fassungsgesetzgeber zusinnbar ist. Aber dieser Streit ist ein alter Hut und in der Praxis nicht relevant. Die Ausnahme in Art 20 Abs 3 B-VG ist aus meiner Sicht genauso wenig schrankenlos, wie dies Art 52 B-VG ist. Beide werden durch das datenschutzrechtliche Regime begrenzt, so dass die Verwaltung sowohl nach der einen als auch nach der anderen Grundlage nur die Informationen weitergeben darf, die unbedingt erforderlich sind, um der Auskunftspflicht nachzukommen. Vertritt man nach Art 20 Abs 3 B-VG daher eine strenge Auffassung in Bezug auf die Bundesregierung, kann der Nationalrat jedes Informationsbedürfnis auch über Art 52 B-VG stillen.

*Hon.-Prof. Dr. Kurt Heller*

Dankeschön. Wenn keine weitere Frage mehr ist, dann schließe ich die heutige Nachmittagsveranstaltung. Es geht morgen wieder hier weiter um 9.00 Uhr Früh. Dankeschön.

*Univ.-Prof. DDr. Christoph Grabenwarter*

Einen schönen guten Morgen, meine Damen und Herren! Ich darf Sie zur zweiten Sitzung der Öffentlich-Rechtlichen Abteilung sehr herzlich begrüßen. Wir werden heute fortsetzen mit dem zweiten Referat, jenem von Prof. Merli, der sich mit den europa- und internationalrechtlichen Aspekten beschäftigen wird. Wir begrüßen neu Hinzugekommene, jetzt nicht nur den ehemaligen Richter am Gerichtshof der Europäischen Union Peter Jann, sondern auch die amtierende Richterin Maria Berger. Wir setzen heute unmittelbar nach dem Vortrag von Prof. Merli ohne eine Pause mit der Diskussion fort, dies aus Zeitgründen, weil wir dann noch das Referat von Präsident Pürstl am Vormittag hören werden. Prof. Merli ist Professor für öffentliches Recht an der Universität Graz, hat sich dort 1994 habilitiert, nach einem Forschungsaufenthalt in Heidelberg, wohin er nach der Habilitation für seine erste Professur zurückgekehrt ist. Dann war er einige Jahre als Professor an der Technischen Universität in Dresden tätig, seit 2006 ist er wieder in Graz. Prof. Merli ist vielen von uns bekannt als jemand, der über die gesamte Breite des öffentlichen Rechts publiziert hat, immer auch mit rechtsvergleichendem Bezug und mit Bezug zum Europarecht, das heißt, er ist der ideale Referent, um europa- und internationalrechtliche Dimension des Datenschutzrechts abzudecken, eine Dimension, die von größtmöglicher Dynamik geprägt ist. Wir haben vor uns Vorschläge für eine Richtlinie im Bereich des Schutzes natürlicher Personen bei der Verarbeitung Personen bezogener Daten zum Zweck der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten und für eine Datenschutzgrundverordnung – Reformschritte, die für das nationale Recht von eminenter Bedeutung sind, etwa in der Frage der Vorratsdatenspeicherung und ihrer Verfassungs- und Europarechtskonformität. Das Thema Vorratsdatenspeicherung wird, weil es von vielen Referaten berührt wird, am Ende der Diskussion gesondert behandelt. Nachdem Frau Prof. Reindl-Krauskopf, wie Sie ihrer Unterlage entnehmen können, auch über den Artikel 10a Staatsgrundgesetz sprechen möchte, wollen wir das für die Diskussion über ihren Vortrag aufsparen. Professor Merli, ich darf dich um dein Referat bitten.





*Univ.-Prof. Dr. Franz Merli*

Ja, Herr Vorsitzender, danke für die freundliche Vorstellung. Es wäre wahrscheinlich besser, wenn ich jetzt nichts mehr sagen würde, um den guten Eindruck nicht zu verderben, aber ich muss es wohl riskieren. Meine Damen und Herren! Meine Aufgabe besteht darin, das sehr anregende und mich sehr beeindruckende Gutachten, das Kollege Berka für uns erstellt hat, um die europäische Dimension zu ergänzen. Ich nähere mich dem Thema nicht abstrakt, sondern von der Anwendungsseite, mit der Frage, welche Aufgaben eigentlich ein Grundrecht auf Datenschutz zu bewältigen hat.

## Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit - Die europäische Dimension*

Spielt der Datenschutz angesichts unserer Sicherheitsregelungen noch eine nennenswerte Rolle? Da sich das ohne Einbeziehung der europäischen Ebene kaum feststellen lässt, schildert dieser Beitrag zunächst die Europäisierung von Sicherheitspolitik und Sicherheitsverwaltung (I.) und gibt einen Einblick in den vielfältigen Datenaustausch, der ihren Kern ausmacht (II.). Eine Antwort auf die Frage ergibt sich dann aus einer datenschutzrechtlichen Bewertung der derzeitigen Lage (III.) und einem Ausblick auf künftige Entwicklungen (IV.).

### I. Sicherheit als europäische Aufgabe[91]

Die Gewährleistung von innerer Sicherheit, also die Verhütung und Ahndung von Verbrechen, ist eine der klassischen Rechtfertigungen des Staates.[92] Einen Staat, der diese Aufgabe nicht einigermaßen bewältigt, halten wir zu recht für gescheitert. Das gilt seit langem und heute mehr denn je. Mehr denn je wird uns heute aber auch bewusst, dass diese Aufgabe kein Staat mehr allein leisten kann.

#### A. Gründe für die Europäisierung

Die Europäisierung hat mehrere Gründe. Die als Globalisierung bezeichnete übernationale Verflechtung vieler Lebensbereiche spart die Kriminalität nicht aus, und die zunehmende Mobilität von Menschen, Waren, Dienstleistungen und Kapital wie auch die Entwicklung von Techniken, die die persönliche

* Für umfangreiche Recherchearbeiten danke ich *Jürgen Pirker*.

91 Teil I folgt weitgehend *Merli*, Innere Sicherheit als eine europäische Aufgabe? in *Hiopoulos-Strangas/Diggelmann/Bauer* (Hrsg), Rechtsstaat, Freiheit und Sicherheit in Europa/Rule of Law, Freedom and Security in Europe/État de droit, liberté et sécurité en Europe, Societas Iuris Publici Europaei Bd 6 (2010) 367; dort auch umfassende Literaturnachweise. Außerdem: *Wollenschläger*, Die Gewährleistung von Sicherheit im Spannungsfeld der nationalen, unionalen und EMRK-Grundrechtsordnungen, ebenda, 45; *Schöndorf-Haubold*, Europäisches Sicherheitsverwaltungsrecht (2010); *Bruggemann/den Boer*, Policing and Internal Security in the Post-Lisbon Era: New Challenges Ahead, in *Wolff/Goudappel/de Zwaan* (Hrsg), Freedom Security and Justice after Lisbon and Stockholm (2011) 135.

92 *Berka*, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit (Gutachten zum 18.ÖJT, 2012) 98.

Anwesenheit der Akteure in vielen Fällen erübrigen, eröffnen neue Chancen auch für Verbrecher. Wenn Polizei und Strafverfolgungsbehörden dagegen nur auf nationaler Ebene agieren, geraten sie zwangsläufig ins Hintertreffen.

Das spricht für internationale Zusammenarbeit, aber noch nicht automatisch für Europäisierung. Die Europäische Union ist allerdings in zweifacher Hinsicht die nächstliegende Ebene der Kooperation. Zum einen hat sie einige der geschilderten Bedingungen, die grenzüberschreitendes Verbrechen erleichtern, selbst gefördert oder gar geschaffen, etwa ein Mehrwertsteuersystem, einen Stromhandelsmechanismus oder eine Mehrebenensubventionspolitik, die zu Betrug einladen, va aber einen „Raum ohne Binnengrenzen, in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital [...] gewährleistet ist"[93], in dem dann aber eben auch keine Personenkontrollen an den Binnengrenzen mehr stattfinden. Daher liegt es nahe, dass die Mitgliedstaaten, die vom Binnenmarkt und der Unionsbürgerfreizügigkeit profitieren, auch bei der Abwehr negativer Folgeerscheinungen zusammenarbeiten.

Zum anderen ist die Europäische Union unabhängig davon das Forum, das sich am besten für eine Sicherheitszusammenarbeit eignet. Die EU ist groß genug, um merkbare Kooperationsgewinne nach innen zu ermöglichen und gemeinsame Interessen nach außen wirksam zu vertreten. Sie setzt sich aus Mitgliedstaaten zusammen, die eine bestimmte Mindesthomogenität an Interessen, Kulturen und Rechtsgrundlagen aufweisen.[94] Sie verfügt über kooperationserprobte Mitglieder, Institutionen und Verfahren und über Erfahrung in vielen Formen der Koordinierung, gegenseitigen Unterstützung und Harmonisierung. Und sie ist unter allen in Frage kommenden Alternativen jene Organisation, die noch am ehesten die erforderliche demokratische und rechtsstaatliche Mindestqualität sichern kann.

## B. Entwicklung des Sicherheitsrechts

Aus diesen Gründen ist Sicherheit im letzten Jahrzehnt zu einer Kernaufgabe der EU geworden, nach außervertraglichen Anfängen über die Dritte Säule der EU und ihre Teilvergemeinschaftung in Amsterdam bis zur vollständigen Integration des Raums der Freiheit, der Sicherheit und des Rechts durch den Vertrag von Lissabon.[95] Ihre Bedeutung und Dynamik zeigt sich in den vertraglichen Grundlagen, die weiteres Wachstum vorsehen,[96] in den systematischen Ausbauplänen wie dem Stockholmer Programm,[97] in einer mittlerweile unübersehbaren Zahl von unmittelbar einschlägigen Sekundärrechtsakten und in einem institutionellen Ausbau, der sich etwa im Ständigen Ausschuss nach

93 Art 26 Abs 2 AEUV.
94 Vgl Art 2 EUV.
95 Übersicht und umfassende Nachweise zB bei *Suhr*, Art 67 AEUV, in *Callies/Ruffert* (Hrsg), EUV/AEUV[4] (2011).
96 ZB Art 68, 71 AEUV.
97 ABl 2010 C 115/1.





