UN und Europarat

Januar

Februar

März

April

Mai

21. Juni – Das Büro des Beratenden Ausschusses des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten veröffentlicht einen Bericht über die Konsultation zur Modernisierung des Übereinkommens Nr. 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.

Juni

Juli

August

September

Oktober

November

Dezember

EU

Januar

2. Februar – Die Europäische Kommission billigt einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität.

Februar

16. März – Bericht der Europäischen Kommission über die gemeinsame Überprüfung der Umsetzung des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus.

März

18. April – Bewertungsbericht der Europäischen Kommission an den Rat und das Europäische Parlament zur Richtlinie über die Vorratsdatenspeicherung.

April

Mai

16. Juni – Veröffentlichung der Umfrage von Eurobarometer Spezial 359 betreffend Einstellungen zu Datenschutz und elektronischer Identität in der Europäischen Union.

Juni

13. Juli – Die Europäische Kommission verabschiedet eine Mitteilung über Optionen für ein EU-System zum Aufspüren der Terrorismusfinanzierung.

Juli

August

26. September – Der Ministerrat der Europäischen Union stimmt den Vorschlägen der Europäischen Kommission über den Einsatz von Körperscannern auf EU-Flughäfen zu.

29. September – Unterzeichnung des Abkommens über Fluggastdatensätze (PNR-Daten) zwischen der EU und Australien.

September

25. Oktober – Verordnung des Europäischen Parlaments und des Rates zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts

27. Oktober – Das Europäische Parlament verabschiedet eine legislative Entschließung zum Entwurf eines Beschlusses des Rates über den Abschluss des Abkommens zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an den Australian Customs and Border Protection Service.

Oktober

10. November – Die Europäische Kommission verabschiedet eine Verordnung zur Änderung der Verordnung zur Ergänzung der gemeinsamen Grundstandards für die Sicherheit der Zivilluftfahrt bezüglich des Einsatzes von Sicherheitsscannern an EU-Flughäfen.

11. November – Die Europäische Kommission verabschiedet eine Durchführungsverordnung betreffend die gemeinsamen Grundstandards in der Luftsicherheit bezüglich des Einsatzes von Sicherheitsscannern an EU-Flughäfen.

24. November – Der Gerichtshof der Europäischen Union urteilt in zwei Rechtssachen in Bezug auf den Datenschutz und die Informationsgesellschaft: *ASNEF und FECEMD gegen Administración del Estado und Scarlet Extended SA gegen Société belge des auteurs, compositeurs et éditeurs.*

November

13. Dezember – Der Europäische Rat gibt grünes Licht für das PNR-Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika.

Dezember

3 Informationsgesellschaft und Datenschutz

Die zwei Themen Sicherheit und Technologie beherrschten die Debatte im Jahr 2011 – dem Jahr, in dem sich die Terroranschläge vom 11. September in den USA zum zehnten Mal jährten. Angesichts dieses Jahrestages flammte die Auseinandersetzung darüber auf, wie Sicherheit, Schutz der Privatsphäre und Datenschutz in ein ausgewogenes Verhältnis gebracht werden können, und bezog sich hierbei auf aktuelle Themen wie die Vorratsspeicherung von Telekommunikationsdaten, die Sammlung und Auswertung von Fluggastdatensätzen, die Einrichtung eines Systems zum Aufspüren der Finanzierung des Terrorismus und den Einsatz von Ganzkörper-Scannern. Besonders im Zusammenhang mit sozialen Netzwerken im Internet kam außerdem die Frage auf, in welcher Weise der Rechtsrahmen im Bereich des Datenschutzes an den technischen Fortschritt angepasst werden muss.

Dieses Kapitel beschreibt wesentliche Änderungen bezüglich der Rechtsvorschriften, Strategien und Verfahren in der Europäischen Union (EU) und den Mitgliedstaaten im Bereich des Datenschutzes im Jahr 2011. Zunächst werden die wichtigsten Entwicklungen auf europäischer Ebene beschrieben. Anschließend werden die vielbeachteten Themen des Jahres 2011 angesprochen: Vorratsdatenspeicherung, Fluggastdatensätze (Passenger Name Record, PNR), Systeme zum Aufspüren der Terrorismusfinanzierung, Einsatz von Körperscannern und soziale Netzwerke.

3.1. Allgemeiner Überblick

Im November 2010 legte die Europäische Kommission eine Mitteilung im Bereich des Datenschutzes vor.[1] In der Mitteilung erläutert die Kommission ihr Konzept für eine Reform der EU-Vorschriften für den Schutz personenbezogener Daten in sämtlichen Tätigkeitsbereichen der EU unter besonderer Berücksichtigung der Herausforderungen der Globalisierung und der neuen Technologien. Mit dem Konzept werden mehrere Ziele verfolgt: Stärkung der Rechte des Einzelnen, mehr Transparenz und Förderung des Bewusstseins für den Datenschutz, bessere Kontrolle des Betroffenen über seine Daten, Gewährleistung der Einwilligung ohne Zwang und in

1 Europäische Kommission (2010a).

Wichtige Entwicklungen in den Bereichen Informationsgesellschaft und Datenschutz:

- In einigen EU-Mitgliedstaaten äußern die Gerichte und Parlamente Bedenken im Hinblick auf das nationale Recht zur Umsetzung der Richtlinie über die Vorratsspeicherung von Daten; Ende 2010 verabschiedet die Europäische Kommission einen Bewertungsbericht über diese Richtlinie.
- Das Europäische Parlament billigt das Abkommen über Fluggastdatensätze zwischen der EU und Australien, die Billigung des entsprechenden Abkommens zwischen der EU und den USA steht allerdings noch aus; die Europäische Kommission schlägt eine Richtlinie zum Austausch von Fluggastdaten zu Strafverfolgungszwecken zwischen den EU-Mitgliedstaaten vor.
- Die EU führt neue Vorschriften für den Einsatz von Ganzkörperscannern an europäischen Flughäfen ein. Die praktische Anwendung dieser Scanner wird unterdessen in einer Reihe von EU-Mitgliedstaaten bereits erprobt und bewertet.
- Die Europäische Kommission unterbreitet Optionen für ein europäisches System zum Aufspüren der Finanzierung des Terrorismus; unterdessen wird die Umsetzung der bestehenden Zusammenarbeit zwischen der EU und den USA, des sogenannten Programms zum Aufspüren der Finanzierung des Terrorismus, zwei Überprüfungen unterzogen, die beide mehr Transparenz fordern.

Kenntnis der Sachlage, Prüfung des Schutzes sensibler Daten sowie wirksamere Rechtsbehelfe und Sanktionen. In seiner Stellungnahme zur Mitteilung forderte der Europäische Datenschutzbeauftragte ehrgeizigere Lösungen, die den Bürgern[2] eine bessere Kontrolle über ihre personenbezogenen Daten bieten und das System damit wirksamer machen. Er betonte, dass die Einbeziehung der polizeilichen und justiziellen Zusammenarbeit in den Rechtsrahmen für einen wirksamen Datenschutz unabdingbar sind.[3]

Die Eurobarometer-Umfrage *Attitudes on Data Protection and Electronic Identity in the European Union* (Einstellungen zu Datenschutz und elektronischer Identität in der Europäischen Union) wurde im Jahr 2011 veröffentlicht.[4] Die wichtigsten Ergebnisse der Umfrage, in deren Rahmen 26 574 Europäer ab 15 Jahren in den 27 Mitgliedstaaten befragt wurden, zeigen, dass für drei von vier Europäern die Offenlegung von personenbezogenen Daten ein zunehmender Teil des modernen Lebens ist, wobei die Art und Weise der Verwendung dieser Daten durch die Unternehmen (darunter Suchmaschinen und soziale Netzwerke) Anlass zur Sorge gibt. Aus dem Bericht geht hervor, dass 62 % der EU-Bürger zum Schutz ihrer Identität nur die unbedingt notwendigen Daten angeben, während 75 % sich wünschen, dass online gespeicherte personenbezogene Daten gelöscht werden, wann immer sie sich dazu entscheiden – das ist das sogenannte Recht auf Vergessen („right to be forgotten"). Viele Europäer wünschen sich darüber hinaus Maßnahmen der EU: 90 % befürworten einheitliche Datenschutzrechte in der gesamten EU. Die Umfrage wurde von Ende November bis Mitte Dezember 2010 durchgeführt. Alle Befragungen erfolgten in einem persönlichen Interview in der Wohnung und in der Landessprache des Befragten.

> *„Mehr als die Hälfte der befragten Europäer ist der Ansicht, dass […] Unternehmen (die personenbezogene Daten ohne Wissen der Betroffenen nutzen) eine Geldstrafe auferlegt werden sollte (51 %). Vier von zehn Europäern sind dafür, dass diesen Unternehmen die Nutzung solcher Daten künftig untersagt werden sollte (40 %) oder dass diese Unternehmen gezwungen werden sollten, die Opfer zu entschädigen (39 %)."*
>
> *Eurobarometer Spezial 359,* Attitudes on Data Protection and Electronic Identity in the European Union*, Brüssel, Juni 2011, S. 190*

In ihrem Bericht *The Evolving Privacy Landscape: 30 years after the OECD Privacy Guidelines* (Entwicklung der Datenschutzlandschaft: 30 Jahre nach Annahme der OECD-Datenschutzleitlinien)[5] beschreibt die OECD aktuelle Tendenzen in der Verarbeitung personenbezogener Daten und die damit verbundenen Datenschutzrisiken. Der Bericht weist auf Initiativen und innovative Ansätze zum Schutz der Privatsphäre hin, wobei der Schwerpunkt auf wirtschaftlichen Tätigkeiten liegt. Die OECD veröffentlichte außerdem ein Economic Paper zur Regelung des grenzüberschreitenden Datenaustauschs, um der zunehmenden Gefährdung der Privatsphäre angesichts der steigenden Zahl der internetbasierten Datenübertragungen in einer globalisierten Weltwirtschaft zu begegnen. Das Economic Paper enthält eine systematische Bestandsaufnahme der Vorschriften auf globaler Ebene und untersucht die den Vorschriften zugrunde liegenden politischen Konzepte[6] mit dem Ziel, einen Beitrag zu der Debatte über die künftige Regelung des grenzüberschreitenden Datenaustauschs zu leisten.

