universität wien

DISSERTATION

Titel der Dissertation

„Moderne Verwaltung und Datenschutz – ein Widerspruch?“

Verfasser

Egmar Wolfeil

angestrebter akademischer Grad

Doktor der Rechtswissenschaften (Dr. iur.)

Wien, 2012

Studienkennzahl lt. Studienblatt:	A 083 101
Dissertationsgebiet lt. Studienblatt:	Rechtswissenschaften
Betreuer:	Ao. Univ.-Prof. Mag. DDr. Erich Schweighofer

Inhaltsverzeichnis

Abstract: ..... - 1 -
1. Einleitung ..... - 2 -
1.1 Gegenstand der Arbeit ..... - 2 -
1.2 Ziele der Arbeit ..... - 2 -
1.3 Gang der Untersuchung ..... - 3 -
2. Datenschutzrechtliche Rahmenbedingungen für die Verarbeitung personenbezogener Daten durch staatliche Organe ..... - 4 -
2.1 § 1 Datenschutzgesetz 2000 ..... - 4 -
2.2 Art 8 der Europäischen Menschenrechtskonvention ..... - 5 -
2.3 Art. 10 a StGG ..... - 7 -
2.4 Verhältnis von Art. 8 EMRK und § 1 DSG 2000 ..... - 9 -
2.5 Die Richtlinie 95/46 EG ..... - 11 -
2.6 Abgrenzung von nationalem und gemeinschaftsrechtlichem Datenschutz ..... - 13 -
2.7 Rechtsprechung des EuGH zum Datenschutz ..... - 14 -
2.8 Rechtsprechung des EGMR zum Datenschutz in Art. 8 EMRK ..... - 17 -
2.8.1 Eingriff in die Privatsphäre ..... - 17 -
2.8.2 Gesetzliche Grundlage ..... - 18 -
2.8.2.1 Bestimmtheit der gesetzlichen Regelung ..... - 18 -
2.8.2.2 Legitimes Ziel ..... - 20 -
2.8.3 Verhältnismäßigkeit ..... - 20 -
2.9 Verhältnis von § 1 DSG 2000 und Art. 8 EMRK ..... - 22 -
2.10 Löschung und Archivierung ..... - 25 -
2.11 Europäisierung des Datenschutzes ? ..... - 29 -
3. Umsetzung des Datenschutzes bei der Formulierung von Gesetzen ..... - 32 -
4. E-Government-Gesetz, EGovG ..... - 34 -
4.1 Der Begriff E-Government ..... - 34 -
4.2 Die Entwicklung des E-Government ..... - 35 -
4.3 Die gesetzlichen Grundlagen des E-Government ..... - 38 -
4.4 Das Konzept des Datenschutzes im E-Government, Identifizierung, Bürgerkarte ..... - 40 -
4.5 Zweckbindung im Datenschutz und Amtshilfe ..... - 41 -

4.5.1 Der Begriff der Zweckbindung ..... - 45 -
4.6 Kritische Betrachtung des Datenschutzkonzeptes im EGovG ..... - 51 -
4.7 Datenschutz bei ämterübergreifenden Verwaltungshandeln ..... - 53 -
4.8 Die Europäisierung der Amtshilfe ..... - 57 -
4.9 Zusammenfassung zum EGovG und Datenschutz ..... - 63 -
5. Bildungsdokumentation ..... - 65 -
5.1 Identifizierung und Nummerierung ..... - 66 -
5.2 Zusammenfassende Betrachtung der Identifizierung nach dem BilDokG ... - 72 -
5.3 Beachtung datenschutzrechtlicher Kriterien ..... - 78 -
5.3.1 Erforderlichkeit der Datenverwendung ..... - 80 -
5.3.2 Löschung von personenbezogenen Daten ..... - 84 -
5.4 Zusammenfassung zum BilDokG ..... - 86 -
6. Registerzählungsgesetz ..... - 88 -
7. Datenschutz im Gesundheitswesen ..... - 94 -
7.1 Die Entwicklung der Elektronischen Gesundheitsakte (ELGA) ..... - 95 -
7.2 Datenschutzrechtliche Rahmenbedingungen für ELGA ..... - 97 -
7.3 Das GTelG 2011 ..... - 100 -
7.4 Rechtliche Begründung des GTelG 2011 ..... - 101 -
7.5 Zusammenfassende Stellungnahme zum GTelG 2011 ..... - 107 -
8. Datenverwendung und Datenschutz bei der Sicherheitspolizei ..... - 110 -
8.1 Einleitung ..... - 110 -
8.2 Sachliche und örtliche Zuständigkeit bei der Sicherheitspolizei ..... - 112 -
8.3 Ausgewählte Beispiele der Datenverwendung bei der Sicherheitspolizei . - 115 -
8.4 Voraussetzungen für Eingriffe der Sicherheitspolizei in das Recht auf Datenschutz ..... - 121 -
8.5 Prüfung der Datenschutzregelungen des SPG nach den vom EGMR entwickelten Kriterien ..... - 122 -
8.5.1 Regelungen des SPG, die eine Speicherung von personenbezogenen Daten ohne Vorliegen einer sonst üblichen Gefahrensituation im Sinne von § 16 Abs. 1 SPG ermöglichen ..... - 124 -
8.5.2 Exkurs zur Strafprozessordnung ..... - 125 -
8.5.3 Entsprechen die Voraussetzungen für die anlasslose und geheime Verwendung personenbezogener Daten im Rahmen der erweiterten Gefahrenforschung (§ 21 Abs. 3 SPG) den Anforderungen des Art. 8 Abs. 2 EMRK? ..... - 126 -

8.6 Entsprechen die mit der Novelle 2007 eingeführten Bestimmungen der § 53 Abs. 3 a und 3 b SPG datenschutzrechtlichen Anforderungen? ..... - 136 -
8.7 Zusammenfassung ..... - 139 -
8.7.1 Schlussfolgerungen ..... - 139 -
8.7.2 Rechtswirkungen der Urteile des EGMR ..... - 141 -
8.8 Terrorismusbekämpfung in der EU ..... - 141 -
9. Internationale polizeiliche Zusammenarbeit und Datenschutz ..... - 143 -
9.1 Interpol ..... - 143 -
9.2 Instrumente des Datenaustausches in der Europäischen Union ..... - 146 -
9.2.1 Das Europäische Polizeiamt (Europol) ..... - 148 -
9.2.1.1 Entwicklung von Europol ..... - 148 -
9.2.1.2 Aufgaben von Europol ..... - 148 -
9.2.1.3 Verantwortung für den Datenschutz ..... - 151 -
9.2.1.4 Datenschutz und Rechtsschutz ..... - 152 -
9.2.1.4.1 Datenschutz in Österreich in der Zusammenarbeit mit Europol ..... - 152 -
9.2.1.4.2 Datenschutz bei Europol ..... - 154 -
9.2.1.4.3 Zwischenergebnis ..... - 170 -
9.2.1.4.4 Rechtsschutz bei Datenübermittlungen an Europol ..... - 171 -
9.2.1.4.5 Rechtsschutz gegen Maßnahmen von Europol ..... - 172 -
9.2.1.4.6 Rechtschutz gegen Europol durch Klage beim EGMR? ..... - 174 -
9.2.1.5 Zusammenfassende Stellungnahme zu Europol ..... - 175 -
9.2.2 Das Schengener Informationssystem (SIS) ..... - 177 -
9.2.3 Eurojust ..... - 180 -
9.2.4 Eurodac ..... - 184 -
9.2.5 Das Visa-Informationssystem VIS ..... - 186 -
9.2.6 Das Zollinformationssystem ZIS ..... - 189 -
9.2.7 Multilateraler Datenaustausch zwischen nationalen Polizeibehörden ..... - 193 -
9.2.7.1 Schwedische Initiative ..... - 194 -
9.2.7.2 Vertrag von Prüm und Ratsbeschluss vom 23. Juni 2008 ..... - 196 -
9.2.7.3 Richtlinie über Vorratsdatenspeicherung ..... - 200 -
10. Die Vorratsdatenspeicherung in Österreich ..... - 214 -
10.1 Grundzüge der gesetzlichen Regelung ..... - 214 -
10.2 Bestimmtheit der Vorschriften ..... - 218 -

10.3 Verhältnismäßigkeit ..... - 219 -
10.4 Speicherung von Vorratsdaten von zur Amtsverschwiegenheit verpflichteten Personen ..... - 221 -
10.5 Zusammenfassung zu Vorratsdatenspeicherung ..... - 223 -
11. Zusammenfassung und Schlussfolgerungen ..... - 225 -
11.1 Untersuchungsergebnisse Allgemeine Verwaltung ..... - 225 -
11.2 Untersuchungsergebnisse Sicherheitsbehörden ..... - 231 -

Abkürzungsverzeichnis

aaO	am angegebenen Ort
ABl	Amtsblatt der Europäischen Gemeinschaften
ABGB	Allgemeines Bürgerliches Gesetzbuch
Abs	Absatz
AEUV	Vertrag über die Arbeitsweise der EU
ÄrzteG	Ärztegesetz
Aufl	Auflage
BAO	Bundesabgabenordnung
Bd	Band
BEKZ	Bildungsevidenzkennzahl
BGM	Bundesgesundheitsministerium
BGBl	Bundesgesetzblatt
BilDokG	Bildungsdokumentationsgesetz
BilDokV	Bildungsdokumentationsverordnung
BMUKK	Bundesministerium für Unterricht, Kunst und Kultur
bPk	bereichsspezifische Personenkenziffer
BVerfG	Bundesverfassungsgericht (deutsch)
BVerfGE	Entscheidungen des (deutschen) Bundesverfassungsgerichts
B-VG	Bundesverfassungsgesetz
Diss	Dissertation
DSK	Datenschutzkommission
DS-RL	Datenschutzrichtlinie
DSRLK	Datenschutzrichtlinie für die elektronische Kommunikation
DuD	Datenschutz und Datensicherheit (Zeitschrift)
eCard	elektronische Bürgerkarte
EDSR	Europäischer Datensxchutzbeauftragter
EGMR	Europäischer Gerichtshof für Menschenrechte
EGovG	E-Governmentgesetz
ELGA	Elektronische Gesundheitsakte

EMRK	Europäische Menschenrechtskonvention
EPA	Elektronische Patientenakte
EuDSK	Europäische Datenschutzkonvention
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische Grundrechtezeitschrift
Eurodac	Europäische Datenbank zur Speicherung von Fingerabdrücken
Eurojust	Europäische Einheit für justizielle Zusammenarbeit
Europol	Europäisches Polizeiamt
Eu-PolKG	Eu-Polizeikooperationsgesetz
EUV	Vertrag über die Europäische Union (Lissabon-Fassung)
FS	Festschrift
GA	Generalanwalt
GDA	Gesundheitsdiensteanbieter
GRCh	Charta der Grundrechte der EU
HRRS	hrr-strafrecht.de, Online-Zeitschrift und Rechtsdatenbank
Hrsg	Herausgeber
insb	insbesondere
ITK	Informations- und Kommunikationstechnik
IuK	Informations- und Kommunikationstechnik
iVm	in Verbindung mit
JuS	Juristische Schulung (Zeitschrift)
JZ	Juristenzeitung
Kap	Kapitel
KAKuG	Bundesgesetz über Krankenanstalten und Kuranstalten
Mio	Millionen
Mrd	Milliarden

MRG	Mietrechtsgesetz
NJW	Neue Juristische Wochenzeitschrift
Nr	Nummer
ÖJZ	Österreichische Juristenzeitung
ORF	Österreichischer Rundfunk
PolKG	Polizeikooperationsgesetz
PHG	Produkthaftungsgesetz
Prot	Protokoll
Rdnr	Randnummer
Rz	Randziffer
Slg	Sammlung
StGB	Strafgesetzbuch
StGG	Staatsgrundgesetz
StPO	Strafprozessordnung
UBG	Unternehmensgesetzbuch
VfSlg	Sammlung der Erkenntnisse des Verfassungsgerichtshofes
VwG	Verwaltungsgericht
VwGH	Verwaltungsgerichtshof
ZustG	Zustellgesetz

Abstract:

The following dissertation thesis represents an investigation of several legal acts related to public administration in respect to the concern given to aspects of data protection. At first the national and European legal basis of data protection will be described as well as the relevant jurisdiction of national and European courts. Special attention is given to the Austrian scheme for E-Government and its validity in the European context. The thesis investigates how this scheme has been realized in different sections with regard to the data protection, e.g. in the law for the documentation of education (Bildungsdokumentationsgesetz), in the law for the registration of people (Registerzählungsgesetz) and in the bill for the introduction of data processing in the institutions of medical care in Austria.The legal act concerning the activities of the police and the European or bilateral regulations for police cooperation have been analyzed with regard to aspects of data protection. Special attention was paid to the European Data Retention Directive and its application in Austria.

As a general result of the investigations it can be stated that compliance with data protection rules seems not to be a very important objective of the public administration. It is followed mainly in a formal manner, in a way not to violate data protection rules obviously; privacy of the citizen is not an urgent topic. It has been showed that there is a growing tendency in governmental institutions to learn as much as possible about the features of the citizens and to get complete profiles of them. As a conclusion, this should be stopped and further research should be made in other areas of governmental activities in order to complement this exemplary representation.

The scope of tools, which are used by the police and applied in international police cooperation in order to gain and utilize personal data of citizens, has been vastly extended with the growing phenomenon of international terrorism and the rise of crime rates in a global context. This at least has been the most used argument. On the other hand the measures to avoid misuse of personal data and to protect the privacy of citizens have not been developed to the same extent. The control of national police sections by independent public institutions and judge reserve for intervention into the private sphere of citizens have still to be improved.

