitergabe der Daten ... 58
a) Allgemeine Anforderungen und Übermittlung im Inland ... 58
b) Weitergabe an Drittstaaten ... 59
c) Weitergabe innerhalb der EU und an Europol ... 61
15. Ausgestaltung der Datenübermittlung (Doppeltür-Modell) ... 61

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.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)869 F

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Forschungsinstitut für öffentliche und private Sicherheit (FÖPS Berlin)

Prof. Dr. Clemens Arzt
Direktor

Alt-Friedrichsfelde 60
10315 Berlin

www.foeps-berlin.org
foeps@hwr-berlin.de

Stellungnahme zur Anhörung des Innenausschusses des Deutschen Bundestages am 26. April 2017

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

Prof. Dr. Clemens Arzt

I. Einleitung

Der Gesetzentwurf soll ausweislich der Gesetzesbegründung der Umsetzung der Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) dienen. Diese Richtlinie (nachfolgend PNR-RL) ist bis zum 25. Mai 2018 in nationales Recht umzusetzen.

Ziel der Richtlinie (Erwägungsgrund 7) ist, anhand einer Überprüfung von PNR-Daten Personen zu ermittelt, die vor einer solchen Überprüfung nicht im Verdacht standen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein, und die von den zuständigen Behörden genauer überprüft werden sollen. Dies soll dazu dienen, PNR-Daten mit verschiedenen Datenbanken betreffend Personen und Gegenstände abzugleichen, um terroristische Straftaten und schwere Kriminalität zu verhüten, aufzudecken, zu ermitteln und zu verfolgen und damit einen Beitrag zur inneren Sicherheit zu leisten, um Beweismaterial zusammenzutragen und gegebenenfalls Komplizen von Straftätern aufzuspüren und kriminelle Netze auszuheben (Erwägungsgrund 6).

Ziel der Maßnahme ist mithin die anlass- und verdachtslose Erhebung vielfältiger personenbezogener Daten aller Flugreisenden im von der Richtlinie erfassten Bereich von Drittstaatsflügen wie auch von EU-Flügen zum Zweck der präventiv-polizeilichen Verhütung von Straftaten einerseits und der Verfolgung von Straftaten sowie darüber hinaus die Vorsorge für die Verfolgung solcher Straftaten auf der repressiv-polizeilichen Ebene andererseits. Genaue Zahlen, wie viele Fluggäste hiervon betroffen sind, liefert der Gesetzentwurf nicht. In Europa insgesamt wurden 2015 über 900 Mio. Fluggäste[1] befördert, in Deutschland waren es 2016 rund 223 Mio.[2] Erfasst werden sollen nach § 2 Abs. 3 FlugDaG (und damit weit über die Mindestanforderungen der PNR-RL hinausgehend) alle Flugpassagiere mit Ziel im Ausland oder aus dem Ausland einreisend, das waren nach diesseitiger Kenntnis 2015 rund 170 Mio. Passagiere, mithin rund 3 von 4 Passagiere in Flugverkehr über deutsche Flughäfen.[3] Auch wenn jeder Fluggast bei jedem erfassten Flug erneut gespeichert wird und damit die Zahl der erfassten Personen unter der o.g. Zahl liegen wird, fallen mit Blick auf die vorgesehene Speicherdauer nach § 13 FlugDaG in 5 Jahren rund

[1] http://ec.europa.eu/eurostat/documents/2995521/7680649/7-10102016-AP-DE.pdf
[2] https://de.statista.com/statistik/daten/studie/77928/umfrage/passagiere-auf-deutschen-flughaefen/
[3] http://ec.europa.eu/eurostat/documents/2995521/7680649/7-10102016-AP-DE.pdf

850 Mio. Fluggastdatensätze an, auf die das BKA zugreifen kann, wobei im Rahmen der Depersonalisierung nach § 5 FlugDaG gewisse Beschränkungen des Datensatzes nach Ablauf von 6 Monaten als Regelfall eintreten, für die indes die Möglichkeit der Aufhebung im Einzelfall nach § 5 Abs. 2 FlugDaG besteht.

Das **PNR-Abkommen mit Kanada** liegt derzeit dem EuGH vor. Der Generalanwalt beim EuGH, *Paolo Mengozzi*, hat in seinen Schlussanträgen vom 8. September 2016 (Gutachten 1/15) erhebliche rechtliche Bedenken geltend gemacht, die zum Teil auch mit Blick auf den vorliegenden Gesetzentwurf Relevanz haben[4]. Hinzu kommen die nachstehend ausgeführten Bedenken. Es wird daher, nicht zuletzt mit Blick auf den erheblichen Umfang von fast 600 Stellen zum Betrieb des Systems, dringend empfohlen, vor einer Umsetzung der PNR-RL in deutsches Recht den Ausgang des Verfahrens vor dem EuGH abzuwarten, weil hier zum einen Massendaten von Millionen Menschen wegen eines alltäglichen Vorgangs, der Teilnahme am Reiseverkehr polizeirechtlich anlasslos und ohne Anfangsverdacht strafprozessualer Art erhoben und genutzt werden, zum anderen die Industrie sich auf die Übermittlung dieser Daten vorbereiten muss und bei einer negativen Entscheidung des EuGH Aufwendungen zur Umsetzung des Push-Verfahrens wird umsonst gemacht haben.

II. Zum Gesetzentwurf im Einzelnen

Nachfolgend sollen die vorgeschlagenen gesetzlichen Regelungen ungeachtet einer grundsätzlichen Kritik an dem Vorhaben (s.o.) einer detaillierteren Analyse unterzogen werden, die indes im Rahmen einer Sachverständigenanhörung nicht den Umfang und die Form eines Rechtsgutachtens annehmen kann.