Im Europarat wurde die Debatte in Bezug auf die Änderung des Übereinkommens des Europarates über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108) fortgesetzt.[7] Dem Bericht des Europarates über die zugehörige Konsultation zufolge[8] wiesen die Befragten auf die Bedeutung der Gewährleistung der Vereinbarkeit mit den Schutzvorschriften der EU hin. Darüber hinaus nahm das Ministerkomitee des Europarates Ende November 2010 eine Empfehlung betreffend den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling an.[9] Die Empfehlung zielt auf die Definition einer fairen und rechtmäßigen Profilerstellung bei uneingeschränkter Achtung der Grundrechte ab, insbesondere des Rechts auf Schutz der Privatsphäre und der personenbezogenen Daten sowie des Grundsatzes der Nichtdiskriminierung. Außerdem veröffentlichte der Europarat am 20. September 2011 den Entwurf einer Strategie für die Verwaltung des Internets (2012-2015), der am 15. März 2012 verabschiedet wurde und in dem die Förderung von Datenschutz und Schutz der Privatsphäre zu einem der Hauptziele erklärt wird. Schließlich wurde im Jahr 2011 eine Überprüfung der folgenden Empfehlungen des Ministerkomitees eingeleitet: Empfehlung Nr. R (87) 15 zur Regelung der Benutzung personenbezogener Daten durch die Polizei und Empfehlung Nr. R (89) 2 zum Schutz personenbezogener Daten, die für Beschäftigungszwecke verwendet werden.

Auf EU-Ebene hat die Rolle des Datenschutzes im Raum der Freiheit, der Sicherheit und des Rechts Interesse erregt. Eine für das Europäische Parlament durchgeführte Studie beschäftigte sich mit den

2 Im Interesse einer besseren Lesbarkeit wird in diesem Bericht auf die durchgehende Nennung der männlichen und weiblichen Form verzichtet. Es sind selbstverständlich beide Geschlechter gemeint.
3 Europäischer Datenschutzbeauftragter (2011a).
4 Europäische Kommission (2011a).
5 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) (2011a).
6 OECD (2011b).
7 Europarat (2011a).
8 Europarat (2011b).
9 Europarat (2010).

neuen Herausforderungen im Zusammenhang mit Datenschutzstrategien und -systemen, die in den Anwendungsbereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen fallen.[10] Die Studie enthält eine Reihe allgemeiner Grundsätze und Standards, die sicherstellen sollen, dass der Datenschutz in allen Phasen der Politikgestaltung in der EU wirklich gewährleistet ist und dass dieses Grundrecht wirksam umgesetzt wird.

Auf der Konferenz der europäischen Datenschutzbeauftragten wurde eine Entschließung angenommen, die die Notwendigkeit eines umfassenden Datenschutzrahmens im Bereich der Strafverfolgung betont.[11]

Die Verordnung zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts wurde am 25. Oktober 2011 erlassen.[12] Die neue Agentur ist für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts zuständig: der EU-Datenbank der zweiten Generation zur Verwaltung und Verteilung von Daten zu Personen und Sachen, die für die nationale Sicherheit, die Grenzkontrolle und die Strafverfolgung von Interesse sind (SIS II); eines Visa-Informationssystems (VIS) sowie einer europäischen Fingerabdruck-Datenbank zur Ermittlung von Asylbewerbern und illegal eingereisten Personen (Eurodac).

Auf allgemeinerer Ebene ist die Unabhängigkeit der Datenschutzbehörden (siehe die Liste der nationalen Datenschutzbehörden in Tabelle 3.1) nach wie vor ein wichtiges Anliegen. Wie bereits im letzten Jahresbericht mitgeteilt, hat der Europäische Gerichtshof (EuGH) in einem Urteil[13] befunden, dass die deutschen Datenschutzbehörden ihre Aufgaben auf Länderebene nicht in völliger Unabhängigkeit wahrnehmen; außerdem wurde berichtet, dass die Europäische Kommission Österreich vor dem EuGH wegen unzureichender Unabhängigkeit seiner Datenschutzbehörde verklagt hat.[14] In den Diskussionen über die neue ungarische Verfassung, die Anfang 2012 in Kraft trat, ging es vor allem um die Unabhängigkeit der ungarischen Datenschutzbehörde. Die Europäische Kommission leitete am 17. Januar 2012 diesbezüglich beschleunigte Vertragsverletzungsverfahren gegen Ungarn ein.[15]

Tabelle 3.1: Gemäß Unionsrecht erforderliche Stellen – Datenschutzbehörden (nach Land)

Land	Name der Stelle in englischer Sprache	Name der Stelle in der Landessprache (Alternativsprache)
AT	*Austrian Data Protection Commission*	Österreichische Datenschutzkommission
BE	*Commission for the protection of privacy*	*Commission de la protection de la vie privée/Commissie voor de bescherming van de persoonlijke levenssfeer/*Ausschuss für den Schutz des Privatlebens
BG	*Commission for Personal Data Protection*	*Комисията за защита на личните данни*
CY	*Commissioner for Personal Data Protection*	*Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*
CZ	*The Office for Personal Data Protection*	*Úřad pro ochranu osobnich udajů*
DE	*The Federal Commissioner for Data Protection and Freedom of Information*	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
DK	*Danish Data Protection Agency*	*Datatilsynet*
EE	*Estonian Data Protection Inspectorate*	*Andmekaitse Inspektsioon*

10 Bigo, D. *et al.* (2011).
11 Konferenz der europäischen Datenschutzbeauftragten (2011).
12 Verordnung (EU) Nr. 1077/2011, ABl. L 286 vom 1.11.2011.
13 EuGH C-518/07, *Europäische Kommission/Bundesrepublik Deutschland*, 9. März 2010.
14 Europäische Kommission (2010b).
15 Europäische Kommission (2012).

Tabelle 3.1: (Fortsetzung)

Land	Name der Stelle in englischer Sprache	Name der Stelle in der Landessprache (Alternativsprache)
EL	*Hellenic Data Protection Authority*	*Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*
ES	*Spanish Data Protection Authority*	*Agencia Española de Protección de Datos, AEPD*
FI	*Office of the Data Protection Ombudsman*	*Tietosuojavaltuutetun toimisto, Dataombudsmannens byrå*
FR	*National Commission for information technology and freedoms*	*Commission Nationale de l'Informatique et des Libertés*
HU	*Authority for Data Protection and Freedom of Information*	*Nemzeti Adatvédelmi és Információszabadság Hatóság*
IE	*Data Protection Commissioner*	*An Coimisinéir Cosanta Sonraí*
IT	*Data Protection Authority*	*Garante per la protezione dei dati personali*
LT	*State Data Protection*	*Valstybinė duomenų apsaugos inspekcija*
LU	*National Commission for the Protection of Data*	*Commission nationale pour la protection des données*
LV	*Data State Inspectorate*	*Datu valsts inspekcija*
MT	*Office of the Data Protection Commissioner*	
NL	*Dutch Data Protection Authority*	*College bescherming persoonsgegevens*
PL	*The Bureau of the Inspector General for the Protection of Personal Data*	*Generalny Inspektor Ochrony Danych Osobowych*
PT	*Portuguese Data Protection Authority*	*Comissão Nacional de Protecção de Dados*
RO	*The National Supervisory Authority for Personal Data Processing*	*Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal*
SE	*The Swedish Data Inspection Board*	*Datainspektionen*
SI	*Information Commissioner*	*Informacijski pooblaščenec*
SK	*Office for Personal Data Protection of the Slovak Republic*	*Úrad na ochranu osobných údajov*
UK	*The Office of the Information Commissioner*	*Swyddfa'r Comisiynydd Gwybodaeth*

Quelle: http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm vom 31. Dezember 2011

„Die Unabhängigkeit der Datenschutzbeauftragten wird mit Artikel 16 des Vertrags über die Arbeitsweise der EU und Artikel 8 der Grundrechtecharta garantiert. Ferner sind die Mitgliedstaaten nach den EU-Vorschriften für den Datenschutz (Richtlinie 95/46/EG) gehalten, eine Kontrollstelle einzurichten, die die Anwendung der Richtlinie überwacht und in völliger Unabhängigkeit handelt. […] Allein das Risiko politischer Einflussnahme durch die staatliche Aufsicht ist ausreichend, um die Kontrollstelle bei der unabhängigen Wahrnehmung ihrer Aufgaben zu behindern."

Europäische Kommission, Pressemitteilung IP/12/24, Brüssel, 17. Januar 2012

3.2. Vorratsdatenspeicherung

Gemäß einer EU-Richtlinie müssen Internetdienstanbieter und Betreiber von Telekommunikationsdiensten umfassende Verkehrsdaten über die nicht auf den Inhalt bezogene Nutzung des Internets und der Kommunikationsdienste speichern. Diese **EU-Richtlinie über die Vorratsspeicherung von Daten**[16] hat seit ihrer Verabschiedung im Jahr 2006 immer wieder Fragen im Hinblick auf die Grundrechte aufgeworfen. Im April 2011 veröffentlichte die Europäische Kommission einen Bericht, der die Umsetzung und Anwendung dieser Richtlinie bewertete.[17] Laut diesem Bericht garantiert

16 Richtlinie 2006/24/EG, ABl. L 105 vom 13.4.2006.
17 Europäische Kommission (2011b).

die Richtlinie selbst nicht, dass auf Vorrat gespeicherte Daten in voller Übereinstimmung mit dem Recht auf Privatsphäre und Schutz personenbezogener Daten gespeichert, abgerufen und verwendet werden. Der Kommission zufolge war das Ziel der Richtlinie lediglich eine teilweise Harmonisierung der Herangehensweise an die Vorratsdatenspeicherung. Daher ist das Fehlen eines gemeinsamen Ansatzes der EU-Mitgliedstaaten – sei es in Bezug auf konkrete Vorschriften der Richtlinie wie etwa die Speicherfristen oder in Bezug auf Aspekte außerhalb ihres Anwendungsbereichs wie die Erstattung der Kosten für obligatorische Vorratsdatenspeicherung – nicht verwunderlich.[18] Die Europäische Kommission gelangte zu dem Schluss, dass historische Kommunikationsdaten eine wichtige Rolle für strafrechtliche Ermittlungen spielen und dass die EU die Vorratsdatenspeicherung daher weiterhin als Sicherheitsmaßnahme unterstützen und regeln sollte.