1. Einleitung

1.1 Gegenstand der Arbeit

Mit einer gewissen zeitlichen Verzögerung im Verhältnis zur gewerblichen Wirtschaft wird auch in der öffentlichen Verwaltung massiv die elektronische Datenverarbeitung für die Abwicklung von Verwaltungsvorgängen und die Speicherung von Daten eingesetzt. Als Beispiele werden die Bestrebungen auf der Grundlage des EGovG, die Bildungsdokumentation, der geplante elektronische Gesundheitsakt ELGA und die Erweiterung der sicherheitspolizeilichen Befugnisse in § 53 SPG genannt. Mit der zunehmenden Technisierung und dem damit verbundenem Umfang an gespeicherten Informationen gewinnt der Datenschutz im Verhältnis Bürger/Staat eine wachsende Bedeutung. Es besteht das Bedürfnis, sich nicht jeder Kontrolle über die Verwendung und den Verbleib persönlicher Daten zu entledigen. Dass sich insoweit ein wachsendes soziales und damit letztendlich auch rechtliches Problem entwickelt, wird durch das Entstehen neuer politischer Gruppierungen deutlich, die den Datenschutz zu einer ihrer zentralen Forderungen erhoben haben[1]. In der nachfolgenden Arbeit soll untersucht werden, ob und inwieweit einzelne Datenanwendungen in der öffentlichen Verwaltung in Österreich den Anforderungen des Datenschutzes genügen. Zunächst wird der Prüfungsmaßstab näher beschrieben, d. h. welche datenschutzrechtlichen Normen relevant sind und welche Anforderungen diese an die gesetzlichen Regelungen stellen, die für das Handeln der Verwaltung in den einzelnen Tätigkeitsbereichen die Grundlage bilden. Besonderer Schwerpunkt wird dabei auf die in §§ 6 Abs. 1. Ziff. 2 und 7 Abs. 1 DSG 2000 sowie Art. 6 Abs. 1 der DS-RL geregelte Zweckbindung der jeweiligen Datenverarbeitung und -übermittlung gelegt.

1.2 Ziele der Arbeit

Mit der Arbeit wird das Ziel verfolgt, etwaige Schwachpunkte der gesetzlichen Regelungen für den Einsatz der der Datenverarbeitung in der öffentlichen Verwaltung in Bezug auf Grundsätze und Regeln des Datenschutzes aufzuzeigen und Vorschläge zu Verbesserungen zu unterbreiten. Außerdem sollen national und in europäischem

---

[1] Die Piratenpartei gibt es mittlerweile auch in Österreich, http://www.piratenpartei.at/, letzter Abruf am 20.12. 2011.

Rahmen Entwicklungstendenzen zu einem der technischen Entwicklung angepassten Datenschutz im Bezug auf staatliches Handeln aufgezeigt werden.

1.3 Gang der Untersuchung

Zunächst soll dargestellt werden, an welche wesentlichen datenschutzrechtlichen Bestimmungen der Gesetzgeber bei den gesetzlichen Regelungen für einzelne Bereiche der Verwaltung und den damit verbundenen Umgang mit personenbezogenen Daten der Bürger gebunden ist. Das bedeutet, es wird nicht konkretes Verwaltungshandeln untersucht, das könnte nur durch Prüfung einzelner Verwaltungsakte erfolgen, sondern die gesetzlichen Vorschriften, die für das jeweilige Verwaltungshandeln maßgeblich sind. In den folgenden Schritten sollen wesentliche Bereiche der öffentlichen Verwaltung bzw. die für sie geltenden Vorschriften auf ihre Vereinbarkeit mit den Anforderungen des Datenschutzes untersucht werden. Dabei soll auch der Frage nachgegangen werden, inwieweit der Datenschutz durch geeignete technische Maßnahmen bei der Gestaltung der Anwendungen gewährleistet werden kann, also der Frage des Datenschutzes durch Technikgestaltung.

.

2. Datenschutzrechtliche Rahmenbedingungen für die Verarbeitung personenbezogener Daten durch staatliche Organe

2.1 § 1 Datenschutzgesetz 2000

Der Anspruch der Bürger auf Geheimhaltung der sie betreffenden personenbezogenen Daten gemäß § 1 Abs. 1 DSG ist ein Grundrecht, welches sich von anderen u.a. dadurch unterscheidet, dass es nicht nur im Verhältnis zum Staat, sondern auch gegenüber Privaten geltend gemacht werden kann.[2] Dieses Grundrecht wird seit dem Volkzählungsurteil des deutschen Bundesverfassungsgerichts im Jahre 1983[3] in Europa allgemein als das Recht auf informationelle Selbstbestimmung[4] bezeichnet.

Nach § 1 Abs. 2 DSG 2000 dürfen personenbezogene Daten grundsätzlich nur im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung verwendet werden. Beschränkungen des Anspruchs auf Geheimhaltung sind nur im überwiegenden Interesse eines anderen zulässig und, soweit der Eingriff durch eine staatliche Behörde erfolgt, darf dieser nur auf der Grundlage von Gesetzen erfolgen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) genannten Gründen erforderlich sind. Ein überwiegendes öffentliches Interesse für einen staatlichen Eingriff ist also nur dann gegeben, wenn der Eingriff aus einem der in § 8 Abs. 2 EMRK genannten Gründe notwendig und verhältnismäßig ist und dafür eine gesetzliche Grundlage besteht.[5] Bei der Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, muss für die entsprechenden gesetzlichen Vorschriften ein **wichtiges** öffentliches Interesse gegeben sein und zugleich müssen angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festgelegt werden. Selbst wenn Beschränkungen zulässig sind, darf ein Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden. Als besonders schutzwürdige Daten beschreibt das Gesetz in § 4 Ziffer 2 DSG 2000 Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung und Gesundheit oder Se-

---

[2] Mayer-Schönberger/Brandl, Datenschutzgesetz, 2. Aufl. 2006, S.23.
[3] BVerfGE 65, S. 1ff = NJW 1984, S. 419 ff.
[4] Mayer-Schönberger/Brandl, aaO., S. 13.
[5] Mayer-Schönberger/Brandl, aaO. S. 65, Jahnel Handbuch Datenschutzrecht, 2010, Kap. 2/58, S. 67..

xualleben. Für den in Kapitel 9 behandelten Datenschutz im Gesundheitswesen soll hier festgehalten werden, dass für staatliche Eingriffe in das Grundrecht auf Datenschutz ein wichtiges öffentliches Interesse vorliegen muss.

2.2 Art 8 der Europäischen Menschenrechtskonvention

Österreich ist 1958 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten, EMRK, beigetreten (BGBl. 210/1958). Die ERMK hat wie § 1 DSG 2000 den Charakter einer Verfassungsnorm (BVG BGBl. Nr. 59/1964). Art. 8 Abs. 2 EMRK, auf den § 1 Abs. 2 DSG 2000 Bezug nimmt, legt fest, dass der Eingriff einer Behörde nur auf einer gesetzlichen Grundlage stattfinden darf und darüber hinaus eine Maßnahme darstellen muss, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung, und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist. Mit anderen Worten gesagt, Eingriffe in das informationelle Selbstbestimmungsrecht seitens der Behörden dürfen nur auf der Grundlage eines Gesetzes und nur in dem Umfange erfolgen, wie dies für das Funktionieren und den Bestand eines demokratischen Staatswesens erforderlich ist.
Die Rechtsprechung der Europäischen Kommission für Menschenrechte, EKMR, und des Europäischen Gerichtshofes für Menschenrechte, EGMR, zum Datenschutz entwickelte sich auf der Grundlage von Art. 8 Abs. 1 EMRK, der da lautet:

Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

In dieser Bestimmung wird ein Recht auf Datenschutz nicht ausdrücklich genannt. Die EKMR hat zunächst auf der Grundlage dieser Bestimmung ein Recht des Einzelnen auf Schutz der Privatsphäre erkannt (X gg. Vereinigtes Königreich[6], X gg. Island[7]), das eine Garantie für das Heraushalten des Staates aus dem privaten Bereich des Einzelnen beinhaltet. In der Sache Brüggemann und Scheuten gg. Bundesre-

[6] EKMR vom 12.10.1973(App. 5877/72), Yearbook XVI (1973), S. 328
[7] EKMR vom 18.05 1976, Decisions and Reports of the European Commission of Human Rights (DR) 5, S. 86

publik Deutschland[8] wurde dieser Grundsatz dahingehend erweitert, dass der Anspruch auf Achtung des Privatlebens für den Einzelnen die Sicherung eines Bereiches umfasst, innerhalb dessen er seine Persönlichkeit frei entfalten und erfüllen kann. In dem Fall Pretty gg. Vereinigtes Königreich[9] stellt der EGMR fest, dass Art. 8 zwar nicht ausdrücklich ein Recht auf Selbstbestimmung enthalte, dass die persönliche Autonomie aber Bestandteil der durch diese Bestimmung gewährten Garantien sei. Ohne den Begriff Datenschutz zu verwenden, wird in der Sache Klaas gg. Bundesrepublik Deutschland festgestellt, dass die Telefonüberwachung in den Schutzbereich von Art. 8 EMRK fällt. Entsprechend hat die EKMR im Fall X gg. Vereinigtes Königreich[10] entschieden, dass die Erhebung von persönlichen Daten im Rahmen einer Volkszählung grundsätzlich eine Beeinträchtigung des Rechts auf Privatsphäre im Sinne von Art. 8 Abs. 1 EMRK darstelle. In dem Fall Leander gg. Schweden[11] hat der EGMR die Speicherung von Informationen mit Bezug zum Privatleben als von Art. 8 Abs. 1 EMRK erfasst angesehen, ebenso die EKMR die Erfassung von persönlichen Identifizierungsmerkmalen in öffentlichen Registern im Falle Lundvall gg. Schweden[12]. Mit diesen beiden Entscheidungen sind die Grundlagen für den Schutz persönlicher Daten auf Basis von Art. 8 Abs. 1 EMRK gelegt worden. In dem Urteil Amann gg. Schweiz[13] stellt der EGMR einen Bezug zur Datenschutzkonvention des Europarates vom 28.01.1981 her und rechtfertigt damit die Erstreckung der durch Art. 8 geschützten Privatsphäre auf den Schutz persönlicher Daten. In Österreich ist diese Konvention am 01.07.1988 in Kraft getreten[14]. Auch bezüglich des Schutzbereiches bezieht sich der EGMR auf die genannte Konvention, deren Zweck es sei, die Rechte und Grundfreiheiten von jedermann, insbesondere das Recht auf einen Persönlichkeitsbereich bei der automatischen Verarbeitung personenbezogener Daten, zu schützen, Art. 1 der Konvention. Diese definiert die personenbezogenen Daten als *jede Information über eine bestimmte oder bestimmbare natürliche Person*, Art. 2 Buchst. a der Konvention. Auch in der weiteren Rechtsprechung hat der EGMR in einer Reihe von Entscheidungen Grundsätze für die rechtmäßige Bearbei-

---

[8] EKMR vom 12.07.1977, DR 10, S. 100, abgdr. in EuGRZ 1978, S. 199.
[9] EGMR vom 29.04.2002, Pretty gg. Großbritanien, EuGRZ 2002, S. 234, ÖJZ 2003, S. 311.
[10] EKMR vom 12.10.1973, App. 5877/72, Yearbook XVI (1973), S. 328, .
[11] EGMR vom 26.03.1987, Leander gg Schweden, EGMR-E 3, S. 430.
[12] EKMR vom 11.12.1985, App. 10473/83, DR 45, S. 121.
[13] EGMR vom 16.02.2000, Amann gg Schweiz, ÖJZ 2001, S. 71.
[14] BGBl. Nr. 317/1988.

tung personenbezogener Daten entwickelt, die denen in Art. 5 der Datenschutzkonvention des Europarates entsprechen. U. a. muss die Bearbeitung entsprechend Treu und Glauben erfolgen, es gilt der Grundsatz der Zweckbindung, der Grundsatz der Verhältnismäßigkeit, der auch ein Verbot des Sammelns von Daten auf Vorrat beinhaltet, und schließlich besondere Anforderungen an die gesetzlichen Vorschriften, welche das Sammeln und Speichern von Daten erforderlich machen.[15]

2.3 Art. 10 a StGG

Die im Jahre 1974 (BGBl. 8/1974) in das Staatsgrundgesetz eingefügte Bestimmung gewährt die Unverletzlichkeit des Fernmeldegeheimnisses. Ausnahmen sind nur auf der Grundlage eines richterlichen Befehls in Übereinstimmung mit bestehenden Gesetzen zulässig. Umstritten ist, ob nur der Inhalt der Kommunikation durch die Vorschrift geschützt wird oder auch die Verbindungsdaten umfasst werden.[16] Der OGH geht in einer Entscheidung aus dem Jahre 1998 ohne nähere Diskussion der Problematk mit Hinweis auf die einschlägige Literatur davon aus, dass auch die Vermittlungsdaten vom Schutz des Art. 10 a StGG erfasst werden.[17] In der Literatur wird zum Teil eine gegenteilige Meinung vertreten. Systematisch sei Art. 10 a StGG dem Briefgeheimnis nachempfunden, das sich nicht auf die äußeren Kommunikationsdaten erstreckt. Im Übrigen mache es aus teleologischer Perspektive Sinn, den einem Richtervorbehalt unterliegendem Schutz des Art. 10 a StGG auf Inhaltsdaten zu beschränken, weil ihre Überwachung im Vergleich zum Zugriff auf die Verbindungsdaten für die betroffenen Personen die stärkere Bedrohung darstelle.[18] Diese Auffassung dürfte angesichts der fortgeschrittenen technischen Entwicklung inzwischen überholt sein, weil die elektronische Auswertung von Verbindungsdaten und Standortdaten bei Mobiltelefonen die Darstellung von Profilen einer Person erlaubt, die in ihren Aussagen über eine Person häufig über das Ergebnis einzelner abgehörter Gespräche hinausgehen. Damit dürfte die Auswertung von Verbindungsdaten in ihrer

---

[15] Schweizer, Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zum Persönlichkeits- und Datenschutz, DuD 2009, S. 462 ff, (468); eine ausführliche Darstellung der Rechtsprechung der EKMR und des EGMR zum Datenschutz findet sich bei Siemen, Datenschutz als europäisches Grundrecht, 2006, S. 51 ff.

[16] Wiederin in Merten/Papier (Hrsg.), Handbuch der Grundrechte, Band VII/1 Grundrechte in Österreich 2009, S. 217.

[17] Entscheidung des OGH vom 17.06.1998, 13 Os 68/98, http://www.ris.bka.gv.at/Dokumente/Justiz/JJT_19980617_OGH0002_0130OS00068_9800000_000/JJT_19980617_OGH0002_0130OS00068_9800000_000.pdf, letzte Abfrage 19.01.2012.