Art 71 AEUV, in OLAF[98], Europol[99] und Eurojust[100], im Europäische Justiziellen Netz[101], in Frontex[102], der Europäischen Beobachtungsstelle für Drogen und Drogensucht[103], der Task Force der Europäischen Polizeichefs[104] oder diversen Expertennetzwerke[105] zeigt. Bemerkenswert sind auch die Dominanz der Sicherheit gegenüber den anderen Komponenten des Raums der Freiheit, der Sicherheit und des Rechts und die Sicherheitsaufladung von anderen Politikbereichen, von Asyl über Telekommunikation und Verkehr bis zum Zoll.

## C. Europäisierung und Internationalisierung

Zur europäischen kommt die internationale Dimension, die für die Mitgliedstaaten oft wieder europäisch vermittelt auftritt. Die EU setzt Resolutionen des Sicherheitsrates der Vereinten Nationen zu den schwarzen Listen von Terrorverdächtigen um,[106] bezieht Drittstaaten in den Schengen-Raum ein,[107]

98 VO (EG) 1073/1999 des Europäischen Parlaments und des Rates vom 25.5.1999 über die Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF), ABl L 1999/136, 1.
99 Beschluss 2009/371/JI des Rates vom 6.4.2009 zur Errichtung des Europäischen Polizeiamts (Europol), ABl L 2009/121, 37.
100 Beschluss 2002/187/JI des Rates vom 28.2.2002 über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität, ABl L 2002/63, 1; Beschluss 2009/426/JI des Rates vom 16.12.2008 zur Stärkung von Eurojust und zur Änderung des Beschlusses 2002/187/JI über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität, ABl L 2009/138, 14.
101 Beschluss 2008/976/JI des Rates vom 16.12.2008 über das Europäische Justizielle Netz, ABl L 2008/348, 130.
102 VO (EG) 2007/2004 des Rates vom 26.10.2004 zur Errichtung einer Europäischen Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedstaaten der Europäischen Union, ABl L 2004/349, 1, geändert durch die VO (EG) 863/2007 des Europäischen Parlaments und des Rates über einen Mechanismus zur Bildung von Soforteinsatzteams für Grenzsicherungszwecke, ABl L 2007/199, 30.
103 VO (EWG) 302/93 des Rates vom 8.2.1993 zur Schaffung einer Europäischen Beobachtungsstelle für Drogen und Drogensucht, ABl L 1993/36, 1, zuletzt idF VO (EG) 1651/2003 des Rates vom 18.6.2003, ABl L 2003/ 245, 30.
104 Europäischer Rat von Tampere (15./16.10.1999), Schlussfolgerungen des Vorsitzes, Nr 44, www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/de/ec/00200-r1.d9.htm (Stand 8.12.2012).
105 ZB Beschluss 2006/581/EG der Kommission vom 7.8.2006 über die Einsetzung einer Expertengruppe zur Ermittlung des Bedarfs der Politik an Kriminalitäts- und Strafverfolgungsdaten, ABl L 2006/234, 29; Beschluss 2007/675/EG der Kommission vom 17.10.2007 über die Einsetzung der Sachverständigengruppe für Menschenhandel, ABl L 2007/277, 29.
106 ZB VO (EG) 881/2002 des Rates vom 27.5.2002 über die Anwendung bestimmter spezifischer restriktiver Maßnahmen gegen bestimmte Personen und Organisationen, die mit Osama bin Laden, dem Al-Qaida-Netzwerk und den Taliban in Verbindung stehen, und zur Aufhebung der VO (EG) 467/2001 des Rates über das Verbot der Ausfuhr bestimmter Waren und Dienstleistungen nach Afghanistan, über die Ausweitung des Flugverbots und des Einfrierens von Geldern und anderen Finanzmitteln betreffend die Taliban von Afghanistan, ABl L 2002/139, 9; DurchführungsVO (EU) 1002/2012 der Kommission vom 29.10.2012 zur 181. Änderung der VO (EG) 881/2002 des Rates über die Anwendung bestimmter spezifischer restriktiver Maß-

nimmt Klauseln über die Zusammenarbeit in der Terrorismusbekämpfung in Assoziationsabkommen auf,[108] schließt Abkommen mit Drittstaaten, etwa über Rechts- oder Amtshilfe[109] oder die Auslieferung von Verdächtigen und Straftätern[110], und bewirkt durch eine Mischung aus politischem Druck, finanzieller Hilfe, Visaerleichterungen und Rückführungsübereinkommen eine Vorverlagerung der Außengrenzkontrollen auf Nachbar- und Beitrittsstaaten[111].

Insgesamt ist also die Gewährleistung von Sicherheit zu einer genuin europäischen Aufgabe geworden, und die heutige Sicherheitspolitik und Sicherheitsverwaltung lassen sich ohne Einbeziehung der europäischen Dimension nicht mehr angemessen beschreiben.

## II. Die europäische Sicherheitsverwaltung als Datenverwaltung

Die europäische Sicherheitsverwaltung besteht nun zu einem großen Teil aus Datenverwaltung. Auf europäischer Ebene sind, wie zB die Beteiligung von Europol an Gemeinsamen Ermittlungsgruppen oder die Einsetzung von Soforteinsatzteams durch Frontex zeigen, unmittelbare operative Tätigkeit zwar nicht

nahmen gegen bestimmte Personen und Organisationen, die mit dem Al-Qaida-Netzwerk in Verbindung stehen, ABl L 2012/300, 43.

107 ZB Übereinkommen zwischen dem Rat der Europäischen Union sowie der Republik Island und dem Königreich Norwegen über die Assoziierung der beiden letztgenannten Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, ABl L 1999/176, 36; Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, ABl L 2008/53, 52; Protokoll zwischen der Europäischen Union, der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zu dem Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, ABl L 2011/160, 3.

108 ZB Art 90 Europa-Mittelmeer-Abkommen zur Gründung einer Assoziation zwischen der Europäischen Gemeinschaft und ihren Mitgliedstaaten einerseits und der Demokratischen Volksrepublik Algerien andererseits, ABl L 2005/265, 2; Art 7, 84, 87 Stabilisierungs- und Assoziierungsabkommen zwischen den Europäischen Gemeinschaften und ihren Mitgliedstaaten einerseits und der Republik Montenegro andererseits, ABl L 2010/108, 3.

109 ZB Abkommen über Rechtshilfe zwischen der Europäischen Union und den Vereinigten Staaten von Amerika, ABl L 2003/181, 34; Abkommen zwischen der Europäischen Union und Japan über die Rechtshilfe in Strafsachen, ABl L 2010/39, 20; Protokoll II über die gegenseitige Amtshilfe im Zollbereich zum Wirtschaftspartnerschaftsabkommen zwischen den CARIFORUM-Staaten einerseits und der Europäischen Gemeinschaft und ihren Mitgliedstaaten andererseits, ABl L 2008/289, 3.

110 ZB Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Auslieferung, ABl L 2003/181, 27.

111 Dazu *Weinzierl*, Flüchtlinge: Schutz und Abwehr in der erweiterten EU. Funktionsweise, Folgen und Perspektiven der europäischen Integration (2005); *Thrun*, Quid pro quo? EU-Rückübernahmeabkommen gegen Mobilitätserleichterungen, ZEuS 2008, 699; jeweils mwN.





von vornherein ausgeschlossen, doch bilden sie ganz eindeutig die Ausnahme. Im Regelfall geht es dagegen um Informationsaustausch und -verarbeitung.[112]

### A. Techniken

Das geschieht auf mehreren Wegen:

1. durch informationsverarbeitende Agenturen und Einrichtungen der EU wie Europol[113], Eurojust[114], Olaf[115] und Frontex[116];
2. über spezielle Informationssysteme wie das Schengen Informationssystem (SIS)[117], das Visa Informationssystem (VIS)[118], das Zollinformationssystem (ZIS)[119], Eurodac[120] (für den Bereich Asyl und illegale Einreise) oder das europäische Kriminalitätsregister ECRIS[121];
3. durch die generelle gegenseitige Verfügbarmachung mitgliedstaatlicher Daten gemäß der „Schwedischen Initiative“[122] oder dem „Prüm“-Beschluss[123];

112 Den besten Überblick, jedenfalls aus Datenschutzsicht, bietet *Boehm*, Information Sharing and Data Protection in the Area of Freedom, Security and Justice (2012). Zu operativen Tätigkeiten aus österr Sicht zB *Lachmayer*, Transnationales Polizeihandeln, JBl 2011, 409.

113 FN 99.

114 FN 100.

115 FN 98.

116 FN 102.

117 Beschluss 2007/533/JI des Rates vom 12.6.2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl 2007 L 205/63; VO (EG) 1987/2006 des Europäischen Parlaments und des Rates vom 20.12.2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl L 2006/381, 4.

118 VO (EG) 767/2008 des Europäischen Parlaments und des Rates vom 9.7.2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung), ABl L 2008/218, 60.

119 VO (EG) 515/97 des Rates vom 13.3.1997 über die gegenseitige Amtshilfe zwischen Verwaltungsbehörden der Mitgliedstaaten und die Zusammenarbeit dieser Behörden mit der Kommission im Hinblick auf die ordnungsgemäße Anwendung der Zoll- und der Agrarregelung, ABl L 1997/82, 1, zuletzt geändert durch VO (EG) 766/2008 des Europäischen Parlaments und des Rates vom 9.7.2008, ABl 2008 L 218/48.

120 VO (EG) 2725/2000 des Rates vom 11.12.2000 über die Einrichtung von „Eurodac“ für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens, ABl L 2000/316, 1; Geänderter Vorschlag zur Neuerlassung dieser VO, KOM (2012) 254 endg; VO (EG) 407/2002 des Rates vom 28.2.2002 zur Festlegung von Durchführungsbestimmungen zur VO (EG) 2725/2000 über die Einrichtung von „Eurodac“ für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens, ABl L 2002/62, 1;

121 Beschluss 2009/316/JI des Rates vom 6.4.2009 zur Einrichtung des Europäischen Strafregisterinformationssystems (ECRIS) gemäß Art 11 des Rahmenbeschlusses 2009/315/JI, ABl L 200993, 33.