Die Europäische Kommission konsultierte interessierte Gruppen zu Möglichkeiten für eine Änderung des Rechtsrahmens für die Vorratsdatenspeicherung. Der Europäische Datenschutzbeauftragte gelangte in seiner Stellungnahme zum *Bewertungsbericht* zur Richtlinie zu dem Schluss, dass die Richtlinie die Anforderungen nicht erfüllt, die durch die Grundrechte auf Privatsphäre und Datenschutz gestellt werden.[19]

> *„Die Richtlinie [über die Vorratsspeicherung von Daten] ist zweifellos das am meisten in die Privatsphäre eingreifende Instrument, das jemals von der EU im Hinblick auf Umfang und Anzahl der Menschen, die davon betroffen werden, angenommen wurde."*
>
> *Europäischer Datenschutzbeauftragter,* „Die Stunde der Wahrheit für die Richtlinie über die Vorratsspeicherung von Daten"*, Rede vom 3. Dezember 2010 in Brüssel*

Auf nationaler Ebene wurde diese Richtlinie von Deutschland, den Niederlanden, Rumänien, Schweden, der Tschechischen Republik und Zypern kritisiert. Am 22. März 2011 erklärte das Verfassungsgericht der **Tschechischen Republik** bestimmte nationale Bestimmungen[20] zur Umsetzung der Richtlinie für verfassungswidrig;[21] das entsprechende Verfahren war von einer Gruppe aus 51 Abgeordneten des tschechischen Parlaments angestrengt worden. Das Gericht bemängelte beispielsweise die Unverhältnismäßigkeit des Eingreifens der nationalen Rechtsvorschriften in das Recht auf Privatsphäre, das Fehlen einer eindeutigen Definition des Zwecks der Vorratsdatenspeicherung, das Fehlen einer ausdrücklichen Liste der Institutionen, die zum Zugriff auf die Daten berechtigt sind, das Fehlen einer Pflicht zur Information der betroffenen Personen und das Fehlen einer angemessenen Überprüfung der Rechtmäßigkeit. Auch in **Zypern** erklärte der Oberste Gerichtshof die nationalen Bestimmungen zur Umsetzung der Richtlinie über die Vorratsspeicherung von Daten für verfassungswidrig.[22] Im betreffenden Fall ging es darum, dass Polizeibeamte auf gerichtlichen Beschluss hin Zugang zu Telekommunikationsdaten erhalten. Der Gerichtshof befand, dass die Richtlinie über die Vorratsspeicherung von Daten die Mitgliedstaaten nicht verpflichtet, Rechtsvorschriften zu erlassen, die der Polizei den Zugang zu solchen Daten ermöglicht, da dies nicht in den Geltungsbereich der Richtlinie fällt. Der Gerichtshof stellte außerdem fest, dass die betreffenden gerichtlichen Beschlüsse vor einer Verfassungsreform gefasst wurden, die Ausnahmen vom Recht auf die Vertraulichkeit der Kommunikation vorsieht.

Zwei Ausschüsse des **niederländischen** Senats bekundeten in einem Brief an den Minister für Sicherheit und Recht vom 31. Mai 2011 ihre Enttäuschung über die Einschätzung der Europäischen Kommission bezüglich der Richtlinie über die Vorratsspeicherung von Daten.[23] Die Ausschüsse widersprachen der Kommission in mehreren Punkten. Sie bezeichneten die Bewertung als nicht zufriedenstellend, weil sie die Notwendigkeit der Richtlinie nicht nachgewiesen und der Angemessenheit der Vorratsdatenspeicherung nicht genügend Aufmerksamkeit gewidmet habe. Außerdem stellten die Ausschüsse die angewandte Methodik infrage und schlugen vor, die Richtlinie wieder zurückzuziehen.[24]

Deutschland beabsichtigt, die Richtlinie über die Vorratsspeicherung von Daten in deutsches Recht umzusetzen und dabei sowohl die Richtlinie selbst als auch die Bedingungen eines Urteils des Bundesverfassungsgerichts aus dem Jahr 2010 zu berücksichtigen.[25] Bislang konnte jedoch kein Konsens über einen neuen Gesetzesvorschlag erreicht werden. In Deutschland erklärte der Wissenschaftliche Dienst des Bundestages, es lasse sich keine Umsetzung dieser Richtlinie durchführen, die eine Vereinbarkeit mit der Grundrechte-Charta der EU zweifelsfrei sicherstelle.[26] Seine Zweifel betrafen insbesondere die wirtschaftliche Betätigungsfreiheit, da Unternehmen gemäß der Richtlinie verpflichtet wären, kostenintensive Strukturen für die Vorratsspeicherung von Kommunikationsdaten aufzubauen und zu pflegen. Ein weiteres Gutachten des Bundestages gelangte zu dem Schluss, dass die Vorratsdatenspeicherung die Auf-

18 *Ebenda*, S. 31.
19 Europäischer Datenschutzbeauftragter (2010).
20 Tschechische Republik, Gesetz über elektronische Kommunikation Nr. 127/2005 Coll., Abschnitte 3 und 4; Verordnung zur Umsetzung der Richtlinie über die Vorratsspeicherung von Daten.
21 Tschechische Republik, Verfassungsgericht, Entscheidung Nr. Pl ÚS 24/10, 22. März 2011.
22 Zypern, Oberster Gerichtshof, *Christos Matsias und andere*, Beschwerdesachen 65/2009, 78/2009, 82/2009, 15-22/2010, Entscheidung vom 1. Februar 2011.
23 Niederlande, Senat (2011a).
24 Niederlande, Senat (2011b).
25 Deutschland, Bundesverfassungsgericht (BVerfG), *1 BvR 256/08 vom 2.3.2010*, 2. März 2010.
26 Derksen, R. (2011).

klärungsquote von Straftaten in keinem EU-Mitgliedstaat deutlich erhöht habe.[27] Das Gutachten wies allerdings darauf hin, dass zu den Auswirkungen der Richtlinie auf die Aufklärungsquote von Straftaten keine statistischen Daten verfügbar sind. Auch der Bundesbeauftragte für Datenschutz und Informationsfreiheit verwies auf das Fehlen von Nachweisen dafür, dass die Aufdeckung von Straftaten durch die Vorratsdatenspeicherung deutlich zugenommen habe.[28] Demgegenüber hat die deutsche Bundespolizei Belege dafür veröffentlicht, dass sich das Fehlen der Vorratsdatenspeicherung nachteilig auf strafrechtliche Ermittlungen auswirkt.[29] Die Ergebnisse einer vom Bundesjustizministerium in Auftrag gegebenen und vom Max-Planck-Institut für ausländisches und internationales Strafrecht durchgeführten Studie stellen den Nutzen einer Vorratsdatenspeicherung in Frage. Die Ergebnisse dieser großangelegten Untersuchung wurden dem Rechtsausschuss des Deutschen Bundestages am 27. Januar 2012 vorgelegt.[30]

In **Schweden** wurde Ende 2010 ein Gesetzentwurf zur Umsetzung der Vorratsspeicherung von Daten eingebracht, der sich auf Verkehrsdaten bezieht.[31] Die Partei der Grünen, die Schwedendemokraten und die Linkspartei konnten jedoch mit ihrem Stimmenanteil die Umsetzung der Richtlinie verzögern. Sie wird dem Parlament frühestens am 17. März 2012 erneut vorgelegt. Auch in **Rumänien** hat das Plenum des Senats den neuen Gesetzesvorschlag am 21. Dezember 2011 einstimmig abgelehnt, nachdem das Verfassungsgericht das Gesetz zur Umsetzung in nationales Recht 2009 für verfassungswidrig erklärt hatte.[32]

3.3. Fluggastdatensätze

Fluggastdatensätze (*Passenger Name Record*, PNR) werden von den Fluggästen zur Verfügung gestellt, von den Fluggesellschaften erhoben und in deren Buchungs-/Abfertigungssystemen gespeichert. Kurz nach den Terroranschlägen vom 11. September 2001 erließen Länder außerhalb der EU Vorschriften, denen zufolge Fluggesellschaften, die Flüge in das, aus dem oder über das Gebiet der betreffenden Länder anbieten, deren Behörden die Fluggastdaten übermitteln müssen, die sie in ihren computergestützten Buchungssystemen gespeichert haben. Die frühzeitig vor dem Abflug übermittelten Fluggastdaten helfen Strafverfolgungsbehörden, die Fluggäste im Hinblick auf mögliche Verbindungen zum Terrorismus oder zu anderen Formen schwerer Kriminalität zu überprüfen.[33]

EU-Einrichtungen handelten im Jahr 2011 Abkommen mit verschiedenen Ländern über den Austausch von PNR-Daten aus. Das Europäische Parlament billigte das PNR-Abkommen zwischen der EU und Australien,[34] die Billigung des PNR-Abkommens zwischen der EU und den USA steht allerdings noch aus.[35] Diese Abkommen über Fluggastdaten ersetzen die früheren Abkommen aus den Jahren 2008 und 2007. Das Europäische Parlament forderte eine Änderung des Entwurfs des Abkommens mit den USA, um die Dauer der Datenspeicherung zu kürzen und um sicherzustellen, dass EU-Bürger Rechtsmittel gegen Reisesperren im Zusammenhang mit PNR-Daten einlegen können.[36] Der Europäische Datenschutzbeauftragte gab zu beiden Abkommen Stellungnahmen ab.[37] Er begrüßte die Schutzmaßnahmen in Bezug auf Datensicherheit und Aufsicht, die in beiden Abkommen vorgesehen sind, äußerte jedoch auch Bedenken hinsichtlich allgemeiner grundrechtlicher Grundsätze, wie Notwendigkeit und Verhältnismäßigkeit.