[18] Wiederin aaO., S. 217.

Eingriffstiefe der Auswertung einzelner Kommunikationsinhalte mindestens gleichstehen. Außerdem ist zu berücksichtigen, dass bei Erfassung von Verbindungsdaten zwangsläufig auch die Daten der Verbindungsteilnehmer erfasst werden, die nicht Ziel der jeweiligen Untersuchungen sind. Im Sinne einer teleologischen Auslegung der Bestimmung, die dem Schutz der Privatsphäre dient, spricht also mehr dafür, auch die Verbindungsdaten in den Schutz des Art. 10 a StGG einzubeziehen.
Allerdings hat diese Auslegungsfrage geringe praktische Bedeutung, weil Verbindungsdaten personenbezogene Daten im Sinne von § 4 Ziffer 1 DSG 2000 sind und damit vom Schutz des § 1 Abs. 1 DSG 2000 und als Bestandteil der Privatsphäre von dem des Art. 8 Abs.1 EMRK erfasst werden.[19] Dem entsprechend prüft der OGH im Rahmen der Zulässigkeit von Maßnahmen nach § 149 a StPO, zu denen er auch die rückwirkende Erfassung von Verbindungsdaten rechnet, ob die Verhältnismäßigkeit im Sinne von § 1 Abs. 2 DSG 2000 und Art. 8 Abs. 2 EMRK unter Berücksichtigung der Schwere der verfolgten Straftat gegeben ist. Die Maßnahme müsse einem anerkannten (legitimen) Ziel sowie einem zwingenden sozialen Bedürfnis entsprechen und verhältnismäßig sein.[20]

Die einfach-gesetzlichen Vorschriften zum Fernmeldegeheimnis finden sich im Telekommunikationsgesetz 2003 (TKG 2003),[21] §§ 93 Abs. 1 und 96 Abs. 1 TKG. Das aktuelle Gesetz berücksichtigt u.a. die Datenschutzrichtlinie für die elektronische Kommunikation[22] und die Richtlinie über Vorratsdatenspeicherung[23] Die geplante Vorratsdatenspeicherung in Österreich wird in Kapitel 10 diskutiert.

---

[19] Uerpmann-Wittzak in Ehlers (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Auflage 2009, § 3 Rn. 6, S. 84
[20] Entscheidung des OGH vom 06.12.1995, Os 13 161/95, http://www.ris.bka.gv.at/Dokumente/Justiz/JJT_19951206_OGH0002_0130OS00161_9500000_000/JJT_19951206_OGH0002_0130OS00161_9500000_000.pdf , Entscheidung des OGH vom 17.06.1998, 13 Os 68/98, letze Abfrage 20.12.2011. http://www.ris.bka.gv.at/Dokumente/Justiz/JJT_19980617_OGH0002_0130OS00068_9800000_000/JJT_19980617_OGH0002_0130OS00068_9800000_000.pdf, letzte Abfrage 20.12..2011.
[21] BGBl. Nr. 70/2003.
[22] Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. L 201 vom 31.07.2002, S. 37 ff.
[23] Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, Amtsblatt L 105 vom 13.04.2006, S. 54 ff.

2.4 Verhältnis von Art. 8 EMRK und § 1 DSG 2000

Einerseits geht der Schutzumfang von Art. 8 Abs. 1 EMRK weiter, weil er nicht nur den Schutz personenbezogener Daten, sondern die gesamte Privatsphäre und das Familienleben umfasst. Deren Grenzen sind allerdings unbestimmt, weil sie sich einer genauen Definition entziehen, wie der EGMR selbst einräumt. Andererseits bezieht sich die Schutzwirkung bei Art. 8 EMRK auf das Verhältnis zum Staat und nicht auf Schutzgutverletzungen durch Private.[24] Gegenüber letzteren ist durch die EMRK lediglich mittelbar ein Schutz insoweit gegeben, als dem Staat Schutzpflichten gegenüber den Bürgern obliegen, denen er durch Gesetze und andere Maßnahmen entsprechen muss.[25]

Der Schutzbereich des § 1 Abs. 1 DSG 2000 bezieht sich auch auf das Verhältnis zu natürlichen und juristischen Personen des Privatrechts. Das wird u.a. durch die Vorschrift über den Rechtsweg bei Rechtsverletzungen durch Private in § 32 Abs. 1 DSG 2000 verdeutlicht. Weiter umfasst der Anspruch auf Geheimhaltung nicht nur Daten aus dem Bereich des Privat- und Familienlebens, sondern auch den Bereich des wirtschaftlichen und politischen Lebens.[26] Andererseits ist der Anspruch auf Geheimhaltung personenbezogener Daten dadurch eingeschränkt, dass als Voraussetzung für das Bestehen des Anspruchs schutzwürdige Geheimhaltungsinteressen des Betroffenen gegeben sein müssen. Anders als bei Art. 8 Abs. 1 EMRK, nach dem jede Verwendung personenbezogener Daten zunächst einmal als Eingriff in das Grundrecht des Art. 8 Abs. 1 EMRK zu werten ist, der einer Rechtfertigung nach Art. 8 Abs. 2 EMRK bedarf, setzt der Anspruch nach § 1 Abs. 1 DSG 2000 ein schutzwürdiges Interesse des Betroffenen als Tatbestandsmerkmal voraus. Der Anspruch hängt insoweit von einer Abwägung zwischen den Interessen des Verwenders und denen des Betroffenen ab.[27] Für sensible Daten im Sinne von § 4 Ziffer 2 DSG 2000 enthält § 9 DSG 2000 eine abschließende Auflistung von Fällen, in denen schutzwürdige Interessen als nicht verletzt gelten. Für nicht-sensible Daten enthält § 8 DSG 2000 eine beispielhafte nicht abschließende Aufzählung von Umständen, bei deren

---

[24] Wiederin in Merten/Papier (Hrsg.), Handbuch der Grundrechte, Band VII/1 Grundrechte in Österreich 2009, S. 179.
[25] Uerpmann-Wittzak in Ehlers (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Aufl. 2009, § 3 Rd.-Nr.26, S. 90.
[26] Wiederin in Merten/Papier (Hrsg.), Handbuch der Grundrechte, Band VII/1 Grundrechte in Österreich, 2009, Rd.-Nr.: 134, S. 223.
[27] Lehner, Das Datenschutzgesetz 2000 in Bauer/Reimer, Handbuch Datenschutzrecht, 2009, S. 130.

Vorliegen schutzwürdige Interessen als nicht verletzt anzusehen sind. Deshalb besteht die Auffassung, dass das schutzwürdige Interesse in jedem Falle zu prüfen ist, auch wenn keiner der im Gesetz für das Nichtbestehen genannten Fälle vorliegt. Als Richtschnur für die anzustellende Bewertung seien die Lehre und Rechtsprechung zu § 1 Abs. 1 DSG 1978 heranzuziehen.[28] Schutzwürdige Interessen als Anspruchsvoraussetzung bedeutet im Grunde, dass Fragen der Verhältnismäßigkeit, die üblicherweise im Rahmen der Rechtmäßigkeit der Datenverwendung geprüft werden, als Tatbestandsmerkmal gelten. Dies erscheint auch deshalb überzogen, weil nach § 1 Abs. 2 DSG im Rahmen der Prüfung der Rechtmäßigkeit in jedem Fall eine Interessenabwägung bei der Verarbeitung durch staatliche Stellen unter den Kriterien von Art. 8 Abs. 2 EMRK anzustellen ist. Mit dem DSG 2000 sollte u.a. die Richtlinie 95/46 EG vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Richtlinie, DS-RL[29]) umgesetzt werden. Die Richtlinie geht davon aus, dass der Schutz alle personenbezogenen Daten betrifft und eine Verwendung nur unter den in der Richtlinie genannten Kriterien zulässig (rechtmäßig) ist, Art. 5 bis 8 DS-RL. Als personenbezogene Daten gelten alle Informationen über eine bestimmte oder bestimmbare natürliche Person, Art. 2 Buchst. a DS-RL. Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann. Diese Definition schließt indirekt personenbezogene Daten ein, bei deren Verarbeitung nach §§ 8 Abs. 2 und 9 Ziffer 2 DSG 2000 schutzwürdige Interessen als nicht verletzt gelten, also ein Geheimhaltungsanspruch nicht besteht. Nach der Richtlinie ist die Interessenabwägung eine Frage der Rechtmäßigkeit der Verarbeitung, Art. 7 Buchst. f DS-RL.

Die Frage könnte praktische Auswirkungen in einem Prozess haben, weil jede Partei grundsätzlich die Voraussetzungen für die geltend gemachten Ansprüche zu beweisen hat, also der von einer Datenverwendung Betroffene die Umstände, die sein schutzwürdiges Interesse begründen. Der Verwender müsste das Vorliegen der Voraussetzungen für die Rechtmäßigkeit der Datennutzung beweisen. Wenn Art. 8 EMRK anwendbar ist, also ein Eingriff einer Behörde in die von Art 8 Abs. 1 EMRK geschützten Bereiche bei einer natürlichen Person vorliegt, braucht ein Betroffener

---

[28] Wiederin mit weiteren Nachweisen in Merten/Papier (Hrsg.), Handbuch der Grundrechte, Band VII/1 Grundrechte in Österreich 2009, Rd.-Nr.: 136, S.223 f.
[29] ABl. L 281, S. 31 vom 23.11.1995.

nur zu beweisen, dass ein Eingriff in die Privatsphäre durch Verwendung personenbezogener Daten stattgefunden hat. Die Behörde müsste dann ggf. die Rechtmäßigkeit nachweisen. Die Gerichte prüfen in einschlägigen Fällen die beiden Bestimmungen gemeinsam, so dass sich im gemeinsamen Anwendungsbereich der Bestimmungen keine Beweislastprobleme ergeben.[30]

2.5 Die Richtlinie 95/46 EG

Neben den Bestimmungen des DSG 2000 und der EMRK soll in diesem Zusammenhang auch die Richtlinie 95/46 EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutze natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum Datenverkehr (Datenschutzrichtlinie, DS-RL) näher betrachtet werden. Das DSG 2000 dient der Umsetzung dieser Richtlinie in nationales Recht.

Ein wesentliches Element der Richtlinie ist das zweistufige Verfahren für die Zulässigkeit der Verarbeitung von personenbezogenen Daten. Im Vordergrund steht dabei die strikte Zweckbindung. Der Zweck der Datenverwendung muss eindeutig und festgelegt sein und darf später nicht geändert werden, Art. 6 Abs. 1 Buchst. b DS-RL. Die Daten müssen in Bezug auf den verfolgten Zweck erheblich sein und dürfen nicht darüber hinausgehen, Art. 6 Abs. 1 Buchst. c DS-RL, sie müssen sachlich richtig sein und ggf. berichtigt oder gelöscht werden, Art. 6 Abs. 1 Buchst. d DSRL, und sie dürfen nicht länger gespeichert werden, wie dies für die Zwecke, für die sie erhoben worden sind, erforderlich ist, Art. 6 Abs. 1 Buchst. e DS-RL. In einem zweiten Schritt ist dann nach Art. 7 und 8 DSRL neben der Zweckbindung zu prüfen, ob eine der Ausnahmen für die Zulässigkeit der Verarbeitung personenbezogener Daten vorliegt. Bei der Verarbeitung durch staatliche Organe ist Art. 7 Buchst. e DS-RL einschlägig. Danach darf die Verarbeitung nur für eine Aufgabe geschehen, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Bei besonderen personenbezogenen Daten im Sinne von Art. 8 Abs. 1 DS-RL genügt nicht nur ein schlichtes öffentliches Interesse an der Verarbeitung, es muss ein wichtiges öffentliches Interesse vorliegen. Die Umsetzung dieser Bestimmungen der Richtlinie

---

[30] Entscheidung des OGH vom 06.12.1995, Os 13 161/95, http://www.ris.bka.gv.at/Dokumente/Justiz/JJT_19951206_OGH0002_0130OS00161_9500000_000/JJT_19951206_OGH0002_0130OS00161_9500000_000.pdf , letzte Abfrage 20.12.2011.

geschah durch die §§ 6 bis 9 DSG 2000. In der Literatur wird kritisiert, dass die Umsetzung der Richtlinie in nationales österreichisches Recht nicht immer korrekt und vollständig erfolgt sei, u.a. auch in dem hier gegebenen Zusammenhang.[31] So fehle in § 6 Abs. 1 Ziffer 4 die Verpflichtung aus Art. 6 Abs. 1 Buchst. d DS-RL, dass von dem für die Verwendung von Daten Verantwortlichen alle angemessenen Maßnahmen zu treffen sind, damit im Hinblick auf die Zwecke, für die sie erhoben und weiterverarbeitet werden, nichtzutreffende oder unvollständige Daten gelöscht oder berichtigt werden.

In diesem Zusammenhang wird darauf hingewiesen, dass seitens der EU auf der Grundlage von Art. 16 AEUV umfangreiche Änderungen im Datenschutzrecht geplant sind, auf die in den folgenden Kapiteln noch näher eingegangen werden wird. Am 25. 01.2012 hat die EU-Kommission einen Entwurf für eine Datenschutz-Grundverordnung[32] vorgelegt, die die DS-RL ersetzen soll und im Falle einer Verabschiedung in den Mitgliedstaaten der EU unmittelbar anzuwenden wäre. Ausgenommen von dem Anwendungsbereich der geplanten Verordnung bleibt der das Gebiet der polizeilichen und justiziellen Zusammenarbeit. Insoweit plant die Kommission eine Richtlinie[33], die dann in nationales Recht umzusetzen wäre. Der nationale Gestaltungsspielraum für das Datenschutzrecht wird voraussichtlich kleiner werden.

Ungeachtet dessen ergibt sich für den Fall abweichender Regelungen die Frage, welches Recht auch von den nationalen Gerichten und Behörden zu vorrangig beachten ist, nationales oder Gemeinschaftsrecht.

---

[31] Mayer-Schönberger/Brandl, Datenschutzgesetz, 2006, S. 21.

[32] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF, letzte Abfrage 20.04.2012.

[33] COM (2012) 0010, Vorschlag für RICHTLINIE 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, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:DE:HTML, letzte Abfrage 20.04.2012.