§ 1 (Fluggastdatenzentralstelle und Zweck des Fluggastdaten-Informationssystems)

Nach **§ 1 Abs. 1** erhält das BKA die Aufgabe als **Fluggastdatenzentralstelle** im Sinne des Gesetzes, was offenkundig von der Zentralstellenfunktion des § 2 BKAG abzugrenzen ist. Zweifelhaft

[4] Hierzu auch Wendt, ZD-Aktuell 2016, 0520, Boehm/Cole, ZD 2014, 553/556.

erscheint bereits die **Gesetzgebungskompetenz** des Bundes, wenn die Gesetzesbegründung trotz des angegebenen Ziels der Bekämpfung des internationalen Terrorismus nicht auf Art. 73 Abs. 1 Nr. 9a GG verweist, sondern auf Art. 73 Abs. 1 Nr. 10, obgleich Nr. 9a die Kompetenz aus Nr. 10 verdrängt.[5]

Laut **§ 1 Abs. 2** dient das System der Verhütung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität. Bemerkenswert ist bereits, dass in der Gesetzesbegründung (siehe: A. Problem und Ziel) von der Zielrichtung der Bekämpfung des **internationalen Terrorismus** (s.a. Art. 73 Abs. 1 Nr. 9a GG) die Rede ist, § 1 Abs. 2 dieses Ziel aber sogleich deutlich in der Norm ausgeweitet wird, nämlich auf **jede Form des Terrorismus**, einem weiterhin ungeklärten Begriff, der hier trotz der jüngst vom BVerwG[6] geäußerten Bedenken nicht hinreichend präzisiert wird.

Der Begriff der „**Verhütung von Straftaten**“ ist denkbar weit und beinhaltet als solcher **kaum Grenzen im Sinne des Bestimmtheitsgebots**. Verhütung von Straftaten bedeutet zunächst einmal die Unterbindung eines in der Zukunft mit nicht näher dargelegter Wahrscheinlichkeit von den Polizeibehörden erwartetes Ereignis, das bei seiner Verwirklichung einen Straftatbestand erfüllen würde. Zur Verhütung solcher nicht einmal im Ansatz oder auf Grund bestimmter Tatsachen erkennbaren Straftaten dürfen nunmehr alle Passagierdaten erfasst, gespeichert und gerastert werden. Der erfasste Personenkreis wird in keiner Weise mit Blick auf den Verhältnismäßigkeitsgrundsatz eingegrenzt, es handelt sich mithin um Maßnahmen, die in ihrer „**Eingriffswirkung mit großer Streubreite** gleichsam die gesamte Bevölkerung betreffen“[7]. Ebenso ist für die Verarbeitung durch das BKA als Fluggastdatenstelle für die Verarbeitung von Massendaten der gesamten Bevölkerung auf der **Wahrscheinlichkeitsebene keine Einschränkung** erkennbar; diese greift allenfalls bei der Übermittlung an und dem Datenaustausch mit anderen Stellen und auch nur dann, wenn nicht das BKA selbst im Rahmen einer Initiativübermittlung nach § 7 Abs. 3 Nr. 1 tätig wird.

Hinzu kommt das **Bestimmtheitsdefizit** mit Blick auf den Begriff „**schwerer Kriminalität**“. Dieser ist weder aus dem Wortsinn hinreichend bestimmt ableitbar, noch gesetzlich fixiert, noch in der Rechtsprechung klar

[5] *Uhle* in Maunz-Dürig, GG, Art. 73 Rn. 253.
[6] So zuletzt auch BVerwG 21. März 2017 - 1 VR 2.17.
[7] Vgl. BVerfG 20. April 2016 - 1 BvR 66/09 und 1 BvR 1140/09 (BKAG), Rn. 101 zu

herausgearbeitet. Die PNR-RL kann für das deutsche Recht dieses Defizit nicht verbindlich beseitigen. Die Aufzählung in Anhang II der Richtlinie hat keine unmittelbare Geltung in Deutschland und muß zunächst im Lichte der Anforderungen des Artikel 3 Nr. 9 PNR-RL mit Blick auf das Strafmaß vom nationalen Gesetzgeber geprüft und in nationales Recht umgesetzt werden (zu den Problemen s.u. zu § 4 FlugDaG), um für die Betroffenen aber auch das BKA und die Gerichte hinreichend bestimmt festzulegen, welche Straftaten der „schweren Kriminalität“ zuzuordnen sein sollen.

Gemäß der Intention des Gesetzgebers dient die Verarbeitung umfangreicher personenbezogener Daten aller Flugpassagiere mit Ziel oder Herkunft außerhalb Deutschlands der **anlasslosen "Verdachts-" oder "Verdächtigengewinnung"**[8] gegen jede Personen anlässlich ihrer Nutzung des Flugverkehrs, um „Personen zu identifizieren, die den Sicherheitsbehörden noch nicht bekannt waren und die mit einer terroristischen Straftat oder einer Straftat der schweren Kriminalität in Zusammenhang stehen könnten“ (Gesetzesbegründung S. 26).

Grundlage für diese **Verdachtsgenierung** sind nicht Anhaltspunkte im Verhalten der Betroffenen, sondern „Muster“, welche das BKA aus vorhandenen Daten, die keinen Bezug zu einer bestimmten Person aufweisen, eigenständig generiert (Gesetzesbegründung S. 17 f.). Damit ist die Maßnahme keine „typische“ Maßnahme im Rahmen der Verhütung von Straftaten (Gefahrenabwehr) oder Verfolgungsvorsorge (vorgezogene Repression)[9], sondern dient der **massenhaften präventiven Speicherung von Daten ohne rechtfertigenden Grund im Einzelfall**.