Im Februar veröffentlichte die Europäische Kommission einen neuen Vorschlag für eine Richtlinie über den Austausch von PNR-Daten zwischen EU-Mitgliedstaaten für Strafverfolgungszwecke.[38] Der Vorschlag für eine PNR-Richtlinie greift einen Gesetzesvorschlag aus dem Jahr 2007 auf, und zwar den Rahmenbeschluss über die Verwendung von Fluggastdatensätzen[39], der vor Inkrafttreten des Vertrags von Lissabon verabschiedet wurde. Mehrere Einrichtungen der EU äußerten Zweifel an der Verhältnismäßigkeit des Vorschlags angesichts seiner Auswirkungen auf das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten (Artikel 7, 8 und 52 der Charta der Grundrechte der Europäischen Union). Der Europäische Datenschutzbeauftragte betonte, dass die Notwendigkeit und Verhältnismäßigkeit dieses Systems, das eine großangelegte Sammlung von Fluggastdatensätzen zu Zwecken einer systematischen Bewertung aller Passagiere mit sich bringt, klar belegt werden müssen.[40] Die Empfehlungen des Europäischen Datenschutzbeauftragten betreffen die folgenden Aspekte des Vorschlags: Beschränkung des Anwendungsbereichs; Speicherfrist; Liste der zu speichernden Fluggastdaten; Stärkung der Grundsätze des Datenschutzes und Gewährleistung einer umfassenden Bewertung des Systems. Die Artikel-29-Datenschutzgruppe stellte die Notwendigkeit und Verhältnismäßigkeit von PNR-Systemen ebenfalls

27 Becher, J. (2011).
28 Deutschland, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (2011).
29 Deutschland, Bundesministerium des Innern (2011a).
30 Max-Planck-Institut für ausländisches und internationales Strafrecht (2012).
31 Schweden, Regierungsbehörden von Schweden (2010).
32 Rumänien, Verfassungsgericht Rumäniens, Entscheidung Nr. 1258, 8. Oktober 2009.
33 Europäische Kommission (2011c), S. 3.
34 Europäisches Parlament (2011a).
35 Rat der Europäischen Union (2011).
36 Europäische Kommission (2011d).
37 Europäischer Datenschutzbeauftragter (2011a); Europäischer Datenschutzbeauftragter (2011b).
38 Europäische Kommission (2011c).
39 Europäische Kommission (2007).
40 Europäischer Datenschutzbeauftragter (2011a).

in Frage und ersuchte um eine weitere Klärung des Anwendungsbereichs des Vorschlags.[41] Der Europäische Wirtschafts- und Sozialausschuss (EWSA) hielt die geplante Rechtsvorschrift für unverhältnismäßig, da die Notwendigkeit einer generellen und wahllosen Verwendung der Daten aller Fluggäste von internationalen Flügen in dem Vorschlag nicht ausreichend begründet wird.[42]

> *„Bevor neue Maßnahmen eingeführt werden, sollten die anwendbaren Maßnahmen für die Erhebung personenbezogener Daten für Strafverfolgungs- und Migrationskontrollzwecke bewertet und „Sicherheitslücken" ermittelt werden. Ein neuer Vorschlag über den Austausch von PNR-Daten sollte unbedingt eine umfassende Folgenabschätzung mit zuverlässigen und aktuellen Informationen über die Wirksamkeit, die Kosten und die Folgen für die genannten Grundrechte beinhalten."*
>
> *Schreiben des Ständigen Sachverständigenausschusses für internationales Zuwanderungs-, Flüchtlings- und Strafrecht (Meijers Committee) an die Kommissarin Cecilia Malström, Referenz CM1108, 21. Juni 2011, verfügbar unter: www.commissie-meijers.nl*

AKTIVITÄT DER FRA

Zweites Gutachten betreffend einen Vorschlag für eine Richtlinie über die Verwendung von Fluggastdatensätzen und seine Übereinstimmung mit den Grundrechten

Auf Ersuchen des Europäischen Parlaments erstellte die FRA ein Gutachten betreffend den neuen Vorschlag der Europäischen Kommission für eine PNR-Richtlinie und seine Übereinstimmung mit den Grundrechten.[43] Die FRA hatte bereits im Oktober 2008 auf Ersuchen des Rates der Europäischen Union ein erstes Gutachten zu Fluggastdatensätzen erstellt.

Im zweiten Gutachten werden Fragen im Hinblick auf die Grundrechte angesprochen, die sich auf Folgendes konzentrieren: die Risiken der mittelbaren Diskriminierung in Bezug auf die Profilerstellung und die Bedeutung der Erhebung geeigneter statistischer Daten zur Aufdeckung dieser Art der mittelbaren Diskriminierung, die Bedeutung der Grundsätze der Notwendigkeit und Verhältnismäßigkeit für die Wahrung der Grundrechte sowie die wirksame proaktive Überwachung, um die Rechte der Fluggäste sicherzustellen. Das Gutachten wird in den Erörterungen des Rates der Europäischen Union und des Europäischen Parlaments berücksichtigt werden.

Das **Vereinigte Königreich** unterstützt eine EU-PNR-Richtlinie, die eine Bestimmung für innergemeinschaftliche Flüge enthält. Die Regierung ist der Ansicht, dass klare Abkommen über Fluggastdatensätze zwischen der EU und Drittländern maßgeblich dazu beitragen, eine Situation der Rechtssicherheit für Fluggesellschaften zu schaffen, die Flüge in diese Länder anbieten. Außerdem fördern solche Abkommen den schnellen und sicheren Austausch von PNR-Daten unter Einhaltung aller erforderlichen datenschutzrechtlichen Garantien.[45] Der Sonderausschuss des britischen Oberhauses für EU-Angelegenheiten (Unterausschuss für innere Angelegenheiten) erklärte, Europa käme nicht um EU-weite Rechtsvorschriften umhin. Er vertritt die Ansicht, dass eine einheitliche Legislativmaßnahme die Erhebung von PNR-Daten auf Flügen in alle Mitgliedstaaten sowie den Austausch solcher Daten mit den Behörden anderer Mitgliedstaaten abdecken sollte.[46] Am 10. Mai äußerte der Einwanderungsminister des Vereinigten Königreichs in einer Erklärung vor dem britischen Unterhaus Bedenken bezüglich der Fluggastdatensätze, indem er die Notwendigkeit und Verhältnismäßigkeit der PNR-Daten in Frage stellte.[47]

In **Frankreich** erklärte der Innenminister, dass er die Schaffung eines europäischen PNR-Systems aktiv unterstütze, und gab bekannt, dass ein interministerielles Team aufgestellt worden sei, das die Einführung eines Systems für die Verarbeitung von Fluggastdatensätzen prüfen werde, das alle Länder außerhalb des Schengen-Raums abdeckt.[48] Es waren jedoch auch kritische Stimmen zu hören. Die französische Datenschutzbehörde veröffentlichte am 17. Februar 2011 eine Stellungnahme, in der sie betont, dass die Wirksamkeit des Systems noch nicht klar nachgewiesen worden sei, obwohl bereits seit vier Jahren ein PNR-Vorläufersystem getestet werde. Sie wies außerdem darauf hin, dass die Fehlalarmrate nach wie vor extrem hoch sei. Die französische Datenschutzbehörde äußerte jedoch ihre Bereitschaft, die aktuellen Tests fortzusetzen und damit eine künftige französische Plattform für die Verarbeitung von PNR-Daten im Kontext eines EU-weiten PNR-Systems vorzubereiten.[49]

In anderen Mitgliedstaaten, insbesondere in Österreich, der Tschechischen Republik und Rumänien, äußerten die Parlamente Zweifel bezüglich eines EU-Systems für die Erhebung und Analyse von PNR-Daten.

Österreich steht der Verwendung von Fluggastdatensätzen innerhalb der EU als zusätzliches Instrument im Kampf gegen den Terrorismus skeptisch gegenüber, eine Haltung, die von den Mitgliedern des Parlaments

41 Artikel-29-Datenschutzgruppe (2011).
42 EWSA (2011a).
43 Europäische Kommission (2011c).
44 Commission européenne (2011d).

45 Vereinigtes Königreich, Home Office (2011a).
46 Vereinigtes Königreich, House of Lords (2011), S. 7.
47 Vereinigtes Königreich, Home Office (2011b).
48 Frankreich, Le Fur (2010).
49 Frankreich, Datenschutzbehörde (2011).

aller politischen Parteien im April untermauert wurde. Dem Bundesinnenminister zufolge unterstützt Österreich ein solches System nur, wenn drei Bedingungen erfüllt sind: Die Lösungen müssen im Einklang mit den Menschenrechten stehen, die Verwendung von PNR-Daten muss bei der Terrorismusbekämpfung einen erheblichen Nutzen bringen, und die finanziellen und personellen Ressourcen müssen in einem angemessenen Verhältnis zum Wert des Systems stehen.[50] Der österreichische Datenschutzrat veröffentlichte im Februar 2011 eine Stellungnahme zum Vorschlag der EU für eine PNR-Richtlinie und wies darauf hin, dass die Speicherung personenbezogener Daten aller Fluggäste ohne begründeten Verdacht ein Eingreifen in das Recht auf Privatsphäre darstellt. In solchen Fällen müsse der Gesetzgeber die Angemessenheit und Notwendigkeit eines solchen Eingreifens eindeutig nachweisen. Nach Auffassung des Datenschutzrates weist der Vorschlag der EU eine solche Angemessenheit und Notwendigkeit nicht ausreichend nach.[51]

Im ersten Halbjahr 2011 appellierten der Senat[52] und die Abgeordnetenkammer der **Tschechischen Republik**[53] an die Regierung, bei der Ausarbeitung des PNR-Vorschlags das in der Verfassung verankerte Recht auf Privatsphäre genau einzuhalten. Beide gesetzgebenden Kammern vertraten die Ansicht, dass Straftaten im Zusammenhang mit Fluggastdatensätzen genauer definiert werden müssen, um die Verhältnismäßigkeit zu gewährleisten. Sie wiesen außerdem darauf hin, dass es keine weiteren Vorschriften für die Form gebe, in der die Daten gespeichert werden, und befanden die Speicherfrist für unangemessen. Die beiden Kammern lehnten es auch ab, die Pflicht zum Speichern und Übermitteln der Daten auf Flüge zwischen EU-Ländern auszudehnen.