122 Rahmenbeschluss 2006/960/JI des Rates vom 18.12.2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, ABl L 2006/386, 89.

4. durch die Verpflichtung der Mitgliedstaaten zu Datensammlungen wie nach dem Prüm-Beschluss, der RL über die Vorratsdatenspeicherung[124] oder der geplanten europäische FluggastdatenRL[125];
5. durch Abkommen der EU mit Drittstaaten wie jenes über Luftverkehrspassagierdaten[126] oder das sog SWIFT-Abkommen[127] zur Verfolgung von Terrorfinanzierung mit den USA.

Insgesamt besteht eine fast unüberblickbare Fülle von Regelungen aller Art. Hier kann nur ein Beispiel aus jeder Gruppe herausgegriffen werden.

## B. Beispiele

### 1. Europol[128]

Europol, mittlerweile keine internationale Organisation mehr sondern eine Agentur der EU, hat in Bereichen schwerer Kriminalität nach Art 88 AEUV den Auftrag, die Tätigkeit der nationalen Sicherheitsbehörden zu unterstützen, va durch das „Einholen, Speichern, Verarbeiten, Analysieren und Austauschen

123 Beschluss 2008/615/JI des Rates vom 23.6.2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insb zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, ABl L 2008/210, 1; Beschluss 2008/616/JI des Rates vom 23.6.2008 zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insb zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, ABl L 2008/210, 12.

124 RL 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 RL 2002/58/EG, ABl L 2006/105, 54.

125 Vorschlag für eine RL 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 endg. Zu früheren Vorschlägen *McGinley*, Die Verarbeitung von Fluggastdaten für Strafverfolgungszwecke – das geplante EU PNR System, DUD 2010, 250.

126 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, ABl L 2012/215, 5; davor Abkommen ABl L 2007/204, 16 und ABl L 2006/298, 29; Abkommen 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, ABl L 2012/186, 4; davor Abkommen ABl L 2008/213, 49.

127 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 2010/195, 5.

128 Zum Folgenden *Engel*, Befugnis, Kontrolle und Abwicklung von Europol unter Berücksichtigung des Vertrages über eine Verfassung von Europa (2006) 46 ff; *Günther*, Europol (2006) 46 ff; *Wolter/Schenke/Hilger/Ruthig/Zöller* (Hrsg), Alternativentwurf Europol und europäischer Datenschutz (2008); *de Moor/Vermeulen*, The Europol Council Decision: Transforming Europol into an Agency of the European Union, CMLRev 2010, 1089 (1099 ff); *Bochm* (FN 112) 177 ff.





von Informationen, die insbesondere von den Behörden der Mitgliedstaaten oder Drittländern beziehungsweise Stellen außerhalb der Union übermittelt werden". Dazu betreibt Europol mehrere Datenbanken. Im Mittelpunkt stehen das Informationssystem und die Arbeitsdateien.[129]

In das Informationssystem eingetragen werden unter anderem verurteilte Straftäter, Verdächtige, aber auch „Personen, in deren Fall [...] faktische Anhaltspunkte oder triftige Gründe dafür vorliegen, dass sie Straftaten begehen werden, für die Europol zuständig ist."[130] Die gespeicherten Daten umfassen auch zB „Sozialversicherungsnummern, Fahrerlaubnisse, Ausweispapiere und Passdaten" und „soweit erforderlich, andere zur Identitätsfeststellung geeignete Merkmale, [...] wie daktyloskopische Daten und [...] DNA-Profile".[131] Wann dies erforderlich ist, spezifiziert der Beschluss nicht. Insgesamt sind mehr als 30.000 Personen im System erfasst.

Die Daten können bis zu drei Jahre gespeichert werden, die Frist ist verlängerbar.[132] Sie sind für das Europol-Personal, für die nationalen Europol-Stellen und für die Verbindungsbeamten aller Mitgliedstaaten, von Interpol und von einer Reihe von Drittstaaten zugänglich,[133] darunter vom FBI, dem Secret Service und anderen Behörden der USA, aus Albanien, Kolumbien oder Kroatien.[134]

In die Arbeitsdateien zu Analysezwecken können außer Täter und Verdächtigen auch mögliche Zeugen, Opfer, Kontakt- und Begleitpersonen und Informanten aufgenommen werden.[135] Der Durchführungsbeschluss dazu ermöglicht die Speicherung von 69 verschiedenen Merkmalen (zB zur Finanzsituation, Stimmenprofile, Lebensstil und -gewohnheiten, Bewegungen, soziales Um-

129 Art 10 ff Europol-Beschluss (FN 99).

130 Art 12 Abs 1 lit b Europol-Beschluss (FN 99).

131 Art 12 Abs 2 lit f und g Europol-Beschluss (FN 99). Europol hat Verbindungsbeamte auch von zehn Drittstaaten und -organisationen, Europol Review 2011. General report on Europol activities (2012) 17: Albania, Australia, Canada, Colombia, Croatia, Iceland, Norway, Switzerland, Interpol and the following United States law enforcement agencies: Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Drug Enforcement Administration (DEA); Secret Service (USSS); Federal Bureau of Investigations (FBI); Immigration and Customs Enforcement (ICE); and Internal Revenue Service (IRS).

132 Art 20 Europol-Beschluss (FN 99).

133 Art 13 Europol-Beschluss (FN 99).

134 Europol Review 2011. General Report on Europol Activities (2012) 17: „Europol also hosts liaison officers from 10 non-EU countries and organisations who work together with Europol on the basis of cooperation agreements."; mit der Fußnote: „Albania, Australia, Canada, Colombia, Croatia, Iceland, Norway, Switzerland, Interpol and the following United States law enforcement agencies: Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Drug Enforcement Administration (DEA); Secret Service (USSS); Federal Bureau of Investigations (FBI); Immigration and Customs Enforcement (ICE); and Internal Revenue Service (IRS)." Zur zweifelhaften Verträglichkeit dieser Situation mit der Rechtsprechung des EGMR *Bochm* (FN 112) 194 f.

135 Art 14 Abs 1 Europol-Beschluss (FN 99).

feld).[136] Er unterscheidet dabei zwar grundsätzlich zwischen Tätern, Verdächtigen und Unschuldigen, erlaubt, soweit für die Bestimmung der jeweiligen Rolle des Beteiligten erforderlich, eine volle Speicherung auch bei diesen.[137] Die Verarbeitung der Daten umfasst dabei ausdrücklich auch" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe, der/die im Hinblick auf personenbezogene Daten ausgeführt werden, wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Abrufen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Abgleichung, sowie das Sperren, Löschen oder Vernichten".[138]

Zugang zu den Arbeitsdateien haben grundsätzlich nur die Mitglieder der jeweiligen Analysegruppe, die sich freilich wieder aus Europol-Bediensteten, Verbindungsbeamten verschiedener Mitgliedstaaten und Vertretern von OLAF und Eurojust und (nach Maßgabe von Arbeitsübereinkommen) auch aus externen Experten zusammensetzen kann.[139]

Europol kann Daten auch an andere EU-Stellen, Behörden von Drittstaaten und internationale Organisationen weitergeben.[140] Voraussetzung dafür ist regelmäßig ein Abkommen mit der jeweiligen Stelle und bei Nicht-EU-Einrichtungen grundsätzlich auch die förmliche Feststellung von Europol, dass der Empfänger ein angemessenes Datenschutzniveau gewährleistet. Abkommen dieser Art sind in einem Durchführungsrechtsakt für eine Vielzahl von Staaten und Organisationen vorgesehen, ua mit Bolivien, Bosnien, China, Serbien und der Ukraine.[141] Tatsächlich abgeschlossen wurden („operative") Abkommen, die auch den Transfer von personenbezogenen Daten umfassen, ua mit Eurojust, Interpol, den USA, der Schweiz oder Monaco,[142] aber auch ein nicht publiziertes Abkommen mit dem Joint Situation Centre[143], einer Art Geheimdienstabteilung im Auswärtigen Dienst des Rates. Die Durchführungsbestimmungen zur internationalen Zusammenarbeit sehen eine Zweckbindung der weitergegebenen Daten und eine Beschränkung der Weitergabe durch den Empfänger vor,[144] doch lässt sich das, wie sich zeigt, in den Abkommen nicht immer vollständig umsetzen.[145] Außerdem ist die Zweckbindung nicht immer dieselbe wie bei der ursprünglichen Datenspeicherung, und es sind auch Übermittlungen ohne Abkommen zulässig[146]. 2007 wurden ca 21.000 Informationen mit Dritten ausgetauscht.[147]

Die Verantwortlichkeit für die Datenverarbeitung in Europol ist geteilt: Für Daten, die von den Mitgliedstaaten eingegeben wurden, sind diese verantwortlich, für Daten, die Europol selbst aufgenommen hat oder die von Dritten stammen, sowie für die Übermittlung von Daten an Dritte muss Europol selbst einstehen.[148] Dabei hilft ein agentureigener Datenschutzbeauftragter.[149]

Betroffene haben grundsätzlich einen Anspruch auf Auskunft, Richtigstellung und Löschung ihrer Daten gegenüber Europol,[150] doch gelten für die Auskunft und damit faktisch auch für die anderen Rechte weitreichende Ausnahmen.[151] Eine amtswegige auch nur nachträgliche Verständigung von der Datenverarbeitung ist nicht vorgesehen. Kommt Europol einem Antrag nicht nach, befasst sich auf Wunsch der Betroffenen die Gemeinsame Kontrollinstanz mit dem Fall.[152] Die Kontrollinstanz, die sich aus Vertretern der nationalen Datenschutzbehörden zusammensetzt,[153] kann freilich eine Europol-Entscheidung nur bei Auskunftsverweigerung und auch da nur mit Zweidrittelmehrheit korrigieren.[154] Daneben kann die Übermittlung von Daten oder ihr Abruf durch die Behörden eines Mitgliedstaates vor dessen nationaler Kontrollinstanz angefochten werden.[155]

136 Art 6 Abs 2 Beschluss 2009/936/JI des Rates vom 30.11.2009 zur Annahme der Durchführungsbestimmungen für die von Europol geführten Arbeitsdateien zu Analysezwecken, ABl L 2009/325, 14.