Anders als im Bereich der TK-Vorratsdatenspeicherung werden die in der **Fluggastdaten-Vorratsspeicherung** erhobenen personenbezogenen Daten im Rahmen der weiteren Verarbeitung indes nicht erst dann genutzt, wenn dies etwa zur Feststellung einer möglichen strafbaren Handlung in Bezug auf konkrete Personen und bereits begangene Straftaten oder zumindest einen Anfangsverdacht hierzu von den Polizeibehörden als sinnvoll angesehen wird, sondern das BKA selbst kann die Fluggastdaten jedes Flugreisenden einerseits mit „Mustern“ abgleichen, um hieraus (bisher nicht einmal vorhandene) **Verdachtsmomente neu zu generieren**, die dann ggf. Anschlussmaßnahmen gegen den Betroffenen begründen.

[8] Vgl. BVerfG 4. April 2006 - 1 BvR 518/02 Rn. 107 f. (Rasterfahndung).
[9] Vgl. BVerfG 27. Juli 2005 - 1 BvR 668/04.

Die Fluggastdaten jedes Flugreisenden werden darüber hinaus auch dazu genutzt, ständig neue „Muster“ zu erstellen (Gesetzesbegründung S. 17 f.).

Beides stellt eine **völlig neue Dimension der anlasslosen Massenüberwachung** dar, unter Nutzung vielfältigster personenbezogener Daten (vgl. § 2) von derzeit rund 170 Mio. Fluggästen/Jahr. Mit den Anforderungen des EuGH an die Vorratsdatenspeicherung[10] ist dies nicht kompatibel.

Soweit **§ 1 Abs. 3** auf die **Auftragsverarbeitung** durch das Bundesverwaltungsamt verweist, wäre ein ausdrücklicher Verweis auf die einschlägigen Regelungen im BDSG zumindest vorzugswürdig[11], wenn nicht gar aus Gründen der Normenbestimmheit notwendig, zumal der GE (S. 23) selbst darauf verweist, dass die weitere Ausgestaltung noch einer „Vereinbarung“ zwischen den Beteiligten unterliegt. Dabei ist zu beachten, dass das Bundesverwaltungsamt die Daten „im Auftrag und nach Weisung“ verarbeitet, die Sachhoheit also alleine beim BKA liegt.

§ 2 Datenübermittlung durch Luftfahrtunternehmen

§ 2 Abs. 1 verpflichtet Luftfahrtunternehmen zur Übermittlung der in Absatz 2 festgelegten personenbezogenen Informationen. Anders als im Bereich der TK-Vorratsdatenspeicherung geht der Grundrechtseingriff hier indes deutlich weiter und ist intensiver, weil personenbezogene Daten seitens der staatlichen Sicherheitsbehörden nicht nur im Einzelfall bei den verpflichteten Unternehmen abgerufen werden können, wenn die gesetzlichen Voraussetzungen aus StPO und TKG vorliegen, sondern **alle Daten** werden **ohne weiteren Anlass** oder in der Person des Betroffenen liegendem Grund **an das BKA übermittelt**.

Die Ausmaße der **anlasslosen Nutzung von Massendaten** durch das BKA eher „verniedlichend“ wird in der Gesetzesbegründung (S. 17, 24) darauf verwiesen, es würden nur die Daten übermittelt, die Passagiere ohnehin dem Luftfahrunternehmen zur Verfügung gestellt hätten. Diese Zurverfügungstellung an das Luftfahrunternehmen seitens der Passagiere geschieht indes nicht „freiwillig“ und aus gesondertem Interesse im Rahmen

[10] EuGH 8. April 2014, Digital Rights Ireland u. a., verbundene Rechtssachen C-293/12 und C-594/12; s.a. EuGH 21. Dezember 2016 verbundene Rechtssachen C-203/15 und C-698/15.
[11] Vgl. *Petri* in Simitis, BDSG, 7. Aufl. § 11 Rn. 16.

eine „informed consent“, sondern ist notwendige Voraussetzung um überhaupt einen Beförderungsvertrag abschließen zu können. Wie auch in der TK-Vorratsdatenspeicherung werden also die **verpflichteten Unternehmen** durch den Gesetzgeber gezwungen, Daten für denselben nach Maßgabe des Gesetzgebers zu übermitteln. Andererseits werden viele Passagiere diese Daten gerade nicht an das BKA liefern wollen, allein weil sie ein Flugzeug besteigen. Es herrscht also eine „**Ablieferungspflicht**“ zu Gunsten staatlicher Interessen.

Interessanterweise hält die Bundesregierung es in ihrer Gesetzesbegründung (S. 24) für zulässig, dass die Fluggastdatenzentralstelle alle nach § 2 Abs. 1 an das BKA übermittelten personenbezogenen Daten ohne Rechtsgrundlage auch **an die Fluggastdatenzentralstellen aller Mitgliedsstaaten der EU übermitteln** darf. Hierzu wird auf eine „Auskunft der Europäischen Kommission“ verwiesen. Dies erstaunt, weil die Übermittlung von Daten nach § 78 BDSG n.F. zumindest einen gemäß Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 gefassten **Angemessenheitsbeschluss** der Kommission voraussetzt. Soll **§ 78 BDSG n.F.** hier also nicht greifen, wenn die Notwendigkeit einer Rechtsgrundlage seitens der Bundesregierung in der Begründung zum GE verneint wird?