Der **rumänische** Senat (*Senatul*) vertrat in einer Stellungnahme zum Vorschlag für eine PNR-Richtlinie[54] die Auffassung, dass der Vorschlag zwar mit dem Subsidiaritätsprinzip im Einklang steht, nicht aber mit dem Grundsatz der Verhältnismäßigkeit. Der Senat begründete seine Zweifel an der Verhältnismäßigkeit damit, dass seiner Ansicht nach die Definitionen einiger zu erfassender Datentypen unklar seien und dass schwerwiegende Entscheidungen nicht auf der Grundlage einer automatischen Verarbeitung der PNR-Daten getroffen werden sollten.[55] Ähnliche Bedenken wurden auch in Litauen[56], Portugal[57] und Deutschland[58] geäußert.

Die Debatte über die Wahrung der Grundrechte durch den Vorschlag für ein EU-PNR-System wird voraussichtlich im Jahr 2012 fortgesetzt.

3.4. Programm zum Aufspüren der Finanzierung des Terrorismus

Das Programm zum Aufspüren der Finanzierung des Terrorismus (*Terrorist Finance Tracking Programme*, TFTP) hat eine weitere wichtige Debatte in der EU ausgelöst, in deren Rahmen gefordert wird, dass Datenschutz und Sicherheitserwägungen in ein ausgewogenes Verhältnis gebracht werden. Diese Pläne sehen vor, dass den Sicherheitsdiensten Zahlungsverkehrsdaten aus bestimmten Zahlungsverkehrsdatendiensten übermittelt werden, bei denen es sich um sichere Plattformen handelt, die für Intra- und Interbankenanwendungen entwickelt wurden. Hinter dem Programm steckt die Grundidee, zur Bekämpfung des Terrorismus die Geldkanäle unter Verwendung allgemeiner, für internationale Finanztransaktionen entwickelter Verkehrsdatenstandards zurückzuverfolgen. Das Programm zum Aufspüren der Finanzierung des Terrorismus war ursprünglich ein Programm der US-Regierung und Teil ihres „globalen Kriegs gegen den Terror".

Unter dem TFTP-Abkommen[59] zwischen der EU und den USA, das 2010 in Kraft trat, ist Europol verpflichtet zu überprüfen, ob die Ersuchen der USA zur Übermittlung von Zahlungsverkehrsdaten gemäß den Bestimmungen dieses Abkommens verhältnismäßig und notwendig sind. Das Abkommen sieht einen regelmäßigen gemeinsamen Überprüfungsmechanismus vor, durch den die Umsetzung und Wirksamkeit des Abkommens einschließlich der darin für Europol vorgesehenen Rolle überwacht wird.[60] Im November 2010 stellte die gemeinsame Kontrollinstanz von Europol (GKI) im Zuge einer Inspektion fest, dass die schriftlichen Ersuchen, die bei Europol eingegangen waren, nicht spezifisch genug formuliert waren, um eine Entscheidung über ihre Genehmigung oder Ablehnung zu ermöglichen. Dennoch hatte Europol jedem eingegangenen Ersuchen stattgegeben.

50 Österreich, Parlament (2011).
51 Österreich, Datenschutzrat (2011).
52 Tschechische Republik, Senat, Entscheidung Nr. 207, 28. April 2011.
53 Tschechische Republik, Abgeordnetenkammer, Entscheidung Nr. 446, 28. April 2011.
54 Europäische Kommission (2011c).
55 Rumänien, Senat des rumänischen Parlaments (2011).
56 Litauen, Ausschuss für Europäische Angelegenheiten des Seimas (2011).
57 Portugal, Datenschutzbehörde (2011).
58 Deutschland, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (2011), S. 145.
59 Europäische Union, Vereinigte Staaten von Amerika (2010).
60 Gemeinsame Kontrollinstanz von Europol (2011).

„Europol hatte mitgeteilt, dass sich die Agentur bei der Prüfung der einzelnen Ersuchen auch auf mündlich bereitgestellte Informationen stützt. [...] Der erhebliche Umfang mündlicher Informationen macht eine angemessene interne und externe Revision durch die Datenschutzbehörde von Europol und die Gemeinsame Kontrollinstanz unmöglich."

Der Vorsitz der Gemeinsamen Kontrollinstanz (GKI) am 2. März 2011

Als der GKI-Bericht am 16. März 2011 im Ausschuss des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres erörtert wurde, äußerten Abgeordnete des Europäischen Parlaments schwerwiegende Bedenken im Hinblick auf den Datenschutz. Die Reaktion des Ausschusses sei von „Unzufriedenheit, Beunruhigung und Unbehagen" geprägt, erklärte der Ausschussvorsitzende, und fügte hinzu, dass „das EP [Europäische Parlament] die Umsetzung dieses Abkommens kontrollieren muss".[61] Nach Angaben des **deutschen** Bundesbeauftragten für den Datenschutz und die Informationsfreiheit standen die meisten Zahlungsverkehrsdaten, die an die US-Behörden übermittelt wurden und dort jahrelang gespeichert werden, in keinem Zusammenhang zum internationalen Terrorismus und drohten für andere Zwecke verwendet zu werden. Nach Ansicht des Bundesbeauftragten für den Datenschutz eignet sich Europol nicht als Kontrollbehörde für den Datenaustausch mit den USA, da es selbst Nutznießer dieses Austausches ist.[62]

Die Europäische Kommission veröffentlichte die erste gemeinsam von der EU und den USA vorgenommene Überprüfung des TFTP, die, wie im Abkommen vorgesehen, im März 2011 stattfand.[63] Im gemeinsamen Bericht über diese Überprüfung wird festgestellt, dass Europol seine Aufgaben mit großer Ernsthaftigkeit erfüllt und die notwendigen Vorkehrungen getroffen hatte, um ihnen professionell und im Einklang mit dem Abkommen nachzukommen. Dennoch stimmte der Bericht der GKI darin zu, dass „offenbar noch Spielraum für genauere und zielgerichtetere Begründungen für die Ersuchen besteht", die Europol in die Lage versetzen würden, „seine Aufgaben noch effektiver zu erfüllen".[64] Der gemeinsame Bericht enthält mehrere Empfehlungen, die die Umsetzung des Abkommens weiter verbessern sollen, und kommt vor allem zu dem Schluss, dass mehr Transparenz in Bezug auf den zusätzlichen Nutzen, den das Programm für die Terrorismusbekämpfung bringt, in Bezug auf die Gesamtmengen der betreffenden Daten und in Bezug auf andere wichtige Aspekte erheblich dazu beitragen würde, ein breiteres Publikum vom tatsächlichen Nutzen des TFTP und des Abkommens zu überzeugen und das Vertrauen in das Programm zu stärken. Wo immer möglich, sollte eine solche Transparenz angestrebt werden, ohne die Wirksamkeit des Programms zu gefährden.

Als Reaktion auf das Ersuchen des Europäischen Parlaments und des Rates der Europäischen Union stellte die Europäische Kommission im Juli verschiedene Optionen für ein EU-System zum Aufspüren der Terrorismusfinanzierung (EU-TFTS) vor.[65] Die Mitteilung der Europäischen Kommission wurde einmal kurz im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments erörtert, aber nicht weiter behandelt. Der Rat der Europäischen Union hielt mehrere Diskussionsrunden ab, unter anderem auf Ministerebene, wobei vor allem die Kosten eines künftigen EU-TFTS und seine Vereinbarkeit mit dem bestehenden Abkommen mit den Vereinigten Staaten von Amerika erörtert wurden.

Die Mitteilung betont die Notwendigkeit, dass die Grundrechte, insbesondere das Recht auf Datenschutz, uneingeschränkt eingehalten werden müssen. Auf Ebene der EU-Mitgliedstaaten wurde zu diesem Thema noch keine Einigung erzielt. Die Regierung des **Vereinigten Königreichs** hob hervor, dass sie sich dem bestehenden TFTP vollständig verpflichtet fühle, aber der Ansicht sei, dass die grundlegende Frage noch zufriedenstellend beantwortet werden müsse, weshalb überhaupt ein EU-TFTS eingerichtet werden müsse. Nach Angaben des **deutschen** Bundesbeauftragten für den Datenschutz und die Informationsfreiheit würde der Vorschlag der Europäischen Kommission ähnliche Grundsätze verfolgen wie das Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika und zu einer Massenspeicherung von Daten führen, die zum Großteil unverdächtige Personen betreffen.[66]

3.5. Körperscanner

Der Einsatz von Körperscannern (oder „Sicherheitsscannern" – so der Begriff, den die Europäische Kommission in ihrer Mitteilung aus dem Jahr 2010 *über den Einsatz von Sicherheitsscannern auf EU-Flughäfen* verwendete)[67] war 2011 wegen der Auswirkungen ihres Einsatzes auf die Würde und Privatsphäre des Menschen ein umstrittenes Thema. Das Europäische Parlament[68] und der Europäische Wirtschafts- und Sozialausschuss[69] hielten Anhörungen in dieser Angelegenheit ab. Ende 2011 verabschiedete die Europäische Kommission Rechtsvorschriften über den Einsatz von

61 Europäisches Parlament (2011b).
62 Deutschland, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (2011).
63 Europäische Kommission (2011e).
64 *Ebenda*, S. 12.
65 Europäische Kommission (2011f).
66 Deutschland, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (2011).
67 Europäische Kommission (2010c).
68 Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) (2010).
69 EWSA (2011b).