2.6 Abgrenzung von nationalem und gemeinschaftsrechtlichem Datenschutz

Ursprünglich bestand die Auffassung, dass beide Rechtskreise sich weder berühren noch beeinflussen, sondern unabhängig voneinander bestehen (sog. Zweikreistheorie).[34] Schon früh erkannte der EuGH, dass die Zweikreistheorie für die Vereinheitlichung des Rechts in der europäischen Gemeinschaft wenig geeignet war und entwickelte insbesondere in der Entscheidung Costa gg. ENEL den Grundsatz des Vorranges des Gemeinschaftsrechts gegenüber dem nationalen Recht.[35] Der EuGH sieht sich als berechtigt an, nationale Vorschriften auf ihre Vereinbarkeit mit europäischem Recht zu überprüfen und betont,

1. dass – im Gegensatz zu anderen völkerrechtlichen Verträgen – der EWG-Vertrag eine eigene Rechtsordnung darstelle, die die Mitgliedstaaten in ihre nationalen Rechtsordnungen übernommen haben [Rn. 8];
2. dass gegen das Recht des EWG-Vertrages verstoßende nationale Regelungen der vertraglich eingegangenen Verpflichtung der Mitgliedstaaten zur Gründung einer Gemeinschaft widersprechen (nämlich der Europäischen Wirtschaftsgemeinschaft) [Rn. 9 f.];
3. dass die Mitgliedstaaten ihre (gesetzgeberische) Souveränität zur Verabschiedung von eigenständigem nationalen Recht zugunsten der Europäischen Gemeinschaften beschränkt und auf diese übertragen haben [Rn. 8 ff.] [36]

Der Vorrang besteht allerdings nur dann, wenn ein Konflikt mit nationalem Recht besteht, also dann nicht, wenn nationales und Gemeinschaftsrecht zu gleichen Ergebnissen kommen oder das nationale Recht strengere Regeln als das Gemeinschaftsrecht vorsieht, Art. 137 Abs. 4 und 176 EGV (jetzt 153 Abs. 4 und 193 AEUV). Der Grundsatz des Vorrangs europäischen Rechts gilt nach Auffassung des EuGH auch im Verhältnis zu nationalem Verfassungsrecht.[37] Mit dem Prinzip des Vorrangs des Gemeinschaftsrechts ist die Verpflichtung nicht nur der nationalen Gerichte, sondern

---

[34] Von der EWG zur EU, S. 9, http://www.school-scout.de/extracts/18956/18956.pdf, letzte Abfrage 20.04.2012.

[35] EuGH vom 15.07.1964 (Rs 6/64) Flamio Costa gg. ENEL, Slg. 1964, S. 1251

[36] Siehe auch: EuGH, Rs. 26/62, Slg. 1963, S.1 (25) – van Gend & Loos, *„Aus alledem ist zu schließen, daß die Gemeinschaft eine neue Rechtsordnung des Völkerrechts darstellt, zu deren Gunsten die Staaten, wenn auch in begrenztem Rahmen, ihre Souveränitätsrechte eingeschränkt haben, eine Rechtsordnung, deren Rechtssubjekte nicht nur die Mitgliedstaaten, sondern auch die Einzelnen sind".*

[37] EuGH, Beschluss vom 22. Juni 1965, Acciaierie San Michele gg. Hohe Behörde der EGKS, Rs. 9/65, Slg. 1965, S. 37 (39).

auch der Behörden verbunden, Gemeinschaftsrecht anzuwenden, wenn nationale Bestimmungen diesem widersprechen, ebenso die Verpflichtung des nationalen Gesetzgebers, keine dem Gemeinschaftsrecht widersprechenden nationalen Vorschriften zu erlassen.[38] Diese Position ist in den Mitgliedstaaten nicht unbestritten.[39]

2.7 Rechtsprechung des EuGH zum Datenschutz

Wichtig ist in diesem Zusammenhang, dass der EuGH bei der Auslegung der DS-RL und der Kommunikations-Datenschutz-Richtlinie[40] auf das grundrechtliche Fundament des Datenschutzes zurückgreift und sich dabei ausdrücklich auf die ERMK und die Charta der Grundrechte der Europäischen Union bezieht.[41]

Die Weitergabe personenbezogener Daten an einen Dritten stellt danach unabhängig von der späteren Verwendung der übermittelten Informationen eine Beeinträchtigung des Rechts der Betroffenen auf Achtung ihres Privatlebens und damit einen Eingriff im Sinne von Art. 8 EMRK dar. Ein solcher Eingriff verstößt nur dann nicht gegen Art. 8 EMRK, wenn er "*gesetzlich vorgesehen*" ist. Dieser muss daher gemäß dem Erfordernis der Vorhersehbarkeit so genau formuliert sein, dass die Adressaten des Gesetzes ihr Verhalten danach einrichten können. Das Erfordernis der Vorhersehbarkeit hat im Datenschutzrecht mit der in Art. 8 Abs. 2 der Charta der Grundrechte der EU vom 7. Dezember 2000[42] ausdrücklich genannten Zweckbindung eine besondere

---

[38] http://europa.eu/legislation_summaries/institutional_affairs/decisionmaking_process/l14548_de.htm, letzter Zugriff 20.12.2011

[39] So hat z. B. das deutsche BVerfG zuletzt in seinem Urteil zum Lissabon-Vertrag seine Befugnis betont, Gemeinschaftsrecht auf seine Vereinbarkeit mit den europäischen Verträgen und dem nationalen Grundrechtskatalog zu überprüfen, BVerfG, Urteil vom 30.06.2009, JZ 2009, S. 890 ff.; siehe dazu auch Ronellenfitsch, Der Vorrang des Rechts auf informationelle Selbstbestimmung vor dem AEUV, DuD 2009, S. 451 ff..

[40] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L201/ 37 ff vom 31.07.2002, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:de:PDF, letzte Abfrage 20.12.2011.

[41] Urteil des EuGH vom 18.07.2007, C 275/06, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006J0275:DE:HTML, letzte Abfrage 20.12.2011, Rn. 61 bis 70; Urteil des EuGH (Große Kammer) vom 27. Juni 2006 , C-540/03, Europäisches Parlament gegen Rat der Europäischen Union, Rn. 35, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62003J0540:DE:HTML. Letzte Abfrage 20.12.2011; siehe auch Tinnefeld, Reformvertrag von Lissabon, Charta der Grundrechte und Rechtspraxis im Datenschutz, DuD 2009, S. 504.

[42] Amtsblatt der Europäischen Gemeinschaften C 364/1, http://www.europarl.europa.eu/charter/pdf/text_de.pdf, letzte Abfrage 20.12.2011.

Ausprägung gefunden. Obwohl eine Rechtsverbindlichkeit der Charta erst mit Inkrafttreten des Lissabon-Vertrages vom 03. 12. 2007[43] (d.h. seit 1. Dezember 2009) gegeben ist, hat der EuGH bereits in der Entscheidung Promusicae gg. Telefonica[44] auf den Grundrechtskatalog der Charta Bezug genommen. Gemäß dem zweiten Erwägungsgrund der Richtlinie 2002/58 sei Ziel dieser Richtlinie die Achtung der Grundrechte und sie stehe im Einklang mit den durch die Charta der Grundrechte der Europäischen Union anerkannten Grundsätzen. Insbesondere solle mit dieser Richtlinie gewährleistet werden, dass die in den Art. 7 und 8 jener Charta niedergelegten Rechte uneingeschränkt geachtet werden. Art. 7 der Charta gebe im Wesentlichen Art. 8 der am 04.11.1950 in Rom unterzeichneten Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten wieder, der die Achtung des Privatlebens garantiere, und Art. 8 der Charta proklamiere ausdrücklich den Schutz personenbezogener Daten.[45] Im Hinblick auf diese Rechtsprechung wird in der Literatur auch schon von einer Europäisierung des Datenschutzes gesprochen.[46]

Unter Berücksichtigung des Grundsatzes, dass die Befugnisse der Organe der EU nicht weiter gehen als ihnen solche durch die Verträge mit den Mitgliedstaaten übertragen worden sind, soll diese Aussage hinterfragt werden. Die Charta der Grundrechte der Europäischen Union, GRCh, gilt nicht uneingeschränkt, sondern nach Art. 50 Abs. 1 GRCh nur für die Organe, Einrichtungen und sonstige Stellen der Union unter Wahrung des Subsidiaritätsprinzips und für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union. In Abs. 2 der Bestimmung wird nochmals klargestellt, dass mit der Charta der Geltungsbereich des Unionsrechts nicht über die Zuständigkeit der Union hinaus ausgedehnt wird oder neue Befugnisse geschaffen werden. In Art. 3 Abs. 2 DS-RL ist bestimmt, dass die Richtlinie keine Anwendung auf die Verarbeitung personenbezogener Daten findet, die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemein-

---

[43] http://europa.eu/lisbon_treaty/full_text/index_de.htm, letzte Abfrage 20.12.2011.
[44] Urteil des EuGH (Große Kammer) vom 27. Juni 2006 , C-540/03, Europäisches Parlament gegen Rat der Europäischen Union, Rn. 35, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62003J0540:DE:HTML, letze Abfrage 20.12.2011.
[45] EuGH, Urteil vom 29. 01. 2008 - C-275/ 06, Promusicae gg. Telefonica, Rd.-Nr. 64, http://lexetius.com/2008,63, letzte Abfrage 20.12.2011.
[46] Tinnefeld, Reformvertrag von Lissabon, Charta der Grundrechte und Rechtspraxis im Datenschutz, DuD 2009, S. 504.

schaftsrechts fallen. Hierzu ist die Entscheidung des EuGH in Sachen Rechnungshof gg. Österreichischen Rundfunk u. a. sowie Christa Neumann und Josef lauermann gg. Österreichischen Rundfunk[47] von Interesse, deren erster Leitsatz lautet:

> *„Die Anwendbarkeit der Richtlinie 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr kann nicht davon abhängen, ob im jeweiligen Sachverhalt ein hinreichender Zusammenhang mit der Ausübung der durch den EG-Vertrag garantierten Grundfreiheiten, insbesondere mit der Arbeitnehmerfreizügigkeit, bestand. Eine gegenteilige Auslegung würde nämlich dazu führen, dass die Abgrenzung des Anwendungsbereichs der genannten Richtlinie ungewiss wäre und von Zufälligkeiten abhinge, was deren Hauptzweck zuwiderliefe, der darin besteht, die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten einander anzugleichen, um Hindernisse für das Funktionieren des Binnenmarktes zu beseitigen, die sich gerade aus den Unterschieden zwischen den nationalen Regelungen ergeben.“*

Der Gerichtshof argumentiert, die Richtlinie sei auf der Grundlage von Art. 100 a EGV (aF) (= Art. 95 EGV (nF) = Art. 114 AVEU) erlassen worden und solle dadurch die Harmonisierung der nationalen Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten für den freien Verkehr dieser Daten zwischen den Mitgliedstaaten sicherstellen. Nach Art. 1 Abs. 1 der Richtlinie gewährleisten die Mitgliedstaaten den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten, und nach Abs. 2 dieser Bestimmung dürfen sie den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten aus Gründen des nach Abs. 1 gewährten Schutzes nicht beschränken. Da somit alle personenbezogenen Daten zwischen den Mitgliedstaaten übermittelt werden können, erlange die

---

[47] EuGH vom 20.05.2003, verbundene Rs. C-465/00, C-138/01 und C-139/01, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000J0465:DE:NOT, letzte Abfrage 20.12.2011.

Richtlinie 95/46 grundsätzlich die Einhaltung von Regeln zum Schutz solcher Daten bei einer Verarbeitung im Sinne der Definition in Art. 3 DS-RL.[48]

Unter Berücksichtigung dieser Rechtsprechung sind im praktischen Ergebnis nur die in Art 3. Abs. 2 DSRL ausdrücklich genannten Sachgebiete von dem Geltungsbereich der Richtlinie ausgenommen, so dass sich aufgrund der erweiterten Zuständigkeiten nach dem Lissabon-Vertrag und auch in Zukunft weiter zu erwartender Rechtsakte der EU ein sehr breiter Anwendungsbereich ergibt.

Im Gegensatz zur Charta der Grundrechte der Europäischen Union und der DS-RL gibt es bei der ERMK keine Einschränkungen im sachlichen Geltungsbereich. Inzwischen sind auch alle Mitgliedstaaten der Konvention beigetreten.

2.8 Rechtsprechung des EGMR zum Datenschutz in Art. 8 EMRK

2.8.1 Eingriff in die Privatsphäre

Art. 8 EMRK enthält keine ausdrückliche Garantie des Rechts auf Schutz personenbezogener Daten. Er gewährleistet das Recht jeder Person auf Achtung ihres Privat- und Familienlebens und ihrer Korrespondenz. Der EGMR hat jedoch in ständiger Rechtsprechung den Datenschutz als spezifisch ausgestalteten Teilbereich des Rechts auf Privatleben angesehen.[49] Der Gerichtshof legt dabei den Begriff des Privatlebens weit aus. Er sei einer erschöpfenden Definition nicht zugänglich und umfasse die physische und psychische Unversehrtheit einer Person. Als mögliche Elemente werden Geschlecht, Name, sexuelle Orientierung, Informationen aus dem Privat- und Familienleben, die Gesundheit, ethnische Identität, das Bild und die Beziehungen zu anderen Menschen genannt.[50]
Es ist mittlerweile gefestigte Rechtsprechung des EGMR, dass jede Verwendung personenbezogener Daten einen Eingriff in die Privatsphäre im Sinne von Art. 8 Abs. 1 EMRK darstellt, der nur unter Voraussetzungen des Art. 8 Abs. 2 EMRK gerechtfer-

---

[48] EuGH vom 20.05.2003, verbundene Rs. C-465/00, C-138/01 und C-139/01, Rd.-Nr. 39 und 40, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000J0465:DE:NOT, letzte Abfrage 20.04.2012.
[49] Tettinger/Stein, Kölner Gemeinschaftskommentar zur Europäischen Grundrechtecharta, 2006, Art. 8 Rd.-Nr. 17.
[50] EGMR-Urteil vom 04.12.2008, Marper gg. Vereinigtes Königreich, EuGRZ 2009, S. 299 ff. (Ziffer 67, S. 307).

tigt werden kann.[51] Bereits die Speicherung von Daten, die das Privatleben einer Person betreffen, stelle einen Eingriff im Sinne von Art. 8 EMRK dar[52], auf die spätere tatsächliche Verwendung der Daten komme es nicht an.[53] Als personenbezogene Daten sind alle Informationen zu qualifizieren, die sich auf bestimmte oder bestimmbare Personen beziehen.[54]

2.8.2 Gesetzliche Grundlage

Neben der Voraussetzung eines Eingriffs muss die Maßnahme gesetzlich vorgesehen sein und auf einer innerstaatlichen Rechtsgrundlage beruhen. Die betreffende Rechtsvorschrift müsse hinreichend zugänglich und vorhersehbar sein, d.h. sie müsse so genau formuliert sein, dass der Einzelne sein Verhalten danach ausrichten könne.[55] Art. 8 Abs. 2 EMRK[56] setzt ferner voraus, dass für den Eingriff eine gesetzliche Grundlage besteht, die mit dem sonstigen nationalen Recht vereinbar ist.