§ 2 Abs. 2 legt im Detail fest, **welche Daten** Fluggastdaten im Sinne des Gesetzes sind. Hierunter fallen nicht nur mannigfaltige personenbezogene Informationen über den Fluggast selbst, sondern **auch über Dritte**, z.B. über Mitreisende (was deren Verhältnis zueinander offenbart) und über Reisebüros sowie deren Sachbearbeiter. In keiner Weise wird im Gesetzentwurf dargelegt, **weshalb** die insgesamt 20 unterschiedlichen Kategorien personenbezogener Daten **im Einzelnen** für den in § 1 Abs. 2 genannten Zweck **notwendig** sein sollen; deren Eignung und die Erforderlichkeit im Einzeln ist mithin nicht dargetan. Hinzu kommt, dass in Nr. 2 unter „allgemeine Hinweise“ ein **Freitextfeld** eingefügt wird, das vom Gesetzgeber in keiner Weise näher bestimmt ist. Hier können seitens der Unternehmen mannigfaltige Hinweise gespeichert werden, die durchaus auch **sensible Daten** beinhalten, die nach § 2 Abs. 3 aber nicht Gegenstand der vom BKA festgelegten „Muster“ sein dürfen.

§ 2 Abs. 3 legt fest, für welche Flüge Fluggastdaten zu übermitteln sind. Dabei geht das FlugDaG weiter über das hinaus, was von der PNR-RL als Mindeststandard verlangt wird, nämlich nur Flüge mit **Drittstaaten**. Nach deutschen Recht sollen auch die Daten für alle EU-Flüge erhoben und

ausgewertet werden, was die Pflichten aus Art. 2 Abs. 1 PNR-RL nach sich zieht. Unzulässig ist dies nicht, indes wird in der Gesetzbegründung an keiner Stelle begründet, weshalb Deutschland hier deutlich über das von der Richtlinie gebotene **Mindestmaß der zu verarbeitenden Daten** durch die Zentralstelle hinausgeht.

Unklar ist auch, weshalb der Gesetzentwurf keine **Informationspflicht der Luftfahrt-Unternehmen** analog § 31a Absatz 4 BPolG vorsieht; auch wenn hier konzediert werden muss, dass gegen diese Verpflichtung fortwährend verstoßen wird. Ein Vollzugsdefizit[12] auf der einen Seite kann aber nicht zur Begründung des Fehlens einer Transparenz staatlichen Handelns auf der anderen Seite führen.

§ 4 Voraussetzungen für die Datenverarbeitung

Hier ist zunächst herauszuarbeiten, welche Befugnisse dem BKA als Zentralstelle zuwachsen. Zulässig ist eine **Verarbeitung** aller von den Luftfahrunternehmen übermittelten personenbezogenen Daten und ein Abgleich mit eigenen Datenbeständen des BKA sowie „Mustern".

Unbegrenzte Verarbeitung von Daten durch das BKA

Der Begriff der **Datenverarbeitung** ist – anders als im geltenden BDSG – im BDSG n.F. nach meiner Kenntnis nicht länger definiert. Es ist daher auf den Begriff in Art. 3 Nr. 2 der **EU-Richtlinie 2016/680** vom 27. April 2016 zurück zu greifen, der mit dem der Datenschutz-Grundverordnung vom gleichen Datum identisch ist. Danach ist von der „**Verarbeitung**" jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit **personenbezogenen Daten** wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung umfasst.

Insoweit gewährt **§ 4 Abs. 1** in Abweichung von der bisherigen Grundstruktur des deutschen Rechts mit einer klaren befugnisrechtlichen

[12] Hierzu vertiefend *Arzt* in Sicherheitsrecht des Bundes, § 31a BPolG Rn. 17.

Trennung der verschiedenen Eingriffs“stufen“ (z.B. Erheben, Speichern, Nutzen), die jeweils einer spezifischen Eingriffsbefugnis bedürfen, gleichsam in Form einer **Blankettnorm** dem BKA **umfassende und nicht näher definierte Befugnisse** der „Verarbeitung“ personenbezogener Daten von Fluggastdaten.

Zulässigkeit der anlasslosen Rasterfahndung in Massendaten

Der so genannte **Abgleich mit Mustern** stellt faktisch eine **Rasterfahndung**[13] in dem Sinne dar, dass Daten einer großen Menge (derzeit rund 170 Millionen mal im Jahr) „**unverdächtiger“ Personen** mit vom BKA vorab festgelegten Mustern abgeglichen werden, um diejenigen Personen herauszufiltern, die aus Sicht des BKA für den weiteren Verlauf weiterer Ermittlungen „interessant“ sind. „Die Rasterfahndung ist "**Verdachts-" oder "Verdächtigengewinnungseingriff**" (…) insbesondere dann, wenn sie - wie im vorliegenden Fall - zur Aufdeckung von so genannten terroristischen Schläfern führen soll.“[14]

Anlass der Maßnahme ist also nicht das konkrete Verhalten einer Person, das bestimmte polizeiliche Maßnahmen hervorruft, sondern das BKA legt im Rahmen der weitgehend unbestimmten Voraussetzungen des § 4 FlugDaG Muster fest, die sodann „**verdachtsgenerierend**“ mit umfassenden Fluggastdaten abgeglichen werden.