Körperscannern an EU-Flughäfen.[70] Der Europäische Datenschutzbeauftragte kritisierte die Annahme der neuen Rechtsvorschriften über ein Regelungsverfahren, weil die Vorschläge mehr als rein technische Maßnahmen enthalten, da sie Auswirkungen auf die Grundrechte haben.[71]

AKTIVITÄT DER FRA

Körperscanner und Grundrechte

Die FRA stellte ihr Gutachten *The use of body scanners: 10 questions and answers* (Der Einsatz von Körperscannern: 10 Fragen und Antworten) im Januar 2011 auf einer vom Europäischen Wirtschafts- und Sozialausschuss veranstalteten Anhörung vor. Darin empfahl sie die folgenden praktischen Maßnahmen zur Wahrung der Grundrechte der Fluggäste: Die Bilder werden von einer Kontrollperson geprüft, die räumliche Distanz zu der kontrollierten Person hat; die Bilder werden nicht gespeichert oder archiviert; das Gesicht der kontrollierten Person wird unkenntlich gemacht, damit die erzeugten Bilder anonymisiert sind; die verwendeten Scanner erzeugen ein genormtes Bild des Körpers (mimic board), damit keine Bilder, sondern Ergebnisse angezeigt werden. Laut FRA-Gutachten sollten die Fluggäste wählen können, ob die Kontrolle durch Körperscanner oder konventionellere Sicherheitsprüfungen wie Abtasten erfolgen soll. Hierzu sollten sie vorab vollständig unterrichtet werden, damit sie eine fundierte Entscheidung treffen können.

Die Rechtsvorschriften erlauben es den EU-Mitgliedstaaten und Flughäfen, Körperscanner unter bestimmten Bedingungen, die Bedenken in Bezug auf die Grundrechte berücksichtigen, als eine mögliche Methode der Fluggastkontrolle an EU-Kontrollpunkten einzusetzen und zu verwenden. Sicherheitsscanner dürfen beispielsweise nicht dazu dienen, Bilder zu speichern, zurückzuhalten, zu kopieren, auszudrucken oder abzurufen; jeder unbefugte Zugang zum Bild sowie seine unbefugte Verwendung ist untersagt und zu verhindern; der menschliche Überprüfer, der das Bild auswertet, muss sich an einem Ort befinden, von dem aus er den kontrollierten Fluggast nicht sehen kann, und das Bild darf nicht mit Daten verknüpft werden, die die kontrollierte oder eine andere Person betreffen. Die Fluggäste müssen über die Bedingungen unterrichtet werden, unter denen die Kontrollen mit dem Sicherheitsscanner erfolgen. Außerdem erhalten die Fluggäste das Recht, die Kontrolle mit dem Scanner zu verweigern und sich einer alternativen Kontrollmethode zu unterziehen.[72]

70 Verordnung (EU) Nr. 1141/2011 der Kommission; Durchführungsverordnung (EU) Nr. 1147/2011 der Kommission.
71 Europäischer Datenschutzbeauftragter (2011c).
72 Europäische Kommission (2011g).

> *„Sicherheitsscanner sind kein Allheilmittel, bieten aber die Möglichkeit, die Fluggastsicherheit zu verbessern. Sie sind eine wertvolle Alternative zu bestehenden Methoden und höchst wirksam beim Aufspüren sowohl metallischer als auch nichtmetallischer Gegenstände. Die Entscheidung über die Einführung von Sicherheitsscannern liegt im Ermessen jedes Mitgliedstaats oder Flughafens. Die neuen Regeln stellen jedoch sicher, dass diese neue Technologie dort, wo sie zum Einsatz kommt, EU-weiten Normen zur Detektionsfähigkeit sowie strengen Garantien in Bezug auf den Gesundheitsschutz und die Wahrung der Grundrechte unterliegt."*
>
> *Der für Verkehr zuständige Vizepräsident der Europäischen Kommission Siim Kallas, Pressemitteilung IP/11/1343, 14. November 2011*

Es wird erwartet, dass die EU-Mitgliedstaaten weiterhin unterschiedliche Ansätze verfolgen. In **Italien** beispielsweise wurde Anfang 2011 an drei Flughäfen (Rom Fiumicino, Mailand Malpensa und Venedig) eine zweite Testphase mit einer neuen Technologie eingeleitet[73], die jedoch erst seit Mai an nur zwei der drei Flughäfen (Rom und Mailand) eingesetzt wird[74]. Die erste Testphase fand im Jahr 2010 statt (Rom Fiumicino, Mailand Malpensa, Venedig und Palermo). Der Nationalen Behörde für Zivilluftfahrt[75] zufolge haben die getesteten Sicherheitsscanner keine Auswirkungen auf die Gesundheit und gewährleisten die Wahrung der Privatsphäre der Fluggäste. Die ermittelten Ergebnisse entsprächen jedoch angesichts der Fehlalarme und der langen Abfertigungszeiten nur teilweise den Erwartungen. Der **deutsche** Bundesinnenminister entschied aufgrund von Feldversuchen, an deutschen Flughäfen vorerst auf den Einsatz von Ganzkörperscannern zu verzichten. Während der Feldversuche mit zwei Ganzkörperscannern am Flughafen Hamburg wurde deutlich, dass die Technologie noch nicht so ausgereift ist, dass die verfügbaren Geräte im Alltag einsetzbar sind.[76] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit vertritt die Ansicht, dass der rechtmäßige Einsatz von Körperscannern die Erfüllung der folgenden Bedingungen voraussetzt: Die Speicherung der Daten und die Anzeige der Körperkonturen auf dem Bildschirm sind auszuschließen.[77]

Bedenken in Bezug auf das Recht auf Privatsphäre, den Datenschutz, die Würde und mögliche Gesundheitsrisiken wurden auch in Schweden[78] und Slowenien[79] geäußert.

73 Italien, Nationale Behörde für Zivilluftfahrt (2010).
74 Italien, Nationale Behörde für Zivilluftfahrt (2011).
75 *Ebenda*.
76 Deutschland, Bundesinnenminister (2011b).
77 Deutschland, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (2011).
78 Schweden, Justizausschuss des schwedischen Parlaments (2010).
79 Slowenien, Innenministerium (2010); Slowenien, Datenschutzbeauftragter (2011).

3.6. Soziale Netzwerke

Die Nutzung, Speicherung und Übertragung personenbezogener Daten durch soziale Netzwerke ist aufgrund der persönlichen Natur der betroffenen Daten und den daraus resultierenden Auswirkungen auf das Recht auf Privatsphäre zu einem weiteren zentralen Thema öffentlicher Debatten geworden.

Die Datenschutzbehörden in den nordischen Ländern stellten Facebook rund 40 Fragen über den Umgang des Unternehmens mit personenbezogenen Daten. Facebook beantwortete die Fragen im September[80] und bestätigte, dass das Unternehmen anhand von Informationen aus Statusaktualisierungen der Nutzer und „Gefällt mir"-Angaben gezielte Werbung anzeigen kann. Das Unternehmen versicherte jedoch, dass es anderen Unternehmen gegenüber keine personenbezogenen Daten offenlege, mit Ausnahme der Daten, die der Nutzer bereit sei, im Rahmen der Installation von Anwendungen preiszugeben. Facebook ist der Ansicht, dass das Unternehmen den europäischen Datenschutzvorschriften unterliegt, da sich seine Hauptniederlassung in Irland befindet.[81]

Die österreichische Gruppe „Europe versus Facebook" sah sich in ihrem Recht auf Privatsphäre verletzt und reichte im August beim irischen Datenschutzbeauftragten 22 Beschwerden gegen Facebook Ireland ein, der Niederlassung, die für alle Tätigkeiten von Facebook außerhalb der USA und Kanada verantwortlich ist. Die Beschwerden umfassten Folgendes: Bei Anklicken der Schaltfläche „Gefällt mir" werden Daten erstellt, anhand derer die Nutzer zurückverfolgt werden können; „Tags" (Suchbegriffe) können ohne Zustimmung des Nutzers angewendet werden; „Pokes" (Anstups-Funktion), Meldungen, Bilder und Nachrichten sind auch nach ihrer Löschung noch sichtbar.[82] Im September gab der irische Datenschutzbeauftragte seine Absicht bekannt, diesen Beschwerden nachzugehen und eine Untersuchung durchzuführen.[83] Da sich die internationale Hauptniederlassung von Facebook in Irland befindet, wird der irische Datenschutzbeauftragte alle Tätigkeiten untersuchen, die den irischen und europäischen Datenschutzvorschriften unterliegen. Alle Entscheidungen des Datenschutzbeauftragten könnten Auswirkungen für Millionen von Nutzern weltweit haben.

Die folgenden Themen riefen in den EU-Mitgliedstaaten Bedenken in Bezug auf soziale Netzwerke hervor: Unsicherheit über den privaten oder öffentlichen Status von Meldungen, die in sozialen Netzwerken veröffentlicht werden; die Erstellung von Profilen und Rückverfolgung von Nutzern in sozialen Netzwerken; der mangelnde Schutz von Kindern in sozialen Netzwerken.

In **Frankreich** entschied das Arbeitsgericht in Boulogne-Billancourt am 19. November 2010 in einer Rechtssache in Bezug auf den öffentlichen Charakter von Meldungen, die in sozialen Netzwerken veröffentlicht werden. Die Rechtssache betraf drei Mitarbeiter, die entlassen wurden, weil sie ihre Vorgesetzten auf Facebook kritisiert hatten.[84] Das Gericht befand, dass die im sozialen Netzwerk verfassten Kommentare für die Öffentlichkeit zugänglich waren, da sie für „Freunde von Freunden" zugänglich waren. Die Nachrichten waren nicht mehr privat, da Personen darauf zugreifen konnten, die nicht an der Diskussion beteiligt waren. Daher wurde die Entlassung als begründet angesehen. Es besteht allerdings einige Unsicherheit hinsichtlich der Rechtsprechung in dieser Angelegenheit. Der Staatsanwalt von Périgueux beispielsweise kam in einem ähnlichen Fall zu einem anderen Schluss. Er vertrat die Auffassung, dass die Meldungen von zwei Mitarbeitern über ihre Vorgesetzten in ausreichendem Maße geschützt waren, um als privat angesehen zu werden, da sie nur für die Kontakte des betreffenden Mitarbeiters sichtbar waren und nicht für den zweiten Kreis der Kontakte.[85] Die Unternehmen der Branche haben schnell auf diese Rechtsunsicherheit reagiert. Am 30. Juni startete Google die Plattform Google+, ein weiteres soziales Netzwerk, in dem Nachrichten mit verschiedenen Kreisen („Circles") geteilt werden können, die der Nutzer festlegt. Am 13. September führte Facebook neue Werkzeuge ein, die es den Nutzern ermöglichen, ihre Listen der „Freunde" zu strukturieren und damit besser zu kontrollieren, welche Informationen geteilt werden.[86] Dennoch bleibt relativ unsicher, ob die in sozialen Netzwerken erfassten Nachrichten öffentlicher oder privater Natur sind.