2.8.2.1 Bestimmtheit der gesetzlichen Regelung

Es genügt jedoch nicht, dass irgendeine gesetzliche Ermächtigungsgrundlage besteht, sondern diese muss bestimmte qualitative Anforderungen erfüllen, um den Bedingungen der Konvention zu entsprechen, wie sie in deren Präambel festgelegt sind.[57] Diese Qualitätsanforderungen bedeuten, dass die fraglichen Vorschriften für

---

[51] EGMR Urteil vom 27. 03. 1987, Leander gg. Schweden, EGMR-E 3, S. 430, http://www.eugrz.info/PDF/EGMR3/EGMR03-35, Ziffer 48: „*Sowohl das Speichern von Daten als auch ihre Weitergabe, verbunden mit der Verweigerung einer Möglichkeit zum Widerspruch gegen die Weitergabe durch Herrn Leander, führen zu einem Eingriff in das Recht auf Achtung des Privatlebens, wie es Art. 8 Abs. 1 gewährt*“, letzte Abfrage 20.04.2012; EGMR Urteil vom 04.05.2000, Rotaru gg. Rumänien, ÖJZ 2001, S. 74 (75), Ziffer 43: “*The Court reiterates that the storing of information relating to an individual's private life in a secret register and the release of such information come within the scope of Article 8 § 1 (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48)”*, http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Rotaru&sessionid=98044349&skin=hudoc-en, Letzte Abfrage 01.06,2012.

[52] EGMR vom 26.03.1987, Leander gg. Schweden, Ziffer 48, http://www.eugrz.info/PDF/EGMR3/EGMR03-35, letze Abfrage 20.04.2012.

[53] EGMR vom 16.02.2000, Amann gg. Schweiz, Ziffer 65 und 70, ÖJZ 2001, S. 71 ff..

[54] EGMR vom 04.12.2008 (Marper./.Vereinigtes Königreich), EuGRZ 2009, S. 299 ff. Ziffer 68, S. 307

[55] EGMR vom 02.08.1984 (Malone ./.Vereinigtes Königreich), EuGRZ 1985, S. 17 ff..

[56] Art. 8 Abs. 2 EMRK :Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

[57] EGMR Urteil vom 02.02.2000, Amann gg. Schweiz, Ziffern 55 und 56, “*The Court would reiterate its opinion that the phrase ‘in accordance with the law’ does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is express-*

die Betroffenen zugänglich und vorhersehbar sind. Vorhersehbar sind sie nach Auffassung des EGMR nur dann, wenn sie so präzise und klar formuliert sind, dass der Einzelne sein Verhalten danach ausrichten kann.[58] Zusätzlich muss ein rechtlicher Schutzmechanismus gegen willkürliche Eingriffe der Behörden in durch die Konvention eingeräumte Rechte bestehen. Auch wenn die nationale Sicherheit berührt wird, müssen Maßnahmen, die in grundlegende Menschenrechte eingreifen, irgendeiner Form der rechtlichen Kontrolle durch eine unabhängige Instanz unterliegen. Die Behauptung der Behörde, dass die nationale Sicherheit berührt wird, muss hinterfragt werden können. Ohne eine entsprechende unabhängige Kontrollinstanz könnten die Behörden willkürlich in Konventionsrechte eingreifen.[59] Ferner muss die Regelung Vorkehrungen gegen willkürliche Eingriffe der staatlichen Behörden in die durch die Konvention gewährten Rechte aufweisen. Das Gesetz muss den Entscheidungsbereich der staatlichen Behörde und die Art und Weise der Ausübung der Kompetenzen mit ausreichender Klarheit festlegen, um eine willkürliche Inanspruchnahme der Kompetenzen zu vermeiden.[60]

---

ly mentioned in the preamble to the Convention ... The phrase thus implies – and this follows from the object and purpose of Article 8 – that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 ... Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident." http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Amann&sessionid=93049950&skin=hudoc-en, letzte Abfrage 23.04.2012, deutsche Kurzfassung des Urteils: ÖJZ 2001, S. 71 ff..

[58] EGMR Urteil vom 20.06.2002 Al-Nashif gg. *Bulgarien*, ÖJZ 2003, S. 344 ff. (346/347), Ziffer 119, *„Der GH wiederholt, dass die Wortfolge " gesetzlich vorgesehen" impliziert, dass die Rechtsgrundlage „zugänglich" und „vorhersehbar" sein muss…..Außerdem muss ein gewisses Maß an Rechtsschutz gegen willkürliche Eingriffe durch staatliche Behörden in die von der Konvention geschützten Rechte im innerstaatlichen Recht geben."*

[59] EGMR aaO. S. 347, vorstehende Fußnote.

[60] EGMR Urteil vom 17.06.2008, Meltex Ltd and Mesrop Movsesyan v. Armenia, http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Meltex%20|%20Ltd%20|%20Mesrop%20|%20Movsesyan%20|%20v.%20|%20Armenia&sessionid=92702268&skin=hudoc-en, Ziffer 81: *„ In addition, domestic law must afford a measure of legal protection against arbitrary interferences by public authorities with the rights guaranteed by the Convention. In matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference"*, letzte Abfrage 20.04.2012.

2.8.2.2 Legitimes Ziel

Im Rahmen der Verhältnismäßigkeit ist sodann zu prüfen, ob die durch das Gesetz ermöglichten Eingriffe den in Art. 8 Abs. 2 EMRK abschließend aufgeführten legitimen Zielen (*legitimate aim*) entsprechen und in einer demokratischen Gesellschaft als notwendig erachtet werden können (*necessary in a democratic society*).

2.8.3 Verhältnismäßigkeit

Ein Eingriff zur Verfolgung eines rechtmäßigen Zieles ist als notwendig in einer demokratischen Gesellschaft anzusehen, wenn er einem dringenden sozialen Bedürfnis entspricht und insbesondere, wenn er in Bezug auf das verfolgte Ziel verhältnismäßig ist und wenn die von den nationalen Behörden zu seiner Rechtfertigung vorgebrachten Gründe zutreffend und ausreichend sind. Dringend sozial notwendig bedeutet, dass das angestrebte Ziel ohne die gesetzliche Maßnahme nicht erreicht werden kann. Dabei ist auch zu prüfen, ob weniger eingriffsintensive Maßnahmen (gelindestes Mittel) zur Verfügung stehen.[61] Die für die Verhältnismäßigkeit erforderliche Bewertung ist von den nationalen Behörden vorzunehmen, unterliegt aber einer endgültigen Prüfung durch den EGMR.[62] Bei dieser Prüfung räumt der Gerichtshof den zuständigen nationalen Organen einen Beurteilungsspielraum ein, dessen Umfang von verschiedenen Faktoren wie Art des in Rede stehenden Rechts, seine Bedeutung für den Betroffenen, die Art des Eingriffs und das mit dem Eingriff verfolgte Ziel gehören.[63] Der Spielraum werde eher enger sein, wenn das in Rede stehende Recht von entscheidender Bedeutung dafür sei, ob der Betreffende sehr persönliche oder wichtige Rechte effektiv wahrnehmen könne.[64] Bei einem besonders wichtigen Aspekt der Existenz oder Identität des Betroffenen werde der Spielraum eingeschränkt

---

[61] EGMR Urteil vom 07.12.1976, Handyside gg. Vereinigtes Königreich, EuGRZ 1977, S. 38, Ziffer 58: " In der mündlichen Verhandlung vom 5. Juni 1976 hat der Delegierte , der die Meinung der Kommissionsminderheit vortrug, schließlich die Auffassung vertreten, der betroffene Staat habe nicht derart unerbittliche Maßnahmen ergreifen müssen wie die Einleitung der Strafverfolgung, die zur Verurteilung des Bf. und zur Einziehung, dann zur Vernichtung des Schulbuches geführt hat. Das Vereinigte Königreich habe den Grundsatz der Verhältnismäßigkeit verletzt, der dem Adjektiv „notwendig" innewohne, da es sich nicht damit begnügt habe, den Bf. zur Entfernung der anstößigen Stellen in seinem Buch aufzufordern oder den Verkauf und die Werbung für dieses Buch zu beschränken." .

[62] EGMR Urteil vom 04.12.2008 S. und Marper gg.Vereinigtes Königreich, Ziffer 101, EuGRZ 2009, S. 299 ff. (311).

[63] EGMR Urteil vom 27.05.2004, Connors gg. Vereinigtes Königreich, Nr. 66746/01, Ziffer 82, http://cmiskp.echr.coe.int/tkp197/view.asp?item=3&portal=hbkm&action=html&highlight=connors&sessionid=93051058&skin=hudoc-en , letzte Abfrage 20.04.2012.

[64] EGMR Urteil vom 27.05.2004, Connors gg. Vereinigtes Königreich, Nr. 66746/01, aaO., Ziffer 82.

sein.[65] In Fällen, bei denen es unter den Mitgliedstaaten des Europarates keinen Konsens über die Gewichtung der betroffenen Interessen oder ihres Schutzes gebe, werde der Spielraum weiter sein.[66] Der Beurteilungsspielraum ist ferner enger, wenn es um wesentliche Grundrechte geht ("*Wenn es um einen wesentlichen Aspekt der Existenz oder Identität einer Person geht, ist der Ermessensspielraum des Staates begrenzt."*). Andererseits ist der Spielraum weiter, wenn allgemeine soziale und wirtschaftliche Fragen oder moralische Gesichtspunkte zur Diskussion stehen, die in den einzelnen europäischen Staaten unterschiedlich beurteilt werden.[67]

Zusammenfassend stellt der EGMR fest, dass das Recht auf den Schutz personenbezogener Daten von grundsätzlicher Bedeutung für das durch Art. 8 EMRK geschützte Recht einer Person auf Achtung ihres Privat- und Familienlebens sei. Das innerstaatliche Recht müsse geeignete Schutzvorkehrungen vorsehen, die verhindern, dass personenbezogene Daten in einer Weise verwendet werden, die mit den Garantien nach diesem Artikel nicht vereinbar sind. Die Notwendigkeit solcher Vorkehrungen sei noch größer, wenn es um den Schutz personenbezogener Daten im Rahmen der automatischen Verarbeitung gehe, insbesondere wenn diese Daten zu polizeilichen Zwecken genutzt werden. Das innerstaatliche Recht müsse sicherstellen, dass die Daten für die Zwecke, für die sie gespeichert werden, erheblich seien und nicht über darüber hinausgehen, und dass sie insbesondere in einer Form aufbewahrt werden, welche die Identifizierung der Betroffenen nur so lange erlaubt, wie dies für den Zweck, zu dem diese Daten gespeichert werden, erforderlich sei.[68] In diesem Zusammenhang verweist der EGMR auf Art. 5 der Datenschutzkonvention und den Grundsatz Nr. 7 der Empfehlung des Ministerkomitees zur Regelung der Verwendung personenbezogener Daten im Polizeibereich.[69] Das bedeutet, perso-

---

[65] EGMR Urteil vom 10.04.2007, Evans gg. Vereinigtes Königreich, Nr. 6339/05, Ziffer 77, NJW 2008, S. 2013 (2015).
[66] EGMR vom 04.12.2007 (Dickson ./. Vereinigtes Königreich), Nr. 44362/04, Ziffer 78, NJW 2009, 971 (974/975).
[67] EGMR Urteil vom 10.04.2007, Evans gg. Vereinigtes Königreich, aaO. Ziffer 77.
[68] EGMR vom 04.12.2008 (Marper./.Vereinigtes Königreich), EuGRZ 2009, S. 299 ff. (Ziffer 103, S. 311).
[69] "*Principle 7 - Length of storage and updating of data,*
7.1. Measures should be taken so that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored. For this purpose, consideration shall in particular be given to the following criteria: the need to retain data in the light of the conclusion of an inquiry into a particular case; a final judicial decision, in particular an acquittal; rehabilitation; spent convictions; amnesties; the age of the data subject, particular categories of data.

nenbezogene Daten sind zu löschen, wenn keine zwingenden Gründe mehr für die weitere Speicherung sprechen.