137 Art 6 Abs 3 Beschluss (FN 136).

138 Art 1 lit e Beschluss (FN 136).

139 Art 14 Abs 2 Europol-Beschluss (FN 99).

140 Art 22 f Europol-Beschluss (FN 99); Beschluss 2009/934/JI des Rates vom 30.11.2009 zur Festlegung der Durchführungsbestimmungen zur Regelung der Beziehungen von Europol zu anderen Stellen einschließlich des Austauschs von personenbezogenen Daten und Verschlusssachen, ABl 2009 L 325/6.

141 Beschluss 2009/935/JI des Rates vom 30.11.2009 zur Festlegung der Liste der Drittstaaten und dritten Organisationen, mit denen Europol Abkommen schließt, ABl L 2009/325, 12.

142 Fundstellen unter https://www.europol.europa.eu/content/page/international-relations-31 und https://www.europol.europa.eu/content/page/eu-agencies-135 (Stand 10.12.2012).

143 *Boehm* (FN 112) 253 f; allgemein zum Informationsaustausch mit Geheimdienststellen *Davis Cross*, EU Intelligence Sharing & The Joint Situation Centre: A Glass Half-Full (2011) zugänglich unter http://euce.org/eusa/2011/papers/3a_cross.pdf (Stand 13.12.2012).

144 Art 10, Art 15 ff Beschluss 2009/934/JI (FN 140).

145 Vgl zB Art 5 Abs 1 des Zusatzabkommens zum Abkommen Europols mit den USA, zugänglich unter https://www.europol.europa.eu/sites/default/files/flags/supplemental_agreement_between_europol_and_the_usa_on_exchange_of_personal_data_and_related_information.pdf (Stand 10.12.2012).

146 Art 13 Beschluss 2009/934/JI (FN 140); Art 22 Abs 3 Europol-Beschluss (FN 99).

147 Erklärung von Europol gegenüber dem House of Lords, zitiert nach *Boehm* (FN 112) 207.

148 Art 29 Europol-Beschluss (FN 99).

149 Art 28 Europol-Beschluss (FN 99).

150 Art 30 Europol-Beschluss (FN 99).

151 Art 30 Abs 5 Europol-Beschluss (FN 99).

152 Art 32 Europol-Beschluss (FN 99).

153 Art 34 Europol-Beschluss (FN 99).

154 Art 32 Abs 4 Europol-Beschluss (FN 99).

155 Art 33 Europol-Beschluss (FN 99).

## 2. Schengen Informationssystem (SIS)[156]

Das Schengen Informationssystem ist das älteste der genannten Informationssysteme. Wie Europol entstammt es einer völkerrechtlichen Kooperation außerhalb des früheren Gemeinschaftsrechts und wurde erst nachher in dieses einbezogen. An ihm nehmen nicht alle Mitgliedstaaten, dafür aber, vermittelt über völkerrechtliche Abkommen,[157] auch Island, Norwegen, Liechtenstein und die Schweiz teil.

Das SIS ist ein Instrument zur Außengrenzkontrolle und zu anderen Zoll- und Polizeikontrollen einerseits und für die Vergabe von Visa und anderen Aufenthaltstiteln andererseits. Entsprechend stammen seine Rechtsgrundlagen aus der ehemaligen Dritten und der ehemaligen Ersten Säule. Derzeit läuft immer noch die Umstellung von SIS I[158] zu einem erweiterten SIS II[159], die sich aus verschiedenen Gründen als äußerst schwierig gestaltet und zu einer Vielzahl von Übergangsregelungen geführt hat.[160]

Das SIS II soll „als Ausgleichsmaßnahme zur Wahrung eines hohen Maßes an Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts der Europäischen Union beitragen, indem es die operative Zusammenarbeit zwischen Polizei- und Justizbehörden in Strafsachen unterstützt".[161] Damit ist seine Aufgabe recht weit umschrieben. Allerdings hängen die Eintragung ins System und die Verwendung der Daten vom spezifischen Zweck der jeweiligen Ausschreibung ab. Ausgeschrieben werden können Drittstaatsangehörige, denen die Einreise verweigert werden soll, und Personen jeglicher Staatsangehörigkeit, die entweder vermisst werden oder die mit einem Europäischen Haftbefehl, für eine Auslieferung oder für eine Teilnahme an einem Gerichtsverfahren gesucht werden oder die zur Verbrechensverhütung einer gezielten oder verdeckten Kontrolle unterworfen werden sollen.[162] Ausschreibungen lassen sich auch verknüpfen,[163] etwa nach dem Muster „Ehemann gesuchter Terrorist – Ehefrau

156 Zum Folgenden *Wehner*, Die polizeiliche Zusammenarbeit zwischen den Schengen-Staaten unter besonderer Berücksichtigung des SIS, in *Achermann/Bieber/Epiney/Wehner*, Schengen und die Folgen (1995) 129 (133 ff); *Breitenmoser/Glass/Lagodny* (Hrsg), Schengen in der Praxis (2009); *Fastenrath/Skerka*, Sicherheit im Schengen-Raum nach dem Wegfall der Grenzkontrollen – Mechanismen und rechtliche Probleme grenzüberschreitender polizeilicher und justizieller Zusammenarbeit, ZEuS 2009, 219; *v. Bogdandy*, Die Informationsbeziehungen im europäischen Verwaltungsverbund, in *Hofmann-Riem/Schmidt-Aßmann/Voßkuhle* (Hrsg), Grundlagen des Verwaltungsrechts II[2] (2012) § 25 Rz 80 ff; *Boehm* (FN 112) 260 ff, 314 f.

157 FN 107.

158 Titel IV Schengener Durchführungsübereinkommen, ABl L 2000/239, 19.

159 FN 117.

160 Va VO (EG) 1104/2008 des Rates und Beschluss 2008/839/JI des Rates vom 24.10.2008 über die Migration vom Schengener Informationssystem (SIS 1+) zum Schengener Informationssystem der zweiten Generation (SIS II), ABl L 2008/299, 1 und 43; Vorschlag für eine VO über die Migration vom Schengener Informationssystem (SIS 1+) zum Schengener Informationssystem der zweiten Generation (SIS II), KOM (2012) 81 endg.

161 ErwGr 5 SIS II-Beschluss bzw SIS II-Verordnung (FN 117).

162 Art 24 SIS II-Verordnung, Art 26, 32, 34, 36 SIS II-Beschluss (jeweils FN 117).

163 Art 37 SIS II-Verordnung, Art 42 SIS II-Beschluss (jeweils FN 117).





vermutliche Komplizin" oder „Einreiseverbot – Zeuge in Verfahren über illegale Einreise". Insgesamt hat es bereits mehr als 35 Millionen Eintragungen in das SIS gegeben.[164]

Das System sieht vor, dass beim Zugriff festgestellt werden kann, ob ein Treffer erzielt wurde, und dass dann gegebenenfalls ergänzende Information zum Gesuchten zur Verfügung steht; va handelt es sich dabei um Fotos, Fingerabdrücke und biometrische Daten zur Identitätsbestimmung oder zB um einen Europäischen Haftbefehl.[165] Zusätzliche vertiefte Information wird dann außerhalb der Datenbank über Rückfrage in den nationalen SIRENE-Büros auf der Grundlage eines Handbuchs der EU ausgetauscht.[166] Das Handbuch ist in Teilen geheim.

Zugriff zum SIS haben nationale Zoll- und Polizeibehörden sowie Justiz und Fremdenpolizei, außerdem auch Europol und Eurojust im Rahmen ihrer Aufgaben.[167] Insgesamt gibt es mehr als eine halbe Million Zugriffsterminals.[168] Die Daten dürfen nur für die jeweiligen Ausschreibungszwecke verwendet werden.[169] Eine Weitergabe an Dritte ist nicht erlaubt, allerdings gibt es eine Ausnahme in Bezug auf Pässe zugunsten von Interpol,[170] und ein indirekter Zugang für Dritte ergibt sich über Europol und Eurojust.

Die Datenverantwortlichkeit liegt grundsätzlich bei dem Mitgliedstaat, der die Eintragung vorgenommen hat. Dementsprechend unterliegt er auch der Überwachung durch eine unabhängige nationale Kontrollstelle,[171] während die zentralen Komponenten des SIS, deren Management – wie übrigens auch jenes von VIS und Eurodac – in Kürze einer eigens gegründeten IT-Großsystem-Agentur übertragen werden soll,[172] vom Europäischen Datenschutzbeauftragten überwacht werden.[173]

Bemerkenswert ist, dass Drittstaatsangehörige, die Gegenstand einer Ausschreibung im Zusammenhang mit dem Personenverkehr sind, von Amts wegen informiert werden, soweit nicht eine Ausnahme zutrifft.[174] Im Übrigen hat jeder Betroffene ein Recht auf Auskunft, Richtigstellung und Löschung seiner

164 Ratsdokument 9938/11.

165 Art 3 lit c, Art 22 SIS II-Verordnung bzw SIS II-Beschluss; Art 27 f SIS II-Beschluss (jeweils FN 117).

166 Art 2 Abs 1, Art 3 lit b, Art 8 SIS II-Verordnung bzw SIS II-Beschluss (jeweils FN 117); SIRENE Handbuch, ABl 2003 C 38/1.

167 Art 27 SIS II-Verordnung, Art 40-42 SIS II-Beschluss (jeweils FN 117).

168 Ratsdokument 13305/09, 3.

169 Art 31 SIS II-Verordnung, Art 46 SIS II-Beschluss (jeweils FN 117).

170 Art 39 SIS II-Verordnung, Art 54, 55 SIS II-Beschluss (jeweils FN 117).

171 Art 44 SIS II-Verordnung, Art 60 SIS II-Beschluss (jeweils FN 117).

172 Art 15 SIS II-Verordnung bzw SIS II-Beschluss (jeweils FN 117); VO (EU) 1077/2011 des Europäischen Parlaments und des Rates vom 25.10.2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, ABl L 2011/286, 1.