Auf Initiative des unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein mussten in Schleswig-Holstein angesiedelte **deutsche** Internetseiten bis Ende September die Facebook-Schaltfläche „Gefällt mir" entfernen, ansonsten drohte ihnen ein Bußgeld in Höhe von bis zu 50 000 EUR. Die Sorge war, dass diese Schaltfläche verwendet würde, um Nutzer zurückzuverfolgen und Nutzerprofile zu erstellen.[87]

80 Norwegen, Datenschutzkommission (2011).
81 Schweden, Datenschutzkommission (2011).
82 Weitere Informationen unter: www.europe-v-facebook.org.
83 Siehe auch: http://m.zdnet.com/blog/facebook/irish-dataprotection-commissioner-to-begin-facebook-audit/4262, abgerufen am 14. Oktober 2011.

84 Frankreich, Arbeitsgericht Boulogne-Billancourt, 19. November 2010, *Mme. B./SAS Alten Sir*; *Mme. S./SAS Alten Sir*.
85 Le Monde (2011a).
86 Le Monde (2011b).
87 Deutschland, Landesbeauftragter für Datenschutz Schleswig-Holstein (2010).

> *„Die Formulierungen in den Nutzungsbedingungen und Datenschutzrichtlinien von Facebook genügen nicht annähernd den rechtlichen Anforderungen an gesetzeskonforme Hinweise, an wirksame Datenschutzeinwilligungen und an allgemeine Geschäftsbedingungen."*
>
> *Deutschland, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*

Die **spanische** Datenschutzbehörde äußerte ihre Bedenken in Bezug auf die steigende Zahl der gemeldeten Verletzungen der Privatsphäre in sozialen Netzwerken, insbesondere bei Kindern (40 im Jahr 2010 gegenüber 32 im Jahr 2009). Zur Lösung dieses Problems kam die spanische Datenschutzbehörde mit Vertretern wichtiger sozialer Netzwerke wie Tuenti und Facebook zusammen, um deren Datenschutzkonzepte zu verbessern und Kindern unter 14 Jahren den Zugang zu solchen Netzwerken zu verwehren.

Tuenti versprach daraufhin, bis zu 300 000 Profile pro Jahr zu überprüfen und die Profile von Kindern unter 14 Jahren zu entfernen. Facebook gab auf Ersuchen der spanischen Datenschutzbehörde bekannt, dass das Unternehmen das Mindestalter für den Zugang zum Netzwerk in Spanien auf 14 Jahre anheben werde. Darüber hinaus versprach Facebook, bessere Kontrollen zu entwickeln und verschiedene Optionen für ein Altersverifikationssystem in Kombination mit einem System für die Zustimmung der Eltern zu prüfen.[88]

Ausblick

Institutionen und Mitgliedstaaten der EU werden weiterhin vor dem Problem stehen, den Schutz der Grundrechte und Sicherheitserwägungen in ein ausgewogenes Verhältnis zu bringen. Die laufende Diskussion über die Richtlinie zur Vorratsdatenspeicherung wird einen Aspekt dieser umfassenden Debatte darstellen.

Die EU-Institutionen werden die Debatte über den EU-Rahmen für den Datenschutz fortsetzen. Im Januar 2012 unterbreitete die Europäische Kommission Vorschläge zur Reform des aktuellen Rahmens. Sie bestehen aus einem Vorschlag für eine Verordnung, welche die Datenschutzrichtlinie aus dem Jahr 1995 ablösen soll, und für eine neue Verordnung zur Regelung des Schutzes personenbezogener Daten, die zu Zwecken der Verhütung, Aufdeckung, Aufklärung oder Verfolgung von Straftaten und damit zusammenhängender Tätigkeiten der Justiz verarbeitet werden.

Die Haltung zum Schutz der Daten von Benutzern und Anbietern sozialer Plattformen und anderer Online-Tools wird auch weiterhin für hitzige Debatten in der Öffentlichkeit sorgen und dürfte zunehmend zum Gegenstand gerichtlicher Auseinandersetzungen werden. Die Verfügbarkeit und Nutzung von Rechtsbehelfen muss sorgfältig geprüft werden, um zu gewährleisten, dass die Grundrechte beim Einsatz neuer Informations- und Kommunikationstechnologien in vollem Umfang gewahrt bleiben.

Wahrscheinlich wird sich der EuGH erneut mit einem weiteren Problembereich befassen: der Unabhängigkeit der Datenschutzbehörden.

88 Spanien, spanische Datenschutzbehörde (2011a), S. 28.

Quellennachweise

Artikel-29-Datenschutzgruppe (2011), *Stellungnahme 10/2011 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität*, 00664/11/DE WP 181, 5. April 2011.

Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) (2010), *Sitzung des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres über jüngste Entwicklungen in der Terrorismusbekämpfung*, Europäisches Parlament, Brüssel, 27. Januar 2010.

Becher, J. (2011), *Die praktischen Auswirkungen der Vorratsdatenspeicherung auf die Entwicklung der Aufklärungsquoten in den EU-Mitgliedstaaten*, WD 7 – 3000 – 036/11, März 2011.

Bigo, D., Carrera, S., González Fuster, G., Guild, E., De Hert, P., Jeandesboz, J. und Papakonstantinou, V. (2011), *Towards a new EU legal framework for data protection and privacy: challenges, principles and the role of the European Parliament*, Studien des Europäischen Parlaments, Brüssel, 15. September 2011.

Derksen, R. (2011), *Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta*, WD 11 – 3000 – 18/11, Februar 2011.

Deutschland, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (2011), Jahresbericht 2009/10.

Deutschland, Bundesministerium des Innern (2011a), *Studie des BKA bekräftigt Notwendigkeit von Mindestspeicherfristen*.

Deutschland, Bundesministerium des Innern (2011b), „Körperscanner im Test: Leistungsfähig, aber noch nicht flächendeckend einsetzbar", Pressemitteilung, 31. August 2011.

Deutschland, Bundesverfassungsgericht (BVerfG), *1 BvR 256/08 vom 2.3.2010*, 2. März 2010.

Deutschland, Landesbeauftragter für Datenschutz Schleswig-Holstein (2010), *Sicherheits- und Datenschutzziele miteinander in Einklang bringen*, Interview, 17. September 2010.

Durchführungsverordnung (EU) Nr. 1147/2011 der Kommission vom 11. November 2011 zur Änderung der Verordnung (EU) Nr. 185/2010 zur Durchführung der gemeinsamen Grundstandards in der Luftsicherheit bezüglich des Einsatzes von Sicherheitsscannern an EU-Flughäfen, ABl. L294 vom 12.11.2011, S. 7.

Europäische Kommission (2007), *Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken*, KOM(2007) 654 endgültig, Brüssel, 6. November 2007.

Europäische Kommission (2010a), *Gesamtkonzept für den Datenschutz in der Europäischen Union*, KOM(2010) 609 endgültig, Brüssel, 4. November 2010.

Europäische Kommission (2010b), *Datenschutz: Kommission verklagt Österreich wegen unzureichender Unabhängigkeit seiner Datenschutzbehörde*, Pressemitteilung IP/10/1430, 28. Oktober 2010.

Europäische Kommission (2010c), *Mitteilung der Kommission an das Europäische Parlament und den Rat über den Einsatz von Sicherheitsscannern auf EU-Flughäfen*, KOM(2010) 311 endgültig, Brüssel, 15. Juni 2010.

Europäische Kommission (2011a), *Attitudes on Data Protection and Electronic Identity in the European Union*, Eurobarometer Spezial 359, Brüssel, 16. Juni 2011.

Europäische Kommission (2011b), *Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG)*, KOM(2011) 225, Brüssel, 18. April 2011.

Europäische Kommission (2011c), *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität*, KOM(2011) 32 endgültig, Brüssel, 2. Februar 2011.

Europäische Kommission (2011d), *Entwurf des Abkommens zwischen der EU und den USA über die Verwendung von Fluggastdatensätzen*, SJ (2011) 603245, Juristischer Dienst, 18. Mai 2011.

Europäische Kommission (2011e), *Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, Commission staff working paper*, SEC(2011) 438 final, Brüssel, 30. März 2011.

Europäische Kommission (2011f), *Optionen für ein EU-System zum Aufspüren der Terrorismusfinanzierung*, KOM(2011) 429 endgültig, Brüssel, 13. Juli 2011.

Europäische Kommission (2011g), „Luftsicherheit: Kommission verabschiedet neue Regeln zum Einsatz von Sicherheitsscannern auf europäischen Flughäfen", Pressemitteilung IP/11/1343, 14. November 2011.

Europäische Kommission (2012), „Unabhängigkeit von Zentralbank und Datenschutzbehörden, Maßnahmen im Justizwesen: Europäische Kommission leitet beschleunigte Vertragsverletzungsverfahren gegen Ungarn ein", Pressemitteilung IP/12/24, Brüssel, 17. Januar 2012.

Europäische Union, Vereinigte Staaten von Amerika (2010), *Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus,* ABl. L 195 vom 27.7.2010, S. 5.

Europäischer Datenschutzbeauftragter (2010), *„Die Stunde der Wahrheit für die Richtlinie über die Vorratsspeicherung von Daten"*, Rede, Brüssel, 3. Dezember 2010.

Europäischer Datenschutzbeauftragter (2011a), *Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – „Gesamtkonzept für den Datenschutz in der Europäischen Union"*, 14. Januar 2011.