2.9 Verhältnis von § 1 DSG 2000 und Art. 8 EMRK

Es erscheint angebracht, die Anwendungsbereiche des § 1 DSG 2000 und Art. 8 EMRK, die beide in Österreich Verfassungsrang innehaben, gegeneinander abzugrenzen. § 1 DSG 2000 gewährt einen Anspruch auf Geheimhaltung personenbezogener Daten. Dieser ist durch die Formulierung eingeschränkt „*soweit ein schutzwürdiges Interesse daran besteht".* Als nicht schutzwürdig ist nach Satz 2 des § 1 Abs. 1 DSG das Interesse dann anzusehen, wenn die Daten infolge ihrer allgemeinen Verfügbarkeit oder mangelnder Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind. Bei mangelnder Rückführbarkeit handelt es sich mangels Bezug zu einer Person nicht um personenbezogene Daten, so dass diese Einschränkung entbehrlich erscheint. Die in § 1 Abs. 1 DSG 2000 enthaltene Einschränkung „*soweit ein schutzwürdiges Interesse daran besteht*", stammt noch aus dem Vorgängergesetz DSG 1978. Für nicht sensible Daten enthält § 8 DSG 2000 eine beispielhafte Aufzählung von Fällen des Nichtbestehens schutzwürdiger Geheimhaltungsinteressen. Bei sensiblen Daten ist der Katalog in § 9 DSG 2000 eine abschließende Regelung.[70] Die DS-RL kennt keine Einschränkung auf schutzwürdige Geheimhaltungsinteressen. Sie gilt für alle personenbezogenen Daten, die automatisiert oder nicht automatisiert verarbeitet werden, Art 3 Abs. 1 DS-RL. Deshalb wird die Ansicht vertreten, die Bestimmung des § 1 Abs. 1 DSG 2000 sei richtlinienkonform in der Weise auszulegen, dass alle personenbezogenen Daten als schutzwürdig anzusehen sind, es sei denn, sie sind allgemein verfügbar.[71] Nach anderer Ansicht folgt aus dem Ausschluss eines schutzwürdigen Geheimhaltungsinteresses in bestimmten Fällen nicht, dass es in allen anderen Fällen von Gesetzes wegen als bestehend anzusehen wäre. Andernfalls bliebe die Bezugnahme auf schutzwürdige Geheimhaltungsinteressen in § 1 Abs. 1 DSG 2000 inhaltsleer. Selbst wenn in diesem Punkt eine Änderung der nach dem DSG von 1978 bestehenden Rechts-

---

7.2. Rules aimed at fixing storage periods for the different categories of personal data as well as regular checks on their quality should be established in agreement with the supervisory authority or in accordance with domestic law."

[70] Mayer-Schönberger/Brandl, Datenschutzgesetz, 2. Aufl. 2006, S. 80.

[71] Erläuterungen zum Beamtenentwurf Novelle 2010, zu Art. 2 , S. 4 u. 5, ftp://ftp.freenet.at/privacy/gesetze/dsg-novelle-2010-entwurf.pdf, letzte Abfrage 16.01.2012.

lage beabsichtigt gewesen wäre, komme dies im Wortlaut der Bestimmung nicht zum Ausdruck. Das schutzwürdige Interesse sei jeweils zu prüfen, wobei die Lehre und Rechtsprechung zu § 1 Abs. 1 DSG 1978 als Richtschnur für eine Bewertung gelten könnten.[72]

Diese Interpretation steht jedoch in Widerspruch zur Datenschutzrichtlinie der EU, die ja mit dem DSG 2000 in Österreich umgesetzt werden sollte. Nach Art. 2 Buchst. a DSRL sind personenbezogene Daten alle Informationen über eine bestimmte oder bestimmbare natürliche Person. In den Art. 8 und 9 DS-RL sind die Grundsätze und Voraussetzungen für die Verarbeitung von personenbezogenen Daten niedergelegt. Das Bestehen eines schutzwürdigen Interesses gehört nicht dazu. Ebenso wenig ergibt sich eine derartige Einschränkung aus Art. 8 Abs. 1 GRCh. Auch aus der Rechtsprechung des EGMR zu Art. 8 EMRK ist eine derartige Ausnahme nicht zu entnehmen. Jede Verwendung personenbezogener Daten ist zunächst einmal ein Eingriff in die Privatsphäre. Die Frage eines *schutzwürdigen Interesses* stellt sich erst bei der Prüfung der Rechtmäßigkeit und der Abwägung der Interessen des Betroffenen zu denen des Verwenders im Rahmen der Verhältnismäßigkeit und anderer Kriterien. Aus diesen Gründen war in dem Entwurf der Novelle DSG 2010 ursprünglich vorgesehen, das Kriterium des schutzwürdigenden Interesses für den Geheimhaltungsanspruch entfallen zu lassen und § 1 Abs. 1 DSG 2000 folgenden Wortlaut zu geben: „*Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten*." Dem § 1 Abs. 2 DSG 2000 sollte folgender Satz vorangestellt werden: „*Der Anspruch besteht nicht, wenn die Daten zulässigerweise allgemein verfügbar sind*."[73] Die für eine Verfassungsänderung erforderliche Mehrheit von zwei Dritteln konnte im Nationalrat nicht erreicht werden, so dass die an sich sinnvolle Regelung vorläufig nicht zustande gekommen ist.[74]

Jedoch auch in Bezug auf den derzeit in § 1 Satz 2 DSG 2000 geregelten Fall für das Nichtbestehen eines schutzwürdigen Interesses, die *öffentliche Verfügbarkeit* von personenbezogenen Daten, bestehen Bedenken. Jeder Veröffentlichung von Daten liegt auch ein bestimmter Zweck zugrunde, beispielsweise bei Eintragungen im

---

[72] Wiederin, Schutz der Privatsphäre in Handb. d. Grundrechte VII/1, § 190, Rdnr. 134.
[73] Beamtenentwurf DSG-Novelle 2010 20.5.2009, S. 21, ftp://ftp.freenet.at/privacy/gesetze/dsg-novelle-2010-entwurf.pdf, letzte Abfrage 16.01.2012,
[74] Ennökl, Die DSG-Novelle 2010, ÖJZ 2010, S. 293.

Grundbuch der Nachweis bestimmter Rechte. Bei einer anderweitigen Verwendung ohne eine Einwilligung des Betroffenen stellt sich die Frage der Zweckbindung, Art. 6 Abs. 1 Buchst. b DS-RL, und des Auskunftsrechts, Art. 10 DS-RL. Ist beispielsweise die Nutzung von personenbezogenen Daten aus dem Grundbuch oder Firmenbuch für Werbezwecke noch mit dem ursprünglichen Zweck vereinbar?

In jedem Falle erscheint die tatbestandsmäßige Einschränkung des Datenschutzes in § 1 Abs. 1 DSG 2000 auf das Bestehen eines *schutzwürden Interesses* mit Rücksicht auf die Kollision mit Art. 8 Abs. 1 EMRK und eine richtlinienkonforme Auslegung unbeachtlich. Die EMRK hat in Österreich Verfassungsrang und Art. 8 EMRK bildet für den Schutz der Privatsphäre die zentrale verfassungsrechtliche Norm.[75] Damit gilt auch für § 1 Abs. 1 DSG 2000 der Grundsatz, dass jede Verwendung von personenbezogenen Daten zunächst einmal einen Eingriff in Rechte des Betroffenen bedeutet, der nach den Bedingungen des § 1 Abs. 2 DSG 2000 auf seine Rechtmäßigkeit hin zu überprüfen ist. § 1 Abs. 2 DSG 2000 seinerseits verweist bei Eingriffen einer staatlichen Behörde auf Art. 8 Abs. 2 EMRK.

Der grundsätzliche Einschränkung des DSG 2000 liegt darin begründet, dass das Gesetz in § 1 Abs.1 lediglich einen Geheimhaltungsanspruch für personenbezogene Daten gewährt und nicht wie in anderen Rechtsordnungen und nach europäischem Recht ein Recht auf Schutz personenbezogener Daten oder ein informationelles Selbstbestimmungsrecht. Veröffentlichte Daten kann man naturgemäß nicht geheim halten. Das sollte aber nicht dazu führen, dass jedermann diese für eigene, meist geschäftliche Zwecke, nutzen darf.

Der Ordnung halber sei darauf hingewiesen, dass Art. 8 EMRK und § 1 DSG 2000 in ihrem Anwendungsbereich nicht deckungsgleich sind. Die EMRK gewährt Schutzvorschriften in erster Linie gegenüber staatlichen Eingriffen. Die Staaten werden jedoch als verpflichtet angesehen, die Rechtsgüter der Bürger durch geeignete Maßnahmen auch gegen Eingriffe Dritter zu schützen.[76] Der Datenschutz des DSG 2000 erstreckt sich eindeutig auch auf Eingriffe privater Dritter, wie sich aus u.a. aus der Klagemöglichkeit gegen Private gemäß § 32 Abs. 1 DSG 2000 ergibt.

---

[75] Wiederin, „Schutz der Privatsphäre“ in Handbuch der Grundrechte Bd. VII/1, § 190, Rdnr. 6.
[76] Wiederin, aaO., Rdnr. 16.

Man kann also festhalten, dass Eingriffe in das Recht auf Datenschutz hinsichtlich ihrer Zulässigkeit primär auf der Grundlage des Art. 8 Abs. 2 EMRK zu prüfen sind und datenschutzrechtliche nationale Bestimmungen nur insoweit Beachtung finden können, wie sie in ihrem Schutzbereich über Art. 8 EMRK hinausgehen oder der Rechtfertigung eines Eingriffs im Rahmen von Art. 8 Abs. 2 EMRK dienen. Anders als die GRCh bindet Art. 8 EMRK die Mitgliedstaaten nicht nur bei der Durchführung des Unionsrechts, sondern bei jeder hoheitlichen Tätigkeit.[77]

2.10 Löschung und Archivierung

Es entspricht allgemeiner Erfahrung, dass Daten, sind sie einmal in eine Datenbank aufgenommen worden, vielfach nicht mehr gelöscht und damit nicht dauerhaft einer Nutzung entzogen werden. In Kapitel 2.8 ist bereits kurz auf die Rechtsprechung des EGMR eingegangen worden, nach der Daten, die für einen bestimmten Zweck erhoben und verarbeitet worden sind, nach Erledigung des Zweckes wieder zu löschen sind.

Das DSG 2000 sieht in § 1 Abs. 3 Ziffer 2 ein Recht auf Richtigstellung unrichtiger Daten und auf Löschung unzulässigerweise verarbeiteter Daten vor. Dabei gelten Daten, deren Verwendungszweck sich erledigt hat, als unzulässig verwendete Daten, so dass sie zu löschen sind.[78] Der VfGH hat auch in den Fällen eine Verpflichtung zur Löschung angenommen, in denen im Gesetz Speicherfristen vorgesehen sind, vorausgesetzt, dass die Daten für den Zweck, der ihrer Speicherung zugrunde gelegen hat, nicht mehr erforderlich sind.[79] Diese Auslegung entspricht auch den Regelungen in Art. 6 Abs. 1 Buchst. e DS-RL und § 27 Abs. 1 Ziffer 2 DSG 2000. Die letztgenannte Bestimmung enthält eine Ausnahme für den Fall, dass eine Archivierung zulässig und der Zugang zu den Daten besonders geschützt ist. Eine Richtigstellung oder Löschung von Daten ist nach § 27 Abs. 3 DSG 2000 ebenfalls ausgeschlossen, wenn der Dokumentationszweck eine nachträgliche Änderung nicht zulässt. Dies gilt z.B. für Krankengeschichten.[80]

---

[77] Tettinger/Stein, Kölner Gemeinschaftskommentar zur Europäischen Grundrechtecharta, 2006, Art. 8 Rdnr. 17.
[78] Jahnel, Handbuch Datenschutzgesetz 2010, Kapitel 7, Anm. 65.
[79] Urteil des VfGH vom 16.03.2001, Slg. Nr. 16150.
[80] Mayer-Schönberger/Brandl, Datenschutzgesetz, 2. Auflage 2005, § 27 Anm. zu Abs. 3.

Grundsätzliche Fragen der Archivierung von Daten des Bundes sind im Bundesarchivgesetz[81] geregelt. Das Gesetz bestimmt im Wesentlichen die Zuständigkeit für die Archivierung und deren Gegenstände, die Fristen für die Aufbewahrung und den Zugang zum Archivgut. Die für den Datenschutz maßgebliche Bestimmung ist § 5 BArchG. Nach § 5 Abs. 1 BArchG haben die Bundesdienststellen das gesamte Schriftgut, das bei der Erfüllung ihrer Aufgaben angefallen ist und zur Erfüllung ihrer laufenden Aufgaben nicht mehr benötigt wird, auszusondern und dem Österreichischen Staatsarchiv grundsätzlich zusammen mit den für die Benutzung notwendigen Behelfen (z.B. Register) zur Übernahme anzubieten. Gemäß § 5 Abs. 2 BArchG ist Schriftgut, das keine dem § 1 Abs. 3 des Datenschutzgesetzes unterliegenden Daten enthält, spätestens 30 Jahre nach der letzten inhaltlichen Bearbeitung anzubieten, wenn nicht der besondere Inhalt des Schriftgutes oder gesetzliche Regelungen eine längere Aufbewahrung bei der betreffenden Stelle erfordern. Schriftgut, welches Daten enthält, die nach § 1 Abs. 3 DSG 2000 zu löschen sind, weil sie für die zugrunde liegenden Zwecke nicht mehr erforderlich sind, ist vor seiner Löschung oder Vernichtung auf seine Eigenschaft als Archivgut zu überprüfen, § 5 Abs. 3 BArchG. Wird diese Eigenschaft festgestellt, ist das Schriftgut unter Verschluss dem Österreichischen Staatsarchiv zu übergeben, wobei das Datum des Ablaufs der Schutzfrist anzugeben ist. Die Bundesregierung ist ermächtigt, durch Verordnung festzulegen, welchen Arten von Schriftgut die Eigenschaft eines Archivgutes offenkundig nicht zukommt oder zukommen wird, § 5 Abs. 4 BArchG.

In einigen Bundesländern bestehen Landesarchivgesetze, die die Schwerpunkte zum Teil etwas anders setzen. Beim Bund entscheidet das Staatsarchiv bei an sich wegen des Erhebungszweckes zu löschenden Daten, ob aus öffentlichem Interesse eine Archivierung geboten erscheint. Nach § 7 Abs. 1 des Kärntner Landesarchivgesetzes[82] sind dem Landesarchiv derartige Daten nicht anzudienen, soweit sie aus einer automationsunterstützten Verarbeitung stammen.

---

[81] BGBl. I Nr. 162 /1999.
[82] Kärntner Landesarchivgesetz, Gesetz vom 30. Jänner 1997, mit dem das Kärntner Landesarchiv als Anstalt eingerichtet wird (Kärntner Landesarchivgesetz – K-LAG), LGBl. Nr. 40/1997, http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=LrK&Gesetzesnummer=10000219, Abfrage 29.03.2012.

Nach § 3 des Oberösterreichischen Archivgesetzes[83] sind dagegen auch Unterlagen bei Archivwürdigkeit anzubieten und zu übergeben, die personenbezogene Daten enthalten, welche

1. der Amtsverschwiegenheit, dem Datenschutzgesetz 2000 oder sonstigen Geheimhaltungsvorschriften einschließlich solcher über Berufsgeheimnisse unterliegen oder
2. nach einer Rechtsvorschrift gelöscht werden müssten, sofern nicht die Speicherung der Daten unzulässig war.