In der Gesetzesbegründung (S. 24) wird dargelegt, dass die Bundesregierung selbst von einer „**Trefferquote**“ von ca. 0,1 % ausgeht, die anderen Daten aber auch weiterhin „retrograd“ dem Zugriff zugänglich halten will. Mit anderen Worten: gesucht werden nicht bestimmte Personen oder es wird bestimmten Anhaltspunkten für eine Gefahr oder einen Anfangsverdacht nachgegangen, sondern diese werden durch Massendatenabgleich erst noch generiert und damit zugleich für jeden die potentielle Folge erzeugt, ohne Gründe im eigenen Verhalten einem Verdacht oder polizeilichen Ermittlungsmaßnahmen ausgesetzt zu sein.[15]

Problematisch ist hieran bereits der Mangel einer hinreichenden **Eingriffsschwelle**. Es handelt sich bei der Fluggastdatenverarbeitung gleichsam um eine doppelfunktionale Maßnahme der Verhütung von

[13] Zum Begriff *Petri* in Lisken/Denninger, 5. Auflage, Rn 530.
[14] BVerfG 4. April 2006 - 1 BvR 518/02 Rn. 107 f. (Rasterfahndung) Rn. 119.
[15] Vgl. *Petri* in Lisken/Denninger, 5. Auflage, Rn 532.

Straftaten und der Verfolgungsvorsorge. Zur präventiv-polizeilichen Rasterfahndung stellte das BVerfG fest: „Eine **präventive polizeiliche Rasterfahndung** (…) ist mit dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) nur vereinbar, wenn eine **konkrete Gefahr für hochrangige Rechtsgüter** wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist. Im Vorfeld der Gefahrenabwehr scheidet eine solche Rasterfahndung aus. Eine allgemeine Bedrohungslage, wie sie im Hinblick auf terroristische Anschläge seit dem 11. September 2001 durchgehend bestanden hat, oder außenpolitische Spannungslagen reichen für die Anordnung der Rasterfahndung nicht aus. Vorausgesetzt ist vielmehr das Vorliegen weiterer Tatsachen, aus denen sich eine konkrete Gefahr, etwa für die Vorbereitung oder Durchführung terroristischer Anschläge, ergibt.“[16]

Die hier vorgesehene Maßnahme weist zudem eine hohe Eingriffsintensität mit Blick auf die automatisierte Auswertung von Massendaten auf: „Als **Fahndungsmethode** weist die **Rasterfahndung** die Vorteile auf, die automatisierte, rechnergestützte Operationen generell mit sich bringen, ermöglicht also die Verarbeitung nahezu beliebig großer und komplexer Informationsbestände in großer Schnelligkeit. Ein herkömmliches Verfahren, die nach dem Modell abgestufter Erkenntnisverdichtung erfolgende Ermittlungstätigkeit, wird hierdurch mit einer bislang unbekannten Durchschlagskraft versehen. In grundrechtlicher Hinsicht führt die **neue Qualität der polizeilichen Ermittlungsmaßnahme** zu einer erhöhten Eingriffsintensität.“[17]

Einschüchternde Wirkung

Neben die TK-Vorratsdatenspeicherung als anlassloser Maßnahme der Massenüberwachung der Kommunikation von Bürgerinnen und Bürgern tritt hier als **weitere anlasslose Massenüberwachung** die **des Flugverkehrs** hinzu, wobei der Gesetzentwurf noch deutlich über die Richtlinie hinausgeht und nicht nur den Flugverkehr mit Drittstaaten der Überwachung unterwirft, sondern auch den Flugverkehr innerhalb der EU. Damit bewegt sich der Gesetzgeber immer weiter in eine Richtung, die vom **EuGH** in seinen Entscheidungen zur **TK-Vorratsdatenspeicherung** als unzulässig

[16] BVerfG 4. April 2006 - 1 BvR 518/02 (Leitsätze).
[17] BVerfG 4. April 2006 - 1 BvR 518/02 Rn. 122, zur Rasterfahnung 2001.

angesehen wurde[18] und mit Blick auf die Häufigkeit von Flugreisen in fast allen Bevölkerungsschichten gleichsam die gesamte Bevölkerung betreffen.[19] Geschaffen wird ein Instrument der massenhaften und umfassenden staatlichen Überwachung aller Bürgerinnen und Bürger die am Flugreiseverkehr teilnehmen, was aufgrund der Masse der Betroffenen und des Fehlens eines Anknüpfungspunktes im eigenen Verhalten erhebliche **einschüchternde Wirkung** erzeugt.

Neben die TK-Vorratsdatenspeicherung tritt die **Fluggastdaten-Vorratsdatenspeicherung** als **weiteres Element** einer **gesamt-gesellschaftlichen Überwachung**, mit erheblichen Einschüchterungs-wirkungen.[20] „Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wurde indes der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer."[21] Fraglich ist, ob im Sinne einer „**Überwachungsgesamtrechnung**"[22] diese Grenze mit der hier diskutierten Maßnahme und deren Umfang, also einer Kumulation anlassloser Massenüberwachungsinstrumente nicht überschritten ist, weil diese mit der Identität der bundesdeutschen Verfassung nicht vereinbar und damit **verfassungswidrig** ist.[23] Eine Vereinbarkeit mit Art. 7 und 8 der Europäische Grundrechtecharta im Lichte der Entscheidung des EuGH zur TK-Vorratsdatenspeicherung wird schwerlich zu bejahen sein.[24]

Maßgeblich ist, „ob der Betroffene einen ihm zurechenbaren Anlass, etwa durch eine Rechtsverletzung, für die Erhebung geschaffen hat oder ob sie anlasslos erfolgt und damit praktisch jeden treffen kann. Informationserhebungen gegenüber Personen, die den Eingriff durch ihr Verhalten nicht veranlasst haben, sind grundsätzlich von höherer Eingriffsintensität als anlassbezogene. Werden Personen, die keinen Erhebungsanlass gegeben haben, in großer Zahl in den Wirkungsbereich einer Maßnahme einbezogen, können von ihr auch allgemeine **Einschüchterungseffekte** ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können. Die Unbefangenheit des