Europäischer Datenschutzbeauftragter (2011b), *Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für einen Beschluss des Rates über den Abschluss des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security*, 9. Dezember 2011.

Europäischer Datenschutzbeauftragter (2011c), *Schreiben von Herrn Giovanni Buttarelli, Stellvertretender Datenschutzbeauftragter, an Herrn Siim Kallas, Vizepräsident der Europäischen Kommission*, 17. Oktober 2011.

Europäischer Wirtschafts- und Sozialausschuss (EWSA) (2011a), *Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zu dem „Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität"*, SOC 414, 5. Mai 2011.

EWSA (2011b), *Report from Public Hearing on the Use of Security Scanners at Airports in the EU,* Brüssel, 11. Januar 2011.

Europäisches Parlament (2011a), *Legislative Entschließung zum Entwurf eines Beschlusses des Rates über den Abschluss des Abkommens zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an den Australian Customs and Border Protection Service,* P7_TA-PROV(2011)0470, 27. Oktober 2011.

Europäisches Parlament (2011b), „SWIFT implementation report: MEPs raise serious data protection concerns", Pressemitteilung, 16. März 2011.

Europarat (2010), Empfehlung des Ministerkomitees an die Mitgliedstaaten betreffend den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling, CM/Rec(2010)13, 23. November 2010.

Europarat (2011a), Der Beratende Ausschuss des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108) T-PD (2011) Fahrplan, 19. April 2011.

Europarat (2011b), *Report on the consultation on the modernisation of Convention 108 for the protection of individuals with regard to automatic processing of personal data*, T-PD-BUR(2011) 10 en, Straßburg, 21. Juni 2011.

Frankreich, Arbeitsgericht Boulogne-Billancourt, 19. November 2010, *Mme. B./SAS Alten Sir.*

Frankreich, Arbeitsgericht Boulogne-Billancourt, 19. November 2010, *Mme. S./SAS Alten Sir.*

Frankreich, Datenschutzbehörde (*Commission nationale de l'informatique et des libertés*, CNIL) (2011), *Délibération n° 2011-048 du 17 février 2011 portant avis sur un projet d'arrêté modifiant l'arrêté du 28 janvier 2009 pris pour l'application de l'article 7 de la loi n° 2006-64 du 23 janvier 2006 et visant à proroger l'expérimentation du « fichier des passagers aériens » (FPA) jusqu'au 31 décembre 2011 (demande d'avis n° 1183168V2)* CNIX1108803X, 31. März 2011.

Frankreich, Le Fur (2010), *Schriftliche Anfrage Nr. 91193 von Herrn Marc Le Fur an den Minister für innere Angelegenheiten, überseeische Gebiete und Lokalbehörden, 19. Oktober 2010, Antwort des Ministers für innere Angelegenheiten, überseeische Gebiete und Lokalbehörden*, verfügbar unter: http://questions.assemblee-nationale.fr/q13/13-91193QE.htm.

Gemeinsame Kontrollinstanz von Europol (2011), *US and EU agreement on exchanging personal data for the purposes of the Terrorist Finance Tracking Program (the TFTP Agreement) – first inspection performed by the Europol Joint Supervisory Body (JSB) raises serious concerns about compliance with data protection principles*, Pressemitteilung, Brüssel, 2. März 2011.

Gerichtshof der Europäischen Union (EuGH) Verbundene Rechtssachen C-468/10 und C-469/10, *ASNEF und FECEMD/Administración del Estado*, 24. November 2011.

EuGH, C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs*, 24. November 2011.

Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre (2010), Entschließung für einen Aufruf zur Veranstaltung einer Regierungskonferenz, auf der ein verbindliches internationales Instrument zur Privatsphäre und zum Schutz personenbezogener Daten entwickelt werden soll, verabschiedet am 29. Oktober 2010 in Jerusalem auf der 32. Internationalen Konferenz der Datenschutzbeauftragten, Israel 27.-29. Oktober 2010.

Italien, Nationale Behörde für Zivilluftfahrt (*Autorità per l'Aviazione Civile*) (2010), „In ENAC riunione cisa sui security scanner (body scanner): terminate prima fase sperimentazione senza risultati attesi", Pressemitteilung, 19. Dezember 2010.

Italien, Nationale Behörde für Zivilluftfahrt (*Autorità per l'Aviazione Civile*) (2011), „Messa a punto dei security scanner L3 provision sugli aeroporti di Roma Fiumicino e Milano Malpensa", Pressemitteilung, 9. Mai 2011.

Konferenz der europäischen Datenschutzbeauftragten (2011), *Entschließung über die Notwendigkeit eines umfassenden Rahmens für den Datenschutz,* Brüssel, 5. April 2011.

Le Monde (2011a), *Darf man den Chef auf Facebook beleidigen?*, 10. März 2011.

Le Monde (2011b), *Facebook schlägt Strukturierung der Freundeslisten vor*, 14. September 2011.

Litauen, Ausschuss für Europäische Angelegenheiten des Seimas (*Lietuvos Respublikos Seimo Europos reikalų komitetas*) (2011), *Komiteto Išvados*, 2011.

Max-Planck-Institut für ausländisches und internationales Strafrecht (2012), *Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO*, Forschungsbericht im Auftrag des Bundesministeriums der Justiz, 27. Januar 2012.

Niederlande, Senat (*Eerste Kamer der Staten-Generaal*) (2011a), *E110022 - Evaluatierapport over de dataretentierichtlijn*.

Niederlande, Senat (*Eerste Kamer der Staten-Generaal*) (2011b), *Korte aantekeningen*, 5. Juli 2011.

Norwegen, Datenschutzkommission (2011), *Facebook beantwortet Fragen der norwegischen Datenschutzkommission, September 2011*.

Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) (2011a), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, OECD Digital Economy Paper Nr. 176, 6. April 2011.

OECD (2011b), Christopher Kuner, *Regulation of transborder data flows under data protection and privacy laws*, OECD Digital Economy Paper Nr. 187, 8. Dezember 2011.

Österreich, Datenschutzrat (2011), Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdaten für die Verhinderung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (Richtlinie EU-PNR): Stellungnahme des Datenschutzrates.

Österreich, Parlament (2011), V-19 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXIV. GP – Beratungen des Ständigen Unterausschusses des Hauptausschusses in Angelegenheiten der Europäischen Union, 5. April 2011.

Portugal, Datenschutzbehörde (*Comissão Nacional de Protecção de Dados*) (2011), Parecer Nr. 39, 9. Mai 2011.

Rat der Europäischen Union (2011), *Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security*, 17434/2011, 8. Dezember 2011.

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995.

Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 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. L 105 vom 13.4.2006.

Rumänien, Senat des rumänischen Parlaments (2011), *Mit Gründen versehene Stellungnahme zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität (KOM(2011) 32 endgültig)*, 6. April 2011.

Rumänien, Verfassungsgericht Rumäniens, Entscheidung Nr. 1258, 8. Oktober 2009.

Schweden, Datenschutzkommission (*Datainspektion*) (2011), *Facebook svarar de nordiska länderna*, 20. September 2011.

Schweden, Justizausschuss des schwedischen Parlaments (2010), *Vorschläge für eine Entschließung des Parlaments über den Einsatz von Körperscannern auf EU-Flughäfen* (2010/11:JuU4), 23. November 2010.

Schweden, Regierungsbehörden von Schweden (*Regeringskansliet*) (2010), *Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv*, Prop. 2010/11:46 2006/24/EG.

Slowenien, Datenschutzbeauftragter (*Informacijski pooblaščenec*) (2011), Interview mit einem Vertreter, 7. Oktober 2011.

Slowenien, Innenministerium (*Ministrstvo za notranje zadeve*) (2010), „Staatssekretär Goran Klemenčič nimmt an informeller Tagung des Rates „Justiz und Inneres" in Toledo teil", Pressemitteilung, 21. Januar 2010.

Spanien, spanische Datenschutzbehörde (*Agencia Española de Protección de Datos*) (2011), *Memoria 2010*, AEPD, 2011.

Tschechische Republik, Abgeordnetenkammer, Entscheidung Nr. 446, 28. April 2011.

Tschechische Republik, Gesetz über elektronische Kommunikation (*Zákon o elektronických komunikacích*) Nr. 127/2005 Coll.

Tschechische Republik, Senat, Entscheidung Nr. 207, 28. April 2011.

Tschechische Republik, Verfassungsgericht (*Ústavní soud*), Urteil Nr. Pl ÚS 24/10, 22. März 2011.

Vereinigtes Königreich, *European Scrutiny Committee* (2011c), *Terrorist Finance Tracking Systems*, London, 20. September 2011.

Vereinigtes Königreich, *Home Office* (2011a), *The UK's Opt-in to Council Decision to Sign and Conclude the EU-Australia PNR Agreement*, schriftliche Ministererklärung, 5. September 2011.

Vereinigtes Königreich, *Home Office* (2011b), „EU Directive on Passenger Name Records", Pressemitteilung, London, 10. Mai 2011.

Vereinigtes Königreich, *House of Lords* (2011), *The United Kingdom Opt-in to the Passenger Name Record Directive,* European Union Committee, 11th Report of Session 2010–11, HL Paper 113, The Stationery Office, London, 11. März 2011.

Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit, ABl. L 77 vom 13.3.2004.

Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung), ABl. L 218 vom 13.8.2008.

Verordnung (EU) Nr. 1077/2011 des Europäischen Parlaments und des Rates vom 25. Oktober 2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, ABl. L 286 vom 1.11.2011.

Verordnung (EU) Nr. 1141/2011 der Kommission vom 10. November 2011 zur Änderung der Verordnung (EG) Nr. 272/2009 zur Ergänzung der gemeinsamen Grundstandards für die Sicherheit der Zivilluftfahrt bezüglich des Einsatzes von Sicherheitsscannern an EU-Flughäfen, ABl. L 293 vom 11.11.2011, S. 22.

Zypern, Oberster Gerichtshof, *Christos Matsias und andere*, Beschwerdesachen 65/2009, 78/2009, 82/2009, 15-22/2010, Entscheidung vom 1. Februar 2011.