Nach alledem kann man feststellen, dass eindeutige, für ganz Österreich geltende Bestimmungen für die Archivierung von personenbezogenen Daten fehlen. § 27 Abs. 2 DSG 2000 erlaubt die Unterlassung der Löschung in den Fällen, in denen eine Archivierung rechtlich zulässig und der Zugang zu den Daten besonders geschützt ist. Die Bestimmung ist als Umsetzung des Zweckbindungsprinzips der DS-RL in Art 6 DS-RL anzusehen. Aus Art. 6 Abs.1 Buchst. b DS-RL lässt sich entnehmen, dass eine Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen ist, sofern die Mitgliedstaaten geeignete Garantien vorsehen. An diesen Vorschriften sind die jeweiligen Regelungen zu messen. Zur sonstigen Zulässigkeit der Aufbewahrung von Daten ist zu sagen, dass in einer Reihe von Gesetzen dazu Fristen vorgesehen sind, z. B. § 51 Abs. 3 ÄrzteG= 10 Jahre, § 132 BAO = 7 Jahre, § 212 UBG = 7 Jahre, §13 PHG = 10 Jahre. In diesen Fällen, die in der Literatur zum Teil in Zusammenhang mit einer Archivierung[84] behandelt werden, handelt es an sich nicht um eine Aufbewahrung aus kulturhistorischen Gründen, sondern um gesetzliche Aufbewahrungsfristen im Interesse einer Beweissicherung für zurückliegende Sachverhalte, so dass insoweit eine Vereinbarkeit mit dem Zweck der ursprünglichen Datenerhebung in der Regel gegeben sein dürfte.

---

[83] LGBL. Nr. 83/2003, Landesgesetz über die Sicherung, die Aufbewahrung und die Nutzung von öffentlichem Archivgut sowie die Tätigkeit der damit betrauten Archive (Oö. Archivgesetz), http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=LrOO&Gesetzesnummer=20000258, Abfrage 29.03.2012.

[84] Dohr, Pollirer, Weiss, Knyrim, Kommentar Datenschutzrecht2. Aufl. 2002, 12. Erg.-Lfrg. Dez. 2011, § 27 Anm. 10.

Das ist bei einer Archivierung anders. Die Daten werden für den ursprünglichen Zweck nicht mehr benötigt. Im Einzelfall ist also eine Abwägung zwischen dem öffentlichen Interesse an einer Aufbewahrung im Rahmen der Archivgesetze und dem privaten Interesse an einer Geheimhaltung bzw. Löschung abzuwägen. Das BArchG nimmt für die Beurteilung, was als Archivgut in Betracht kommt, auf das Denkmalschutzgesetz[85] Bezug, § 2 Ziffer 2-4 BArchG. Nach § 1 Abs. 1 des Denkmalschutzgesetzes geht es um Gegenstände, an deren Erhalt ein öffentliches Interesse besteht. Ein solches Interesse besteht nach § 1 Abs. 2 dieses Gesetzes, wenn es sich bei dem Denkmal aus überregionaler oder vorerst auch nur regionaler (lokaler) Sicht um Kulturgut handelt, dessen Verlust eine Beeinträchtigung des österreichichen Kulturgutbestandes in seiner Gesamtsicht hinsichtlich Qualität sowie ausreichender Vielzahl, Vielfalt und Verteilung bedeuten würde. Wesentlich ist auch, ob und in welchem Umfang durch die Erhaltung des Denkmals eine geschichtliche Dokumentation erreicht werden kann. Ähnliche Regelungen finden sich in den Länderarchivgesetzen. Damit ist das Verfahren für die genannte Interessenabwägung festgelegt. Ob diese inhaltlich zutreffend getroffen wird, kann nur im Einzelfall geprüft werden.

Beim Staatsarchiv beträgt die regelmäßige Frist für den Zugang zu Archivgut 30 Jahre seit der letzten Bearbeitung, §§ 8 Abs. 1 und 5 Abs. 2 letzter Satz BArchG. Archivgut mit personenbezogenen Daten wird grundsätzlich erst nach 50 Jahren freigegeben, § 8 Abs. 3 BArchG, ausnahmsweise bereits nach 20 Jahren, wenn

1. die Nutzung die Nutzung für die Durchführung eines bestimmten Forschungsvorhabens einer Person gemäß Abs. 4 erforderlich ist und schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden oder
2. die öffentlichen Interessen an der Durchführung des Forschungsvorhabens gegenüber den schutzwürdigen Interessen der Betroffenen überwiegen.

---

[85] BGBl. Nr. 533/1923 (inzwischen mehrfach geändert), aktuelle Fassung: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009184, letzte Abfrage 29.03.2012.

Damit erscheinen angemessener Zugangsschutz im Sinne von Art 27 Abs. 2 DSG 2000 sowie Garantien im Sinne von Art. 6 Abs.1 DS-RL als gewährleistet.

2.11 Europäisierung des Datenschutzes ?

Im Rahmen einer Entschließung vom 26.03.2009 über eine Empfehlung an den Europäischen Rat zu den Grundfreiheiten hat sich das Europäische Parlament u.a. auch dafür ausgesprochen, das Internet zu einem wichtigen Instrument für die Stärkung der Nutzer zu machen, zu einem Umfeld, das die Entwicklung von basisorientierten Verfahren und einer elektronischen Demokratie ermöglicht und gleichzeitig sicherstellt, dass wichtige Schutzmechanismen geschaffen werden, da sich in diesem Bereich neue Formen der Kontrolle und der Zensur entwickeln können; Freiheit und Schutz der Privatsphäre der Internetnutzer sollte tatsächlich stattfinden und nicht nur vorgespiegelt werden. Es ist nicht auszuschließen, dass sich die Entwicklung zu einer Europäisierung des Datenschutzes mit der zunehmenden länderübergreifenden Zusammenarbeit in der EU weiter verstärkt.[86] In diesem Zusammenhang wird auf das Binnenmarkt-Informationssystem (Internal Market Information System, IMI) und die dazu ergangenen Entscheidung der EU-Kommission über den Schutz personenbezogener Daten bei der Umsetzung des IMI[87] hingewiesen. Darauf wird später bei der Untersuchung des Datenschutzes für E-Government-Anwendungen näher eingegangen. An dieser Stelle soll aber festgehalten werden, dass es angesichts der geschilderten Entwicklung durchaus gerechtfertigt erscheint, von einer Europäisierung des Datenschutzes zu sprechen. Angefangen mit der Unterzeichnung der ERMK im Jahre 1950, der sich daraus entwickelnden Rechtsprechung der EKMR und des EGMR, der Datenschutzkonvention des Europarates aus dem Jahre 1981, der DS-RL der EU aus dem Jahre 1995 und der Charta der Grundrechte der EU, die mit dem Lissabon-Vertrag am 01.12.2009 in Kraft getreten ist und die den Schutz

---

[86] Entschließung des Europäischen Parlaments vom 26. März 2009 mit einem Vorschlag für eine Empfehlung des Europäischen Parlaments an den Rat zur Stärkung der Sicherheit und der Grundfreiheiten im Internet (2008/2160(INI)), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P6-TA-2009-0194, letzer Abruf 20.12.2011.

[87] 2008/49/EG: Entscheidung der Kommission vom 12. Dezember 2007 über den Schutz personenbezogener Daten bei der Umsetzung des Binnenmarktinformationssystems (IMI) (Bekannt gegeben unter Aktenzeichen K(2007) 6306) (Text von Bedeutung für den EWR), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:013:0018:0023:DE:PDF, letzte Abfrage am 20.12.2011.

personenbezogener Daten in Art. 8 ausdrücklich regelt, wird eine Entwicklung zu einem europäischen Datenschutz deutlich. Außerdem ist der Schutz personenbezogener Daten in Art. 16 AEUV ausdrücklich entsprechend geregelt, so dass man von einer doppelten primärrechtlichen Absicherung sprechen kann. Wenn die unter Kapitel 2.6 erwähnten Planungen für eine Datenschutz-Grundverordnung und die Richtlinie über den Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit Wirklichkeit werden, ist die Europäisierung des Datenschutzes nahezu vollendet und den Mitgliedstaaten verbleibt nur ein geringer Gestaltungsrahmen.

Wie bereits erwähnt, gelten die Normen Charta der Grundrechte der EU nur für die Organe und Einrichtungen der EU und für die Mitgliedstaaten bei der Durchführung von Unionsrecht, Art. 51 Abs. 1 GRCh. Diese Einschränkung gilt für die EMRK nicht. Alle Mitgliedstaaten der Union sind auch Unterzeichner der Konvention. Zwar haben die Bestimmungen anders als in Österreich in anderen Vertragsstaaten regelmäßig nicht Verfassungsrang, sondern den Charakter einfach-gesetzlicher Normen. Aber die Vertragsstaaten haben sich verpflichtet, die Urteile in allen Rechtssachen zu befolgen, in denen sie Partei sind, Art. 46 Abs. 1 EMRK[88]. Außerdem wird die Entscheidung jeweils dem Ministerkomitee des Europarates zugeleitet, der die Durchführung überwacht, Art. 46 Abs. 2 EMRK. Die Urteile entfalten zwar nur Bindungswirkung zwischen den Parteien des Verfahrens. Aber die Vertragsstaaten haben allen ihrer Hoheitsgewalt unterstehenden Personen die in der Charta enthaltenen Rechte und Freiheiten zugesichert. Die Urteile des EGMR geben den Konventionsstaaten damit Anlass, ihre Rechtsordnungen zu überprüfen und sich bei etwaigen Änderungen an der Rechtsprechung des EGMR zu orientieren.[89] Die Bedeutung der EMRK hat auch dadurch gewonnen, dass der EuGH sich in seiner Rechtsprechung zum Datenschutz unter Berufung auf Art. 6 Abs. 2 der früheren Fassung des EU-Vertrages ausdrücklich auf Art. 8 der EMRK und die dazu ergangene Rechtsprechung des EGMR bezieht.[90] Art. 6 Abs. EUV lautete: „*Die Union achtet die*

---

[88] In der Fassung des Art. 16 des 14. Protokolls zur EMRK vom 13.05.2004.

[89] Polakiewicz, Durchsetzung von EMRK-Standards mit Hilfe des EU-Rechts?, EuGRZ 2010, S. 11 ff. (13).

[90] EuGH Urteil vom 20.05.2003 in den verb. Rechtssachen - Rechnungshof (C-465/00) gg. Österreichischer Rundfunk und andere und Christa Neukomm (C-138/01) und Joseph Lauermann (C-139/01) gegen Österreichischer Rundfunk. - Ersuchen um Vorabentscheidung: Verfassungsgerichtshof (C-465/00) und Oberster Gerichtshof (C-138/01 und C-139/01) – Österreich Rd.-Nr. 69- 84, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000J0465:DE:HTML, letzter Abruf 20.12.2011,

Grundrechte wie sie in der EMRK gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben." Mit dem Inkrafttreten des Lissabon-Vertrages und der Charta der Grundrechte der EU am 01.12.2009 wird die Verbindung zur EMRK nochmals bekräftigt. In Art. 52 Abs. 3 Satz 1 GRCh wird eine Kohärenz zur EMRK in der Weise hergestellt, dass Konventionsrechte transferiert und deren Anwendung anstelle von charterrechtlichen Grundrechten angeordnet wird. Das bezieht sich nicht nur auf den Wortlaut der Bestimmungen der Konvention, sondern auch auf die dazu ergangene Rechtsprechung des EGMR, wenn das auch nicht ausdrücklich aus der genannten Bestimmung hervorgeht. In den Erläuterungen zu Art. 52 Abs. 3 GRCh findet sich ein entsprechender Bezug.[91]

[91] „ *Die Bedeutung und Tragweite der garantierten Rechte werden nicht nur durch den Wortlaut dieser Vertragswerke, sondern auch durch die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte und durch den Gerichtshof der Europäischen Gemeinschaften bestimmt."* EuGRZ 2000, S. 569.

3. Umsetzung des Datenschutzes bei der Formulierung von Gesetzen

Gemäß der Konkretisierung der Zweckbindung in der DS-RL dürfen personenbezogene Daten nur für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden.

Die Anforderungen an den Gesetzgeber hinsichtlich der Beachtung von datenschutzrechtlichen Gesichtspunkten bei der Formulierung von Gesetzen sind also hoch. Aus diesem Grunde hat sich der Verfassungsdienst im Bundeskanzleramt im Mai 2008 veranlasst gesehen, ein *Rundschreiben zur legistischen Gestaltung von Eingriffen in das Grundrecht auf Datenschutz* zu verfassen.[92] Danach sind an eine gesetzliche Ermächtigung oder Verpflichtung zur Verwendung von Daten im Sinne von § 8 Abs. 1 Ziff. 1 DSG 2000 u.a. folgende Anforderungen zu stellen:[93]

- Anlass und Zweck der Verwendung (§ 4 Z 8 DSG 2000),
- Bezeichnung der von der Verwendung Betroffenen (§ 4 Z 3 DSG 2000),
- Nennung der Kategorien der zu verwendenden Datenarten (§ 4 Z 1 DSG
- 2000),
- Bezeichnung des oder der Auftraggeber (§ 4 Z 4 DSG 2000),
- allfällige Übermittlungsempfänger (§ 4 Z 12 DSG 2000),
- Angaben über technisch-organisatorische Besonderheiten der Verwendung (wie z.B. Speicherung der Daten in einem Register, Verarbeitung der Daten in einem Informationsverbundsystem (§ 4 Z 13 DSG 2000), Möglichkeit von Online-Zugriffen etc.).