173 Art 45 SIS II-Verordnung, Art 61 SIS II-Beschluss (jeweils FN 117).

174 Art 42 SIS II-Verordnung (FN 117).

Daten, das er vor jeder nationalen Kontrollinstanz geltend machen kann.[175] Deren Entscheidung ist dann für alle Mitgliedstaaten verbindlich.[176]

### 3. Prüm-Beschluss[177]

Auch der Prüm-Beschluss[178] ist, wie schon sein Name sagt, der mittlerweile unionisierte Nachfolger eines völkerrechtlichen Vertrags einiger Mitgliedstaaten, nämlich des Vertrags von Prüm[179]. Er dient nach seinem Titel zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insb zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität.

Wesentlicher Inhalt und Besonderheit ist der wechselseitige automatisierte Zugriff der Behörden der Mitgliedstaaten auf DNA-Daten, Fingerabdrücke und Kraftfahrzeug-Zulassungsdaten nach dem Grundsatz der „Verfügbarkeit", soweit es um die Verfolgung und Verhinderung von Straftaten geht.[180]

Während Eigentümer-, Zulassungsbesitzer- und Fahrzeugdaten aus dem Kraftfahrzeugregister direkt eingesehen werden können, beschränkt sich der Zugang auf DNA und Fingerabdrücke allerdings auf anonyme „Treffer/kein Treffer"-Antworten. Im positiven Fall können dann von den jeweiligen Kontaktstellen ergänzend Daten im konventionellen Weg, also nach Prüfung einer individuellen Anfrage und nach Maßgabe des Rechts des ersuchten Staates, übermittelt werden.[181]

Ebenso, aber auch aus eigener Initiative, übermitteln die Mitgliedstaaten einander Daten über Personen, von denen angenommen wird, dass sie terroristische Straftaten begehen oder bei Großveranstaltungen, zB Fußball-Europameisterschaften oder Tagungen des Europäischen Rates, die öffentliche Sicherheit und Ordnung stören werden.[182]

Voraussetzung für den Datenaustausch nach dem Beschluss ist die Gewährleistung eines angemessenen Datenschutzniveaus, das bei jenen Staaten,

[175] Art 41, 43 SIS II-Verordnung, Art 58 SIS II-Beschluss (jeweils FN 117). Diese *„transnationale Prozessstandschaft"* verdient nach *J.-P. Schneider*, Informationssysteme als Bausteine des Europäischen Verwaltungsverbunds, NVwZ 2012, 65 (66) als innovatives Rechtsinstitut *„die besondere Aufmerksamkeit der Europäischen Verwaltungsrechtswissenschaft"*. Diese Aufmerksamkeit könnte sich auch auf die Praxis der Rechtsanwendung richten; dazu unten nach FN 220.

[176] Art 43 Abs 2 SIS II-Verordnung; Art 59 Abs 2 SIS II-Beschluss (jeweils FN 117).

[177] Zum Folgenden besonders instruktiv: *Kunnert*, Datenschutzfragen der EU-weiten Polizeikooperation am Beispiel des „Prümer Vertrags" („Schengen III") und seiner Weiterentwicklung (iE); weiters *Schaar*, Datenaustausch und Datenschutz im Vertrag von Prüm, DuD 2006, 691; *Niemeier/Zerbst*, Der Vertrag von Prüm – vertiefte grenzüberschreitende Zusammenarbeit zur Kriminalitätsbekämpfung in der EU, ERA Forum 2007, 535; *Papayannis*, Die polizeiliche Zusammenarbeit und der Vertrag von Prüm, ZEuS 2008, 219; *Mutschler*, Der Prümer Vertrag (2010); *B. Raschauer*, Prümer Vertrag und Informationsaustausch in der EU, in *BMI* (Hrsg), Rechtsschutz und EU-Reform (2010) 95.

[178] FN 123.

[179] BGBl III 2008/159.

[180] ErwGr 4, Art 3, 9, 12 Prüm-Beschluss (FN 123).

[181] ErwGr 10, 18, Art 5, 10 Prüm-Beschluss (FN 123).

[182] Art 14, 16 Prüm-Beschluss (FN 123).





die nicht schon Vertragspartner von Prüm waren, durch einstimmigen Ratsbeschluss festgestellt werden muss.[183] Die Verwendung der DNA- und Fingerabdruck-Daten ist streng zweckgebunden, bei anderen Daten kann der Verwendungszweck im Einvernehmen erweitert werden, wenn der neue Zweck nach dem Recht der beiden Staaten zulässig ist.[184] Eine Weitergabe an andere Einheiten ist nach vorheriger Zustimmung des übermittelnden Mitgliedstaats und nach Maßgabe des innerstaatlichen Rechts des empfangenden Mitgliedstaats möglich.[185] Übermittelte Daten sind nach Zweckerfüllung oder der vom Übermittlungsstaat mitgeteilten Höchstspeicherdauer zu löschen.[186]

Die Einhaltung der Vorschriften wird durch die nationalen Datenschutzorgane überprüft. Betroffene haben Anspruch auf Auskunft, Richtigstellung und Löschung ihrer Daten sowie auf effektiven Schutz dieser Rechte nach nationalem Recht.[187]

### 4. Vorratsdatenspeicherung

Zur Vorratsdatenspeicherung als Beispiel für eine Verpflichtung der Mitgliedstaaten zu Datensammlungen durch die EU ist das Wesentliche sicher bekannt.[188] Daher hier nur zwei Bemerkungen:

- Vor dem Hintergrund unserer Handy- und Internetnutzungsgewohnheiten ermöglicht die Auswertung der Vorratsdaten die automatische Erstellung eines zumindest sechsmonatigen kompletten Bewegungsprofils und eine Abbildung der Lebensgewohnheiten und der sozialen Beziehungen von einzelnen Bürgern, aber auch von ganzen Gruppen; das ist eben automatisch und in einer Intensität und Genauigkeit möglich, die die Betroffenen selbst nie erreichen könnten. So etwas hat es noch nie gegeben, auch nicht in Regimen, die keinen Überwachungsaufwand gescheut haben.
- Im Rahmen der Sicherheitsverwaltung ist die Verpflichtung zur Vorratsdatenspeicherung nur ein Exkurs, da sie ja, wie der EuGH bestätigt hat,[189] in erster Linie zum besseren Funktionieren des Binnenmarktes geschaffen wurde.[190]

[183] Art 25 Prüm-Beschluss (FN 123).

[184] Art 26 Prüm-Beschluss (FN 123).

[185] Art 27 Prüm-Beschluss (FN 123).

[186] Art 28 Abs 3 Prüm-Beschluss (FN 123).

[187] Art 31 Prüm-Beschluss (FN 123).

[188] FN 124; dazu *Berka*, Gutachten (FN 92) 119 f, 138 ff; außerdem zB *Simitis*, Der EuGH und die Vorratsdatenspeicherung oder die verfehlte Kehrtwende bei der Kompetenzverteilung, NJW 2009, 1782; *Kolb*, Vorratsdatenspeicherung (2011); *Boehm* (FN 112) 370; *Schmaus*, Die Vorratsdatenspeicherungsrichtlinie der Europäischen Union (2012).

[189] EuGH, C-301/06, *Irland gegen Europäisches Parlament und Rat der Europäischen Union*, Slg 2009 I-593, Rz 72, 85.

[190] Rechtsgrundlage und ErwGr 6 der RL (FN 124).

### 5. Passagierdatenabkommen mit den USA[191]

Die über Europa hinausreichende internationale Dimension soll hier nur am Beispiel des Passagierdatenabkommens der EU mit den USA angedeutet werden.

Das Abkommen erlaubt (und gebietet) den europäischen Fluggesellschaften, dem Department of Homeland Security der USA, wie vom amerikanischen Recht vorgesehen, Buchungsdaten ihrer Passagiere zu übermitteln.[192] Dazu gehören neben Namen und Flugnummer auch zB Kontakt- und Zahlungsinformationen (also etwa die verwendete Kreditkarte) und uU Wünsche zum Essen (aus denen zB auf die Religionszugehörigkeit geschlossen werden kann).[193]

Die Daten dürfen von den USA zur Verhütung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von terroristischen Straftaten und von grenzüberschreitenden Taten, die mit mindestens drei Jahren Freiheitsstrafe bedroht sind, verwendet werden. Die Verwendung schließt die analytische Auswertung und Verknüpfung der Daten ein. Erlaubt ist auch die Auswertung, um jene Personen zu bestimmen, die bei der Einreise besonders kontrolliert werden sollen.[194]

Die Informationen dürfen, soweit es sich nicht um sensible Daten handelt, bis zu 15 Jahre gespeichert werden; danach werden sie nicht gelöscht, sondern nur unwiderruflich anonymisiert.[195]

Das Department of Homeland Security darf die Daten an andere amerikanische Behörden unter Wahrung der Zweckbindung weitergeben.[196] Alle amerikanischen Behörden dürfen die Daten wiederum an Drittländer weitergeben; Voraussetzung dafür ist ein Abkommen mit dem Drittstaat, das Datenschutzgarantien wie das Abkommen EU-USA enthält, oder zumindest ein Notfall.[197] Direkt aufgrund dieses Abkommens dürfen Passagierdaten und die Ergebnisse ihrer Auswertung an Polizei- und Justizbehörden der EU-Mitgliedstaaten sowie an Europol und Eurojust weitergegeben werden,[198] was vielleicht auch ein gewisses Interesse des Rates der EU am Abschluss erklärt.

Das Abkommen sieht Rechte auf Auskunft über die gespeicherten Daten und auf ihre Berichtigung und Löschung vor, verweist dafür jedoch auf verschiedene amerikanische Vorschriften.[199] Diese scheinen eine gerichtliche Kontrolle regelmäßig nicht zu ermöglichen. Aufschlussreich ist in diesem Zusammenhang Art 21 Abs 1 des Abkommens. Die Bestimmung lautet: „Durch dieses Abkommen werden nach US-amerikanischem Recht keinerlei Rechte oder Vergünstigungen für Personen privater oder öffentlicher Art begründet oder auf diese übertragen."