[18] S.o. Rn. 10.
[19] Kritisch zur Angemessenheit solcher Maßnahmen BVerfG 20. April 2016 - 1 BvR 66/09 und 1 BvR 1140/09 (BKAG), Rn. 101.
[20] Ausführlich Knieriem ZD 2011, 17.
[21] BVerfG 2. März 2010 - 1 BvR 256/08, 1 BvR 263/08 und 586/08, Rn. 218.
[22] Knieriem ZD 2011, 20 f.
[23] Dies bejaht zutreffend Knierim S. 22 f.; so schon der BfDI 2012, vgl. ZD-Aktuell 2012, 02924
[24] So auch Bundesrat, Empfehlungen der Ausschüsse, BR-Drs. 161/1/17

Verhaltens wird insbesondere gefährdet, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen. Das aber ist gerade bei der seriellen Erfassung von Informationen in großer Zahl der Fall."[25] Die Maßnahme hat mit Blick auf die Vielzahl der anlasslos erfassten Personen „eine außerordentlich hohe Streubreite".[26]

Heimliche Durchführung und Anschlussmaßnahmen

Hinzu kommt die **Heimlichkeit** der Durchführung der Maßnahme als weiteres die **Eingriffsintensität** steigerndes Element.[27] „Die Intensität des Eingriffs für den Grundrechtsträger wird [zudem] davon beeinflusst, welche **über die Informationserhebung hinausgehenden Nachteile** ihm [dem Betroffenen] aufgrund der Maßnahme drohen oder von ihm nicht ohne Grund befürchtet werden. Die Schwere des Eingriffs nimmt mit der Möglichkeit der Nutzung der Daten für Folgeeingriffe in Grundrechte der Betroffenen zu sowie mit der Möglichkeit der Verknüpfung mit anderen Daten, die wiederum andere Folgemaßnahmen auslösen können."[28]

In der Regel zunächst weitere heimliche **Anschlussmaßnahmen** wird jeder gegenwärtigen müssen, der unter ein vom BKA selbst geschaffenes „Muster" fällt. Mangels **Benachrichtigung** über das Ergebnis besteht eine Möglichkeit der gerichtlichen Überprüfung der Rasterung nicht, was **mit Art. 19 Abs. 4 GG in Konflikt** steht.

Hierauf weist auch das **BVerfG** in seiner Entscheidung zur **Rasterfahndung** hin: „Auf die Intensität des Eingriffs wirken sich ferner etwaige aus der Rasterfahndung resultierende weitere Folgen für die Betroffenen aus. Das Gewicht informationsbezogener Grundrechtseingriffe richtet sich auch danach, welche Nachteile den Betroffenen aufgrund der Eingriffe drohen oder von ihnen nicht ohne Grund befürchtet werden. (…) So kann die Übermittlung und Verwendung von Daten für die Betroffenen das **Risiko** begründen, **Gegenstand staatlicher Ermittlungsmaßnahmen zu werden**, das über das allgemeine Risiko hinausgeht, einem unberechtigten Verdacht ausgesetzt zu werden. Auch können informationsbezogene Ermittlungsmaßnahmen im Falle ihres

[25] Vgl. BVerfG 11. März 2008 - 1 BvR 2074/05 und 1 BvR 1254/07 (Kfz-Kennzeichenerkennung), Rn. 78 (unter Auslassung der Verweise).
[26] Vgl. BVerfG 4. April 2006 - 1 BvR 518/02 Rn. 107 f. (Rasterfahndung) Rn. 121.
[27] Ebd. Rn. 79.
[28] Ebd. Rn. 80.

Bekanntwerdens eine stigmatisierende Wirkung für die Betroffenen haben und so mittelbar das Risiko erhöhen, im Alltag oder im Berufsleben diskriminiert zu werden."[29]

Hinzu kommt die Möglichkeit einer **stigmatisierenden Wirkung** der Maßnahme gegen bestimmte Bevölkerungsgruppen, worauf das BVerfG ebenfalls in seiner Entscheidung zur Rasterfahndung hinweist: „Ferner kann die Tatsache einer nach bestimmten Kriterien durchgeführten polizeilichen Rasterfahndung als solche - wenn sie bekannt wird - eine stigmatisierende Wirkung für diejenigen haben, die diese Kriterien erfüllen."[30] Dies gilt (wie bereits bei der Rasterfahnung 2001) insbesondere wegen der Zielrichtung gegen den so genannten internationalen Terrorismus mit Blick auf Muslime und Menschen aus dem arabischen Raum, auch wenn hier die Religionszugehörigkeit kein ausdrückliches Kriterium ist. „So fällt etwa für die Rasterfahndungen, die nach dem 11. September 2001 durchgeführt wurden, im Hinblick auf deren **Eingriffsintensität** ins Gewicht, dass sie sich gegen **Ausländer bestimmter Herkunft und muslimischen Glaubens** richten, womit stets auch das Risiko verbunden ist, Vorurteile zu reproduzieren und diese Bevölkerungsgruppen in der öffentlichen Wahrnehmung zu stigmatisieren (…). Insbesondere die kaum vermeidbaren Nebeneffekte einer nach der Zugehörigkeit zu einer Religion differenzierenden und alle Angehörigen dieser Religion pauschal erfassenden Rasterfahndung erhöhen das Gewicht der mit ihr verbundenen Grundrechtseingriffe und damit die von Verfassungs wegen an ihre Rechtfertigung zu stellenden Anforderungen."[31]