Diese Datenschutzvorkehrungen gelten gemäß Art 19 des Abkommens ausdrücklich als angemessen im Sinne der einschlägigen Datenschutzvorschriften der EU.

### C. Verknüpfung der Elemente

Für die Bewertung ist zweierlei wichtig: Zum einen sind das sind nur Beispiele; es gibt noch viel mehr. Zum anderen können die Beispiele nicht isoliert gesehen werden, nicht nur weil ihre Bedeutung sich erst im Gesamtkontext erschließt, sondern auch deshalb, weil sie über Kooperationsmechanismen untereinander rechtlich zusammenhängen.[200] Informationen, die über den Prüm-Mechanismus oder aus Vorratsdaten gewonnen wurden, können zu Ausschreibungen und Informationsübermittlungen im SIS führen, zu dem wiederum Europol Zugang hat, das Daten an die Amerikaner weitergeben kann, die sie wiederum mit Fluggastdaten verknüpfen dürfen und die Ergebnisse den europäischen Sicherheitsbehörden übermitteln dürfen. (Auch das ist nur ein Beispiel.)

## III. Datenschutzrechtliche Bewertung

### A. Maßstab

Versucht man diese Situation zu bewerten, braucht man zunächst einen Maßstab.[201] Diesen bildet das Grundrecht auf Datenschutz, das in Art 8 Europä-

191 FN 126. Zum Folgenden: *Simitis*, Übermittlung der Daten von Flugpassagieren in die USA: Dispens vom Datenschutz? NJW 2006, 2011; *Sorger*, Übermittlung von Fluggastdaten an die USA, in *Jahnel* (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2008 (2008) 191; *Papakonstantinou/de Hert*, The PNR Agreement and Transatlantic Anti-Terrorism Co-operation: No Firm Human Rights Framework on Either Side of the Atlantic, CMLRev 2009, 885; *Hanschmann*, Das Verschwinden des Grundrechts auf Datenschutz gegen hoheitliche Maßnahmen in der Pluralität von Rechtsregimen, EuGRZ 2011, 219; in *Matz-Lück/Hong* (Hrsg), Grundrechte und Grundfreiheiten – Konkurrenzen und Interferenzen (2012) 293; *Hornung/Boehm*, Comparative Study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security (2012) zugänglich unter https://gruen-digital.de/wp-content/uploads/2012/03/PNR-EU-USA-Study-120313.pdf (Stand 13.12.2012). Zum Vorschlag eines allgemeinen Datenaustauschabkommens zwischen EU und USA *De Busser*, The Adaquacy of an EU-US Partnership, in: *Gutwirth/Leenes/De Hert/Poullet* (Hrsg), European Data Protection: In Good Health? (2012) 185; zum Datenschutz in den USA *Slobogin*, Die Zukunft des Datenschutzes in den USA, Die Verwaltung 2011, 465.

192 Art 3, 15 Abkommen (FN 126).

193 Anhang des Abkommens (FN 126).

194 Art 4 Abkommen (FN 126).

195 Art 8 Abkommen (FN 126).

196 Art 16 Abkommen (FN 126).

197 Art 17 Abkommen (FN 126).

198 Art 18 Abkommen (FN 126).

199 Art 11–13 Abkommen (FN 126).

200 Ausführlich zu den Verknüpfungen zwischen einschlägigen Agenturen und Informationssystemen *Boehm* (FN 112) 321 ff; aktualisierte Kurzfassung in *Boehm*, Information Sharing in the Area of Freedom, Security and Justice – Towards a Common Standard for Data Exchange between Agencies and EU Information Systems, in *Gutwirth/Leenes/De Hert/Poullet* (Hrsg), European Data Protection: In Good Health? (2012) 143; weiters *Demmelbauer*, Europol, Eurojust und das Europäische Justizielle Netz (2012).

201 Dazu *Berka*, Gutachten (FN 92) 68 ff; weiters (abgesehen von den Kommentaren zu GRC und EMRK) *Siemen*, Datenschutz als europäisches Grundrecht (2005);

ischen Grundrechtecharta (GRC) gewährleistet (und in Art 16 AEUV wiederholt) wird. Es ist im Zusammenhang mit Art 7 GRC zum Schutz des Privatlebens, zu dem es lex specialis ist, und im Lichte jener Rechtsquellen auszulegen, auf denen es nach den Erläuterungen zur GRC aufbaut: Art 8 EMRK, das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1981 und die DatenschutzRL der EG. Wichtig ist auch der Zusammenhang mit dem Recht auf effektiven Rechtsschutz nach Art 47 GRC.

Inhaltlich ergeben sich daraus folgende Grundsätze: Die Verarbeitung von Daten vom Erheben bis zum Weitergeben bedarf, sofern es keine freiwillige Einwilligung gibt, einer ausreichend klaren und bestimmten gesetzlichen Grundlage, die Eingriffe vorhersehbar macht. Für die Legitimität und Verhältnismäßigkeit einer entsprechenden Regelung ist zunächst eine bewusste Abwägungsentscheidung des Gesetzgebers Voraussetzung. Dann geht es um die Erforderlichkeit der Erhebung der jeweiligen Daten – Stichwort Datensparsamkeit – und schließlich ist va eine Zweckbindung der Daten entscheidend, die sich in konkreten Beschränkungen ihrer Verwendung, des Zugriffs auf sie und der Dauer ihrer Speicherung niederschlagen muss. Wichtig im Hinblick auf die Angemessenheit ist auch die getrennte Behandlung normaler und sensibler Daten. Den einzelnen Betroffenen sind Möglichkeiten der Information, Richtigstellung und Löschung ihrer Daten einzuräumen; diese Rechte müssen auch effektiv durchsetzbar sein. Außerdem müssen Vorkehrungen gegen Missbrauch getroffen werden; ua ist die Einhaltung der Datenschutzvorschriften von einer unabhängigen Stelle zu überwachen.

## B. Anwendung

Misst man den europäischen Datenaustausch im Sicherheitsbereich an diesen Grundsätzen, ergibt sich folgendes Bild:

*Eeckl*, Die Zulässigkeit von Informationseingriffen in der Rechtsprechung des EGMR, in FS Machacek/Matscher (2008) 95; *Esser*, Europäischer Datenschutz – Allgemeiner Teil – Mindeststandards der Europäischen Menschenrechtskonvention, in *Wolter/Schenke/Hilger/Ruthig/Zöller* (FN 128) 281; *Britz*, Europäisierung des grundrechtlichen Datenschutzes? EuGRZ 2009, 1; *De Hert/Gutwirth*, Data Protection in the Case Law of Strasbourg and Luxemburg – Constitutionalisation in Action, in *Gutwirth/Poullet/De Hert/de Terwangne/Nouwt* (Hrsg), Reinventing Data Protection? (2009) 3; *Bodenschatz*, Der europäische Datenschutzstandard (2010); *Guild*, The Lisbon Treaty, The Stockholm Programme and Data Transfer in the New ASFJ: Where are the Limits? in *Wolff/Goudappel/de Zwaan* (FN 91) 195; *N. Raschauer*, Europäisches Datenschutzrecht – quo vadis? in *N. Raschauer* (Hrsg), Datenschutzrecht 2010 (2011) 89 (91 ff); *Spiecker*, Kommt das „Volkszählungsurteil" nun durch den EuGH? – Der Europäische Datenschutz nach Inkrafttreten des Vertrages von Lissabon, JZ 2011, 169; *Boehm* (FN 112) 19 ff; *Albers*, Umgang mit personenbezogenen Informationen und Daten, in *Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle* (FN 156) § 22 Rz 39 ff; *Balthasar*, Was heißt „völlige Unabhängigkeit" bei einer staatlichen Verwaltungsbehörde? ZÖR 2012, 5.





## 1. Rechtsgrundlage

Eine klare Rechtslage gibt es zu verschiedenen Einzelfragen, aber sicher nicht insgesamt. Vielmehr haben wir es mit einem fast undurchschaubaren Flickwerk von vielfach vagen und nicht auf einander abgestimmten Teilregelungen zu tun. Die DatenschutzRL der EG gilt nur für sicherheitsrelevante Aktivitäten der ehemaligen Ersten Säule wie den personenverkehrsbezogenen Teil des SIS oder die Vorratsdatenspeicherung, nicht aber für die polizeiliche und justizielle Zusammenarbeit für Strafsachen.[202] Für sie gab es lange Zeit überhaupt keine allgemeinen datenschutzrechtlichen Regelungen, für einzelne Bereiche, etwa Frontex, auch keine spezifischen. Dann wurde dafür der Datenschutz-Rahmenbeschluss erlassen, doch gilt dieser wiederum nicht in Bereichen, in denen bereits ein „vollständiges, in sich geschlossenes Regelwerk [besteht], das alle relevanten Datenschutzaspekte erfasst und ausführlicher regelt"[203] – also ua nicht für Europol, den polizeiliche Teil von SIS und den Prüm-Beschluss. In anderen Bereichen soll der Rahmenbeschluss auch nicht einfach so, sondern erst nach Maßgabe eines Günstigkeitsvergleichs mit den dort anwendbaren Regeln gelten.[204] Der Bericht der Kommission über die Umsetzung des Rahmenbeschlusses weist aus, dass von den betroffenen 26 Mitgliedstaaten nur 14 auch nur behaupten, den Beschluss ganz umgesetzt zu haben.[205] Soweit dies der Fall war, unterscheiden sich die Umsetzungsvorschriften erheblich. Die europäischen Sonderregelungen für Einzelbereiche sind aus grundrechtlicher Sicht meist etwas besser als der Rahmenbeschluss, aber untereinander in Konzept und Terminologie keineswegs einheitlich und verteilen sich jeweils auf eine Reihe von Sekundär-, Tertiär- und Quartärakte.[206] Typisch ist auch eine vage Integration völkerrechtlicher Standards, etwa mit der Formulierung: „Unbeschadet der spezifischen Bestimmungen dieses Beschlusses trägt Europol den Grundsätzen des Übereinkommens des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und der Empfehlung R (87) 15 des Ministerkomitees des Europarates vom 17. September 1987 Rechnung."[207] Auf die Besonderheiten, die für das Vereinigte Königreich, Irland, Dänemark, Norwegen, Island, die Schweiz und Liechtenstein gelten, kann hier nur verwiesen werden.

[202] Art 3 Abs 2 RL 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31.

[203] ErwGr 39 Rahmenbeschluss 2008/977/JI des Rates vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl L 2008/350, 60.

[204] ErwGr 40 Datenschutz-Rahmenbeschluss (FN 203).

[205] Bericht der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen auf der Grundlage von Art 29 Abs 2 des Rahmenbeschlusses des Rates vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, KOM (2012) 12 endg 3.

[206] A „legal patchwork"; *Boehm* (FN 112) 373.

[207] Art 27 Europol-Beschluss (FN 99). Ähnlich ErwGr 20, Art 57 SIS II-Beschluss (FN 27), ErwGr 19, 20 und Art 25 Prüm-Beschluss (FN 33).

## 2. Verhältnismäßigkeitsprüfung

In praktisch allen einschlägigen Rechtsakten findet sich eine Bezugnahme auf den Datenschutz und die einschlägigen Grundrechte, und es handelt sich dabei um mehr als eine bloß rituelle Beschwörung und den bloß formalen Nachweis einer Verhältnismäßigkeitsprüfung. Trotzdem gibt es auch hier gravierende Defizite, va im Hinblick auf eine ausreichende politische Diskussion in der Öffentlichkeit. Das hängt zunächst damit zusammen, dass praktisch alle Akte noch im Rahmen der Dritten Säule, das heißt ohne das Europäische Parlament erlassen wurden; einige von ihnen[208] übrigens am letzten Tag vor Inkrafttreten des Vertrags von Lissabon, der zur Mitentscheidung mit dem Europäischen Parlament verpflichtet. Dazu kommt, dass zur Begründung in der Öffentlichkeit oft Teilaspekte wie die Terrorismusbekämpfung, der Kampf gegen Kinderpornografie oder die Wünsche der USA in den Vordergrund gestellt werden, während über andere, oft gleichwertige Motive nicht geredet wird; hier entsteht auch manchmal der Eindruck der Unlauterkeit. Eine ordentliche Verhältnismäßigkeitsprüfung ist auch deshalb schwierig, weil die Entscheidung über die Datenermittlung von der Entscheidung über die Datenverwendung und -weitergabe oft zeitlich und/oder kompetenziell getrennt ist. ZB entscheiden die Mitgliedstaaten zunächst einzeln über die Einrichtung verschiedener Datenbanken und später gemeinsam in der EU über ihre grenzüberschreitende Verwendung nach dem Verfügbarkeitsgrundsatz, oder es entscheidet die EU zunächst über die Vorratsdatenspeicherung als solche und die Mitgliedstaaten dann einzeln über die konkrete Nutzung und Weitergabe der gespeicherten Informationen. Zum Zeitpunkt der Entscheidung über ihre Ermittlung ist ihre Verwendung daher nicht absehbar. Zum Zeitpunkt der Entscheidung über die Verwendung sind die Daten aber schon vorhanden, und nun wäre schwer einzusehen, warum man sie nicht zu neuen Sicherheitszwecken nutzen sollte. Eine umfassende Erörterung unter Berücksichtigung der Kombinationswirkungen unterbleibt daher.[209] Schließlich ist, wie uns das Gutachten von Berka gezeigt hat, eine Erörterung der Verhältnismäßigkeit wegen der Risikostruktur im Sicherheitsbereich zwar besonders schwierig;[210] aber die Informationsprobleme, die sich aus fehlenden Berichten über den Vollzug und bloßen Pseudoevaluierungen wie zur Vorratsdatenspeicherung ergeben, sind vermeidbar.

## 3. Datensparsamkeit

Datensparsamkeit ist – so viel sollte aus den wenigen Beispielen deutlich geworden sein – nicht die Haupttugend der europäischen Sicherheitsverwaltung. Die Menge der Daten und der erfassten Personen und des Informationsaustausches ist in den letzten Jahren rasant gestiegen. Bedenklich ist va die Speicherung von Daten ohne oder nur aus minimalem Anlass – zB die Telekom-Vorratsdaten[211] oder Fluggast- oder Zahlungstransferinformationen[212], die Aufnahme von Personen in das Europol-System, von denen nur vermutet wird, sie könnten Verbrechen begehen[213]. Hier besteht im Übrigen auch die Gefahr der Diskriminierung aus besonders verpönten Gründen wie Rasse, Herkunft, Religion oder Weltanschauung. Ähnlich problematisch ist die Speicherung der Daten von bloßen Verbrechensopfern, Zeugen oder Begleitpersonen, ohne dass dabei ausreichend unterschieden wird.[214] Die Senkung der Schwelle für die Aufnahme in die Systeme verschärft ihre generelle Asymmetrie, nämlich die Tatsache, dass man leicht hinein, aber schwer wieder heraus kommt.

## 4. Zweckbindung

Ein großes Problem der europäischen Sicherheitsverwaltung bildet die Zweckbindung der Daten. Sie ist grundrechtlich fundamental, aber wegen der nachträglichen Hinzufügung neuer Zwecke oft nicht verlässlich, und va wird sie in der Zusammenarbeit der Mitgliedstaaten untereinander, der Mitgliedstaaten mit den Agenturen und anderen Stellen der EU, der Agenturen untereinander oder in gemeinsamen Ermittlungsteams und im Verkehr mit Drittstaaten immer schwächer. Analysiert man die Rechtsvorschriften, führt die Weitergabe von Daten regelmäßig zu Zweckerweiterungen; mehrfache Weitergaben zu weiteren Zweckerweiterungen. Besonders auffällig ist das dann, wenn zunächst nicht aus Sicherheitsgründen aufbaute Datenbanken wie Eurodac oder der personenverkehrsbezogene Teil des SIS für Eurojust und Europol „im Rahmen ihrer" – stetig wachsenden – „Aufgaben" geöffnet[215] oder wenn ursprünglich enger zweckgebundene Daten an Drittstaaten unter sehr vagen Zweckbindungen weitergegeben werden[216] – womit im Übrigen auch die Regeln über die Höchstspeicherdauer unterlaufen werden. Eine übergreifende Zweckbindung dürfte auch daran scheitern, dass dies eine entsprechende Markierung der Daten voraussetzt, was zT, aber wohl nicht durchgängig gewährleistet ist.

208 So die Europol-Durchführungsbeschlüsse (FN 136, 140, 141).

209 Ausführlicher und mit Beispielen *Weinzierl*, Europäische Parallelentwicklungen als Gegenstand menschenrechtsorientierte Evaluierung, in *Albers/Weinzierl* (Hrsg), Menschenrechtliche Standards in der Sicherheitspolitik (2010) 147.

210 *Berka* (FN 92) 102 ff.

211 FN 124.

212 FN 126, 127.

213 FN 130.

214 FN 135.

215 Art 21 Europol-Beschluss (FN 99); Art 41 SIS II-Beschluss (FN 117); Geänderter Vorschlag VO des Europäischen Parlaments und des Rates über die Einrichtung von „EURODAC" für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der VO (EU) [.../...] (zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist) und für der Strafverfolgung dienende Anträge der Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit EURODAC-Daten sowie zur Änderung der VO (EU) 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, KOM (2012) 254.

216 Bei FN 194.

### 5. Rechtsschutz

Schließlich ist der Rechtsschutz unzureichend; oft sogar nur eine Illusion. Das liegt zunächst daran, dass Eingriffe in das Recht auf Datenschutz von den Betroffenen regelmäßig nicht wahrgenommen werden können, eine amtswegige Information aber auch post festum nur in ganz seltenen Ausnahmesituationen vorgesehen ist[217] und Auskünfte nach großzügigen Regeln verweigert werden dürfen.[218] Es liegt auch an der Organisation des Rechtsschutzes, der in vielen Fällen die intergouvernementalen Eierschalen nicht abgestreift hat und die gerichtliche Ebene gar nicht erreicht.[219] Und es liegt auch immer noch an einem mangelnden Willen zur Zusammenarbeit. Statt langer Statistiken eine kurze Geschichte:[220]

Die französische Grenzpolizei verweigerte im Jahr 2000 einem israelischen Staatsbürger die Einreise. Der Betroffene klagte dagegen und erhielt 2001 vor dem zuständigen Verwaltungsgericht recht. 2003 wurde ihm allerdings ein Visum von der österr Botschaft verweigert – unter Berufung auf eine Ausschreibung zur Einreiseverweigerung im SIS, die das französische Innenministerium aufgrund des grenzpolizeilichen Zwischenfalls im Jahr 2000 verfügt hatte. Die Einzelheiten der Ausschreibung erfuhr der Betroffene im dritten Versuch ein Jahr nach der Visumsverweigerung durch eine Auskunft des österr Innenministeriums. Unter Hinweis auf die Entscheidung des französischen Verwaltungsgerichts beantragte er nun die Löschung der Ausschreibung in Frankreich. Da der Antrag ohne Reaktion blieb, klagte er schließlich auf Löschung bei der österr Datenschutzkommission. Diese machte im Sinne effektiven Rechtschutzes alles richtig: Sie bejahte zunächst ihre Zuständigkeit auf der Grundlage des SDÜ, gab dann dem französischen Innenministerium (erfolglos) Gelegenheit zur Stellungnahme, fand den Löschungsanspruch nach den einschlägigen Bestimmungen des SDÜ und des französischen Rechts begründet, leitet aus dem SDÜ ihre Befugnis ab, ausnahmsweise einen Leistungsausspruch zu treffen, und verpflichtete Frankreich Mitte 2005 zur Löschung der Ausschreibung binnen drei Wochen. Die Ausschreibung wurde freilich nicht gelöscht. Stattdessen beschäftigte sich die Gemeinsame Kontrollinstanz des Schengen-Systems mit dem Fall. Frankreich brachte dort vor, das Urteil des

[217] FN 174.