Der Staat darf und muss terroristischen Bestrebungen - etwa solchen, die die Zerstörung der freiheitlichen demokratischen Grundordnung zum Ziel haben und die planmäßige Vernichtung von Menschenleben als Mittel zur Verwirklichung dieses Vorhabens einsetzen – nach den Ausführungen des BVerfG zur Rasterfahndung mit den erforderlichen rechtsstaatlichen Mitteln wirksam entgegentreten. Auf die rechtsstaatlichen Mittel hat sich der Staat unter dem Grundgesetz jedoch auch zu beschränken.[32]

Diese Grenzen sind hier eindeutig überschritten; hinzu kommt, dass die zulässigen Maßnahmen nicht allein der Terrorismusabwehr, sondern auch

[29] BVerfG 4. April 2006 - 1 BvR 518/02 Rn. 107 f. (unter Auslassung der Verweise).
[30] Ebd. Rn. 111.
[31] Ebd. Rn. 112.
[32] Ausführlich ebd. Rn. 126 ff.

der Abwehr der so genannten „schweren Kriminalität“ im Allgemeinen dienen sollen.

§ 4 Absatz 1

Absatz 1 legt fest, dass das BKA als Fluggastdatenzentralstelle alle Fluggastdaten **mit „Datenbeständen und Mustern“ abgleichen** kann. Datenbestände kann hier nicht meinen, dass nur mit den nach dem FlugDaG erhobenen Datenbeständen abgeglichen werden darf, sondern mit allen Datenbeständen des BKA, zumindest soweit die Voraussetzungen des § 12 BKAG n.F. vorliegen, was mit Blick, auf dessen „Weite“ der Regelfall sein dürfte. Dies bestätigt auch der Verweis in Absatz 2 Nr. 1 mit Bezug auf **Fahndungsbestände**, was mit Blick auf die Rechtsprechung des Bundesverfassungsgerichts als nicht hinreichend bestimmt anzusehen ist[33].

Gesucht werden dabei nicht Personen, zu denen konkrete Erkenntnisse im Sinne des Satz 2 vorliegen, sondern entsprechende Erkenntnisse sollen erst noch generiert werden, „um **Personen zu identifizieren**, bei denen tatsächliche Anhaltspunkte dafür vorliegen (…), mithin eine anlasslose **"Verdachts-" oder "Verdächtigengewinnung**"[34]. Erfasst ist ein umfangreicher Straftatenkatalog in der Form der Kettenverweisung, der deutliche Bestimmtheitsmängel aufzeigt, insbesondere in Nr. 3, 5 und 6.

§ 4 Absatz 3 bis 5

Absatz 3 formuliert die näheren Anforderungen an die vom BKA zu erstellenden **Muster**, welche die verdachts- und anlasslose **Rasterfahndung** ermöglichen sollen. Gefordert sind hier in Satz 3 zwar „Tatsachen zu bestimmten Straftaten“, nicht jedoch ein Anfangsverdacht oder die Gefahr der Begehung einer bestimmten Straftat, noch Anhaltspunkte zu bestimmten Person; vielmehr sollen diese erst im Rahmen der Auswertung gewonnen werden. Diese belegt auch Absatz 4 hinsichtlich der Auswertung aller Fluggastdaten zur Erstellung von Mustern. Allein Absatz 5 sieht eine gezielte Suche nach bestimmten Personen im Rahmen der Aufgaben aus § 1 Abs. 2 vor.

Aus den bereits ausgeführten Gründen ist dies **verfassungsrechtlich nicht akzeptabel**.

[33] BVerfG 11. März 2008 - 1 BvR 2074/05 und 1 BvR 1254/07 (Kfz-Kennzeichenerkennung), Rn. 99 ff.
[34] Vgl. BVerfG 4. April 2006 - 1 BvR 518/02 Rn. 107 f. (Rasterfahndung).

§ 5 Depersonalisierung

Die gespeicherten Fluggastdaten werden im Rahmen einer **Vorratsdatenspeicherung** regelmäßig frühestens nach 5 Jahren gelöscht (s.u. zu § 13); eine erheblich längere Frist als dies § 113b TKG für die vom EuGH jüngst mit Blick auf die EU-Richtlinie grundsätzlich beanstandete TK-Vorratsdatenspeicherung vorsah. Dies bedeutet, alle Fluggäste, die unter die Datenspeicherung nach diesem Gesetz fallen, bleiben mit ihren Daten für 5 Jahre erfasst, obgleich sie hierzu keinen Anlass gegeben haben.

„Abgemildert" werden soll dies offenbar durch eine so genannte **Depersonalisierung** nach § 5, die indes nur für bestimmte Fluggastdaten greift und nach Absatz 2 wieder aufhebbar ist. Der Begriff der Depersonalisierung meint offenkundig **„weniger" als** die gängigen Verfahren der **Anonymisierung** oder **Pseudonymisierung** nach dem BDSG auch in seiner neuen Fassung und nach der EU-Datenschutzgrundverordnung (2016/679). Dennoch ist das Verfahren im Gesetz nicht näher bestimmt.

Dies belegt auch Absatz 2, der offenkundig von einer jederzeitigen „**Rückholbarkeit**" aller personenbezogenen Daten ausgeht, wobei diese Option nicht allein auf die Verfolgung einer bestimmbaren Straftat oder gegen eine bestimmte Person eröffnet wird, sondern auch zur denkbar weiten „Verhütung von Straftaten", ohne dass hier ein Bezug zu bestimmten Personen erforderlich wäre.

Zulässig ist auch eine Anordnung durch die Präsidentin oder den Präsidenten des BKA bei „**Gefahr im Verzug**"; eine genaue Frist, bis wann die gerichtliche Entscheidung nachzuholen ist, fehlt. Dies entspricht zwar den Regelungen im BKAG n.F., ist indes **unter Bestimmtheitsgrundsätzen kritisch** zu sehen.