[218] ZB Art 30 Abs 5 Europol-Beschluss (FN 99).

[219] ZB Art 32 Europol-Beschluss (FN 99).

[220] Der folgende Fall wird geschildert von *König*, Die datenschutzrechtliche Umsetzung und Praxis von Schengen in Österreich, in *Breitenmoser/Gless/Lagodny* (FN 156) 171 (180 ff); die referierte Entscheidung der Datenschutzkommission vom 7.6.2005, K121.001/0009-DSK/2005, ist unter www.ris.bka.gv.at/Dsk/ zugänglich. Vergleichbare, für die Effizienz des Rechtsschutzsystems auch nicht gerade schmeichelhafte Fälle präsentiert *Brouwer*, The Other Side of Moon. The Schengen Information System and Human Rights: A Task for National Courts (2008) auch zugänglich unter www.ceps.eu/book/other-side-moons-schengen-information-system-and-human-rights-task-national-courts (Stand 13.12.2012) 5 ff. Zu den strukturellen Problemen, die hinter diesen Rechtsschutzdefiziten stehen, *Merli*, Rechtsschutz in grenzüberschreitenden verwaltungsrechtlichen Kooperationsverfahren, in *Holoubek/Lang* (Hrsg), Verfahren der Zusammenarbeit von Verwaltungsbehörden in Europa (2012) 377 (386 ff).





Verwaltungsgerichts aus 2001 sei noch nicht rechtskräftig. Die Gemeinsame Kontrollinstanz löste den konkreten Fall nicht, nahm ihn aber zum Anlass für eine Umfrage über die Praxis der Anwendung des Art 111 SDÜ und machte dann einen Interpretationsvorschlag für das Nebeneinander von Verfahren in mehreren Mitgliedstaaten. 2009, also nach neun Jahren, war die Ausschreibung noch aufrecht. Was seither geschah, ist öffentlich nicht bekannt.

## D. Ergebnis

Zusammenfassend muss man also sagen, dass die europäische Sicherheitspolitik und -verwaltung einiges erreicht hat, im Datenschutzbereich aber noch viele und schwerwiegende Mängel aufweist. Das ist nun nicht nur die einhellige Meinung aller einschlägigen Untersuchungen, sondern auch den Organen der EU selbst bewusst. Es soll sich daher etwas ändern.

# IV. Ausblick

## A. Vertrag von Lissabon

Zunächst ist zu berücksichtigen, dass der Vertrag von Lissabon hier schon einige Verbesserungen gebracht hat: Durch die Auflösung der Säulenstruktur und die supranationale Wiedervereinigung des Raums der Freiheit, der Sicherheit und des Rechts werden die wesentlichen Rechtsakte auch vom Europäischen Parlament beschlossen und vom EuGH kontrolliert.[221] Auch wenn noch Übergangsregelungen und Ausnahmevorschriften bestehen bleiben, hebt das doch die demokratische Legitimation und die rechtsstaatliche Qualität des einschlägigen Rechts.

## B. Vorschlag der DatenschutzRL im Bereich Polizei und Strafjustiz

Im Mittelpunkt wird aber die Neuordnung des Datenschutzes stehen, wie sie die Kommission in ihrem Reformpaket 2012[222] vorgeschlagen hat. Für die

[221] ZB *Suhr*, Die polizeiliche und justizielle Zusammenarbeit in Strafsachen, in *Fastenrath/Nowak* (Hrsg), Der Lissabonner Reformvertrag (2009) 299; *Hijmans/Scirocco*, Shortcomings in the Data Protection in the Third and Second Pillars. Can the Lisbon Treaty be Expected to Help? CMLRev 2009, 1485; *de Zwaan*, The new governance of justice and home affairs. Towards further supranationalism, in *Wolff/Goudappel/de Zwaan* (FN 91) 7.

[222] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Der Schutz der Privatsphäre in einer vernetzten Welt. Ein europäischer Datenschutzrahmen für das 21. Jahrhundert", KOM (2012) 9 endg; Vorschlag für RL des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM (2012) 10 endg; Vorschlag für VO des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM (2012) 11 endg. Dazu *Souhrada-*

polizeiliche und justizielle Zusammenarbeit in Strafsachen ist eine RL vorgesehen, die für die innerstaatliche Datenverarbeitung ebenso gelten soll wie für den Austausch zwischen Mitgliedstaaten und mit Dritten.[223] Der Entwurf enthält eine ganze Reihe von Verbesserungen, zB die Unterscheidung verschiedener Kategorien betroffener Personen und von Daten aufgrund von Fakten oder bloßer Vermutungen,[224] eine Stärkung der Aufsicht[225] und eine Verbesserung der Rechte der Betroffenen von der Vertretung ihrer Anliegen auch durch Verbände[226] bis hin zum Recht auf einen gerichtlichen Rechtsbehelf gegen Entscheidungen der Aufsichtsbehörde[227]. Er enthält natürlich auch Schwachpunkte, so zB die ganz weiche Beschränkung bei der Datenübermittlung an Drittländer.[228] Sein größter Mangel ist aber, dass er entgegen den Absichten seiner Verfasser[229] eben nicht zu einer umfassenden und kohärenten Regelung führt.[230] Abgesehen davon, dass er den Mitgliedstaaten in manchen Bereichen weite Spielräume lässt, die unterschiedlich genutzt werden können,[231] ist er eben nur ein – schwächerer – Sonderstandard für die polizeiliche und justizielle Zusammenarbeit und nicht Teil des allgemeinen Standards, der mit Verordnung erneuert werden soll; hier wirkt die Säulenteilung immer noch nach. Dazu kommt, dass er die davor erlassenen einschlägigen Datenschutzbestimmungen nicht ersetzen soll.[232] Die Sonderregelungen für zB Europol, das SIS oder Prüm sollen also bleiben und allenfalls später nach und nach angepasst werden. Freilich ist abzuwarten, welche Veränderungen die RL in dem nun begonnen Diskussionsprozess bis zu ihrer Erlassung noch erfahren wird.

In einem Punkt wirkt der Vorschlag freilich ganz besonders vereinheitlichend: Weil er auch die rein innerstaatlichen Datenverarbeitungen erfasst und auch diese daher in „Durchführung des Rechts der Union" erfolgen, unterliegen auch sie vollständig dem europäischen Grundrecht auf Datenschutz. Für ein österr Grundrecht auf Datenschutz lässt der Entwurf nur mehr einen marginalen

*Kirchmayer*, Das Gesamtkonzept für den Datenschutz in der Europäischen Union, in *Jahnel* (Hrsg), Datenschutzrecht. Jahrbuch 2010 (2011) 33; *Kotschy*, Daten schützen und nützen: Datenschutzrechtliche Weichenstellungen für die EU, in *Vogl/Wandt* (Hrsg), Grundrechtsschutz, Minderheitenschutz, Datenschutz – Weichenstellungen für Europa (2012) 97; *Priebe*, Die innere Sicherheit im Lichte des neuen Datenschutzrahmens, ebenda, 115; *Lachmayer*, Zur Reform des europäischen Datenschutzes. Eine erste Analyse des Entwurfs der Datenschutz-Grundverordnung, ÖJZ 2012, 841.

223 Art 2 Abs 1 RLvorschlag (FN 222).

224 Art 5 und 6 RLvorschlag (FN 222).

225 Art 40, 41 RLvorschlag (FN 222).

226 Art 50 Z 2, Art 53 Z 1 RLvorschlag (FN 222).

227 Art 51 RLvorschlag (FN 222).

228 Va Art 35, 36 RLvorschlag (FN 222).

229 RLvorschlag (FN 222).

230 So auch die Stellungnahme des Europäischen Datenschutzbeauftragten www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_DE.pdf (Stand 13.12.2012) 5 ff.

231 ZB Art 13 RLvorschlag (FN 222) zu den Einschränkungen des Auskunftsrechts.

232 Art 59 RLvorschlag (FN 222).





Anwendungsbereich. Nicht nur die Datenverwendung, sondern auch der Datenschutz erfährt also einen weiteren Europäisierungsschub.[233]

## C. Bleibende Probleme

Vermutlich wird die neue DatenschutzRL einige Probleme lösen. Andere werden aber sicher bleiben. Dazu gehören die Fortdauer von ernsthaften Sicherheitsbedrohungen, die Notwendigkeit der Zusammenarbeit mit unterschiedlich mächtigen und rechtsstaatlich orientierten Partnern in einer unvollkommenen Welt, die fehlende Überblickbarkeit und Beherrschbarkeit des internationalen Informationsaustauschs, die Vermeidung von Diskriminierungen angesichts der Notwendigkeit von Generalisierungen und die rechtliche Beurteilung von Sicherheitsmaßnahmen, zu deren Anwendung und Effizienz aus Sicherheitsgründen keine Informationen preisgegeben werden (dürfen), so dass man sich mit der Plausibilität von bloßen Behauptungen begnügen muss. Angesichts der immer weiter wachsenden technischen Möglichkeiten fällt datenschutzrechtlicher Optimismus daher schwer.

233 Vgl aus deutscher Sicht *Britz* (FN 201); *Wollenschläger* (FN 91) 51 ff; *Kotzur*, Der Schutz personenbezogener Daten in der europäischen Grundrechtsgemeinschaft, EuGRZ (2011) 105; *Masing*, Ein Abschied von den Grundrechten, Süddeutsche Zeitung 9.1.2012; *Masing*, Herausforderungen des Datenschutzes, NJW 2012, 2305 (2310 f).

VERHANDLUNGEN DES ACHTZEHNTEN ÖSTERREICHISCHEN JURISTENTAGES LINZ 2012

**Band I/2**

# Öffentliches Recht

## Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit

**Referate und Diskussionsbeiträge**

Wien 2013
Manzsche Verlags- und Universitätsbuchhandlung

**Zitiervorschlag:** 18. ÖJT Band I/2 [Seite]

**Herausgeber:**

Österreichischer Juristentag



ISBN 978-3-214-09144-6



# Inhaltsverzeichnis