§§ 6 bis 10 Datenübermittlungen, -austausche und gemeinsame Verfahren

Nach **§ 6 Absatz 2** dürfen die Daten nicht nur an Bundes- und Landespolizeibehörden übermittelt werden, sondern auch an die Nachrichtendienste. Der Schutzmechanismus eines **Trennungsgebotes** oder auch nur der **informationellen Trennung** wird hiermit im Anschluss an das ATDG und § 17 BKAG n.F. weiter ausgehöhlt.

§ 6 Absatz 4 macht deutlich, dass auch die das Recht auf informationelle Selbstbestimmung schützende Idee einer **Zweckbindung** von personenbezogenen Daten analog zu § 12 BKAG n.F. **beseitigt** werden soll.

Die umfassenden Möglichkeiten des **Datenaustauschs mit Mitgliedstaaten** der EU nach **§ 7** knüpfen an die „Verhütung von Straftaten“ und deren Verfolgung an; ersteres eröffnet Datenübermittlungen weit im Vorfeld konkreter Gefahren oder einem Anfangsverdacht. Während nach Absatz 3 bei Ersuchen aus dem Ausland hierfür „tatsächliche Anhaltspunkte“ verlangt werden, ist diese bei einer Übermittlung auf Initiative des BKA nicht erforderlich.

Nach **§ 8** ist die Entwicklung und Durchführung **gemeinsamer Rasterfahndungsverfahren** mit allen Mitgliedstaaten der **EU** zulässig. Ausweislich der Gesetzesbegründung (S. 33) soll dies offenbar auch im Vorfeld des Vorfelds („**vorgelagerte Sachaufklärung**“) zulässig sein. Das hierbei auch unbegrenzt **personenbezogene Daten** übermittelt werden können, belegt der Verweis in Satz 2 auf § 7, der nach Absatz 3 Nr. 1 Initiativübermittlungen des BKA gestattet, auch zur „**Erforschung von Gefährdungssachverhalten**“, mithin ohne konkreten Anlass im Einzelfall. Neben dem internationalen Terrorismus soll so zum Beispiel auch die **Bekämpfung von Fluchtbewegungen** in die EU unterstützt werden (Gesetzesbegründung S. 31 unter Verweis auf „Schleuserbanden“).

Diese Entgrenzung der Datenübermittlung findet ihre Fortsetzung in § 10, der als Maßstab wiederum auf die Verhütung von Straftaten abstellt.

§ 13 Löschung von Daten

Eine Löschung von Daten aus der Fluggastdaten-Vorratsspeicherung soll gemäß **Absatz 1 Satz 1** nach 5 Jahren erfolgen, allerdings nur, soweit diese nicht innerhalb des genannten Zeitraums nach § 6 weiter übermittelt wurden. In diesem Fall gelten die jeweiligen für diese Behörden geltenden Vorschriften, die nicht selten eine Standardspeicherdauer von 10 Jahren vorsehen. Im Ergebnis kann hieraus eine **Speicherdauer von bis zu 15 Jahren** folgen. **Absatz 4** enthält hierzu nur Einschränkungen für so genannten **Trefferfälle** (vgl. Art. 12 Abs. 5 der Richtlinie (EU) 2016/681) im Rahmen der Verarbeitung.

Im Ergebnis ist der vorgelegte Gesetzentwurf nach meiner Auffassung mit den Anforderungen der EuGrCh wie auch dem Grundgesetz nicht vereinbar.

gez. Prof. Dr. Clemens Arzt

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)798

18. Wahlperiode

Deutscher Bundestag
Parlamentarischer Beirat
f. nachhaltige Entwicklung

Ausschussdrucksache
18(23)99-6

Gutachtliche Stellungnahme

Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz - FlugDaG)

Bundesrats-Drucksache 161/17

Im Rahmen seines Auftrags zur Überprüfung von Gesetzentwürfen und Verordnungen der Bundesregierung auf Vereinbarkeit mit der nationalen Nachhaltigkeitsstrategie hat sich der Parlamentarische Beirat für nachhaltige Entwicklung gemäß Einsetzungsantrag (BT-Drs. 18/559) in seiner 59. Sitzung am 8. März 2017 mit dem Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz - FlugDaG) (BR-Drs. 161/17) befasst.

Folgende Aussagen zur Nachhaltigkeit wurden in der Begründung des Gesetzentwurfes getroffen:

„Der Gesetzentwurf steht im Einklang mit dem Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Nationalen Nachhaltigkeitsstrategie. Die Wirkungen des Gesetzentwurfs zielen auf eine nachhaltige Entwicklung, weil er dem Bundeskriminalamt als Fluggastdatenzentralstelle des Fluggastdaten-Informationssystems rechtssichere Befugnisse zur Verarbeitung von Fluggastdaten zum Schutz der Bürgerinnen und Bürger vor terroristischen Straftaten und schwerer Kriminalität an die Hand gibt und zugleich durch hohe datenschutzrechtliche Anforderungen den Schutz der personenbezogenen Daten der Fluggäste gewährleistet.“

Formale Bewertung durch den Parlamentarischen Beirat für nachhaltige Entwicklung:

Eine Nachhaltigkeitsrelevanz des Gesetzentwurfes ist nicht gegeben.

Die Darstellung der Nachhaltigkeitsprüfung ist plausibel.

Eine Prüfbitte ist daher nicht erforderlich.

Berlin, 8. März 2017

Dr. Lars Castellucci, MdB
Berichterstatter

Dr. Valerie Wilms, MdB
Berichterstatterin