Wichtig sei, dass die Zusammenschau der in den Materiengesetzen enthaltenen Regelungen mit den allgemeinen Grundsätzen über die Verwendung von Daten gemäß §§ 4 ff. DSG 2000 eine im Auslegungswege zu ermittelnde hinreichend präzise Regelung darstelle. Dabei sei vorauszusetzen, dass sich die daraus ergebenden Gren-

---

[92] Rundschreiben zur legistischen Gestaltung von Eingriffen in das Grundrecht auf Datenschutz http://www.bka.gv.at/DocView.axd?CobId=29801, letzter Abruf am 20.12.2011.
[93] Rundschreiben aaO., Ziff. 4.1.

zen der Datenerhebung und -verwendung gemäß § 1 Abs. 2 letzter Satz DSG 2000 nach Maßgabe des Grundsatzes der Verhältnismäßigkeit bestimmt werden, so dass der Eingriff nur in der gelindesten zum Ziel führenden Art vorgenommen wird.[94] Bei Verwendung sensibler Daten seien noch strengere Anforderungen an die Erforderlichkeit und Determinierung des Eingriffs zu stellen und das notwendige wichtige Interesse müsse sich aus den Erläuterungen zum Gesetz ergeben.[95]

[94] Rundschreiben aaO. Ziff. 5.1; siehe auch VfGH vom 15.06.2007, G 147/06.
[95] Rundschreiben aaO. Ziff. 5.2.

4. E-Government-Gesetz, EGovG

4.1 Der Begriff E-Government

Laut einer Definition der EU-Kommission meint E-Government den Einsatz der Informations- und Kommunikationstechnologien (IKT) in öffentlichen Verwaltungen in Verbindung mit organisatorischen Änderungen und neuen Fähigkeiten, um öffentliche Dienste und demokratische Prozesse zu verbessern und die Gestaltung und Durchführung staatlicher Politik zu erleichtern.[96] Die österreichische Regierung versteht unter E-Government die Transformation (Veränderung)des öffentlichen Sektors durch Informations- und Kommunikationstechnologien (IKT).[97] Elektronische Serviceangebote von Behörden ermöglichen Nutzerinnen und Nutzern einen bequemen Zugang zur öffentlichen Verwaltung. Für Behörden, die Informations- und Kommunikationstechnologien (IuK) einsetzen, um elektronische Services anbieten zu können, ergeben sich intern große organisatorische Veränderungen und Chancen. Prozesse müssen teilweise neu modelliert und Arbeitsabläufe an die neuen Anforderungen angepasst werden. Die Arbeit wird behördenintern zunehmend automationsunterstützt abgewickelt. Mitarbeiterinnen und Mitarbeiter benötigen daher die notwendigen Kenntnisse und Fertigkeiten, um mit den eingesetzten Technologien umgehen zu können. E-Government setzt sich aus all diesen Elementen zusammen.[98]

In der wissenschaftlichen Literatur wird zwischen E-Government im engeren und im weiteren Sinne differenziert,[99] und es werden vier Entwicklungsstufen unterschie-

---

[96] http://www.bildung.at/content/egov/e-gov_uberblick_20070918.pdf , S. 16 , letzte Abfrage 28.10.2009.
[97] http://www.bildung.at/content/egov/e-gov_uberblick_20070918.pdf, S. 18, letzte Abfrage 28.10.2009.
[98] http://www.ag.bka.gv.at/index.php/E-Gov:Abgrenzung, letzte Abfrage 20.12.2011
[99] http://www.verigo.net/verigo/index.php/Verigo/E-Government, letzte Abfrage 20.12.2011: „E-Government“ (auch eGovernment) ist die Kurzform für Electronic Government und bedeutet übersetzt so viel wie „elektronische Verwaltung“. Zu Beginn ihrer Amtszeit 1993 hat die Clinton/Gore-Regierung in den USA die zugrunde liegende „Vision“ formuliert, erstmals praktisch verwendet hat ihn das Unternehmen IBM im Jahre 1995. Der durchaus schillernde Anglizismus wird – trotz zahlreicher Definitionsversuche (hierzu sogleich) – in der Praxis willkürlich im Kontext der Nutzung von Informations- und Kommunikationstechnik (IuK) innerhalb der öffentlichen Verwaltung („G2G“: government to government) als auch deren Gebrauch im Verhältnis zu Wirtschaft („G2B“: government to business) und Bürgern („G2C“:government to citizens) verwendet. **E - Government im weiteren und engeren Sinne**
Im weiteren Sinne gilt der Begriff E-Government inzwischen als Oberbegriff für die Teilbereiche E-Democracy, E-Administration, E-Election (respektive E-Voting), E-Justice, etc.. Parallel dazu wird E-Government aber auch enger gefasst und auf seinen Kernbereich - die Verwaltung - reduziert: So

den.[100] In der ersten Stufe geht es darum, dem Bürger einen einheitlichen Ansprechpartner für einen Vorgang zu bieten und Gänge zu verschiedenen Behörden zur Erledigung einer Sache zu vermeiden. In der zweiten Stufe erfolgt die Kommunikation zwischen Bürger und Verwaltung online. Die dritte Stufe ist dadurch gekennzeichnet, dass die Bürger nicht mehr mit Einzelinformationen belastet werden und sie lediglich die relevante Leistung kennen müssen. Die vierte und höchste Stufe bedeutet proaktives staatliches Verhalten. Der Staat wird unabhängig von Anträgen aufgrund vorhandener personenbezogener Daten tätig und erbringt gewissermaßen automatisch entsprechende Leistungen.

4.2 Die Entwicklung des E-Government

E-Government in seiner heutigen Form ist das Ergebnis eines Evolutionsprozesses. Am Beginn, in den 1960er Jahren, erfolgte die Massenverarbeitung von Daten auf Großrechnern. Mit der Ausweitung der Anwendungen und Datenbanken sowie der Eröffnung zusätzlicher Rechenzentren für die Verwaltung ist das Entstehen einer neuen Disziplin, der Verwaltungsinformatik, verbunden, die die Klärung von organisatorischen Fragen bei der Nutzung der IT durch die Verwaltung zum Gegenstand hat. Das Aufkommen der PC in den 1980er Jahren brachte die unmittelbare Nutzung der

---

versteht man unter E-Government im engeren Sinne die IT-gestützte öffentlich-rechtliche Verwaltungstätigkeit im Sinne des § 1 Abs. 1 VwVfG, also den Bereich der E-Administration.

Speyerer Definition

Häufig wird im Zusammenhang mit dem Begriff E-Government die sog. "Speyerer Definition" genannt, nach welcher unter E-Government die "Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien" zu verstehen ist.

Inhalt des E-Government im engeren Sinne

Der Inhalt des E-Governments im engeren Sinne lässt sich mit den Schlagworten „Information, Kommunikation und Transaktion" im Verhältnis Staat-Bürger umschreiben. Die Bereitstellung von Informationen und Nachrichten, deren Übermittlung sowie die Abwicklung von Verwaltungsvorgängen eröffnet dabei einen weiten juristischen Problembereich, der nicht nur unmittelbar technische Fragen wie z.B. Fragen nach der elektronischen Signatur, die die Informationssicherheit und Verlässlichkeit des neuen Mediums sicherstellen sollen, umfasst. Vielmehr muss sich die Ausarbeitung der rechtlichen Rahmenbedingungen an den Prinzipien des „good governance" , des verantwortungsvollen Regierens, orientieren und die Bürger als Nutzer der IT-gestützten Verwaltungsangebote in den Mittelpunkt stellen. So sind Fragen nach dem notwendigen Maß an „Usability" oder nach der Verfügbarkeit der technischen Mittel bzw. eines „Zwanges zur Nutzung" praktische Fragen des E-Government. Aus Sicht der Bürger muss das Ziel sein, das Verwaltungsangebot an den Lebenslagen der Bürger zu orientieren und ein One-Stop-Government, in dem die Dienstleistungen der Verwaltung einheitlich erfolgen, zu etablieren.

[100] Winter,Makolm,Weiß, *„Die Rückwirkung von Werkzeugeinsatz auf die Kultur: Wie Informationstechnik unsere Wissens- und Rechtskultur verändert"* in Traunmüller/Wimmers, Informatik in Recht und Verwaltung: Gestern-Heute-Morgen, Ehrenband für Prof. Fiedler zum 80. Geburtstag, 2009, S. 162 ff. (164).

IT am Arbeitsplatz und die Vernetzung von Abteilungen mit dem Ziel einer Optimierung der Verwaltungsabläufe mit sich. Die Entwicklung des Internet und die zunehmende Verbreitung der Technologie auch in der Bürgerschaft ermöglichte seit der Jahrtausendwende eine unmittelbare rechnergestützte Kommunikation zwischen Bürger und Verwaltung, den Übergang zum E-Government in seiner heutigen und ständig weiterentwickelten Ausprägung.[101]

Zu Beginn des Jahrhunderts erstarkte in der Europäischen Gemeinschaft das Bewusstsein, dass der Informationstechnologie eine Schlüsselrolle für die wirtschaftliche und soziale Entwicklung in der Gemeinschaft zukommt. Im März 2000 verabschiedeten die Staats- und Regierungschefs die so genannte Lissabon-Strategie, mit der die Union zum wettbewerbsfähigsten und dynamischsten wissensbasierten Wirtschaftsraum in der Welt gemacht werden sollte - einem Wirtschaftsraum, der fähig ist, ein dauerhaftes Wirtschaftswachstum mit mehr und besseren Arbeitsplätzen und einem größeren sozialen Zusammenhalt zu erzielen.[102] U.a. sollten die Mitgliedstaaten einen allgemeinen elektronischen Zugang zu den wichtigsten grundlegenden öffentlichen Diensten bis 2003 sicherstellen. Nachdem die Halbzeit-Bilanz eher ernüchternd ausfiel, verabschiedete die EU-Kommission im Jahr 2006 den i2010 E-Government Action Plan, mit dem u.a. das Ziel verfolgt wird, bis 2010 zu verhindern, dass auf nationaler Ebenen neue Barrieren durch Fragmentierung und Mängel in der Interoperabilität zwischen Mitgliedstaaten entstehen und die Zusammenarbeit zwischen den Mitgliedstaaten gefördert wird.[103]

In Österreich ist schon in den 1990-er Jahren mit dem Einsatz der IuK in der öffentlichen Verwaltung begonnen worden und die Initiative der EU hat die Entwicklung im Lande weiter beschleunigt.[104] Zur Umsetzung der Gemeinschaftspläne wurde ein Aktionsplan eAustria in eEurope beschlossen. In allen Bundesministerien wurden

---

[101] Eine detaillierte Darstellung der historischen Entwicklung, von der hier nur die Schwerpunkte genannt werden, findet sich bei Traunmüller/Wimmers, „*Von der Verwaltungsinformation zum E-Government*“ in Traunmüller/Wimmers, Informatik in Recht und Verwaltung: Gestern-Heute-Morgen, Ehrenband für Prof. Fiedler zum 80. Geburtstag, 2009, S. 7 bis 19.

[102] http://www.europarl.europa.eu/summits/lis1_de.htm, letzte Abfrage 20.12.2011.

[103] http://ec.europa.eu/information_society/eeurope/i2010/archive/eeurope/index_en.htm, letze Abfrage 20.12.2011.

[104] Zu der Entwicklung des E-Government in Österreich im Einzelnen siehe Thiele, Aktuelle Entwicklungen des E-Government in Österreich, http://www.rechtsprobleme.at/doks/thiele-egovernment.pdf, letzte Abfrage 20.12.2011.

Chief Information Officer (CIO) bestellt, die gemeinsam das im Bundeskanzleramt eingerichtete ITK-Board bilden. Im Jahre 2003 hat die Bundesregierung eine E-Government-Strategie für Österreich beschlossen, in deren Folge im Jahre 2004 das E-Government-Gesetz (EGovG, zuletzt geändert im Jahr 2008)[105] erlassen worden ist. Österreich hat mittlerweile einen Spitzenplatz bei E-Government-Diensten innerhalb der EU erreicht. In der Zeit von 2002 bis 2006 konnte sich Österreich nach einem von der IT-Beratung Capgemini im Auftrage der Europäischen Kommission durchgeführten Bewertungsverfahren von dem 11. auf den 1. Platz unter den Mitgliedstaaten verbessern[106] und diesen bisher auch halten[107]. Mittlerweile stehen eine Reihe von wesentlichen Werkzeugen zur Verfügung, wie z.B. Bürgerkarte, Elektronischer Akt, Elektronische Zahlung, Elektronische Signatur, Elektronische Zustellung, Zeitstempeldienst.[108]

Die Strategie wird ständig fortgeschrieben. Aktuell (Stand Dezember 2011) werden folgende Ziele[109] verfolgt:

- Anpassung der Kommunikationswege an die neuen elektronischen Medien sowie Verbesserung und/oder neue Modellierung der Geschäftsprozesse, um die Bürger in die Lage zu versetzen, in Verfahren mit der öffentlichen Verwaltung ohne Kenntnis von Zuständigkeiten und technisches Spezialwissen kommunizieren zu können.
- Verstärkung der Zusammenarbeit zwischen Bund, Ländern, Städten und Gemeinden, um vorhandene Ressourcen noch effizienter einsetzen zu können. Optimierung der Kommunikation und der Zusammenarbeit, damit Verfahren schneller bearbeitet und erledigt werden können. Dazu ist es erforderlich, die verschiedenen Systeme technisch aufeinander abzustimmen und gemeinsame Standards zu verwenden.

Dabei strebt das Bundeskanzleramt, in dem die Aktivitäten koordiniert werden, einen modularen Aufbau der Systeme an. Teil I der E-Government-Strategie betrifft Online-

---

[105] BGBl. I Nr. 10/2004, BGBl. I Nr. 7/2008
[106] http://www.news.at/articles/0626/542/144462/e-government-oesterreich-platz-1-spitzenposition-ranking, letzte Abfrage 20.12.2011.
[107] FAZ vom 24.11.2000, Seite 17.
[108] http://www.bka.gv.at/site/5240/default.aspx, letzter Abruf am 20.12.2011
[109] E-Government Strategie des Bundes: http://www.bka.gv.at/site/5237/default.aspx, letzte Abfrage 22.12.2011.

Verfahren, Teil II konzentriert sich auf Methoden und Verfahren innerhalb der Verwaltung und schließlich die Entwicklung von Online Applikationen, die den Verwaltungen vom Bundeskanzleramt zur Verfügung gestellt werden.

Über den aktuellen Stand der Entwicklung des E-Government in Österreich im Vergleich zu anderen Ländern in der EU gibt ein jährlicher Bericht der EU-Kommission Auskunft. Der Nutzungsgrad von E-Government-Diensten in Österreich liegt über dem EU-Durchschnitt.[110]

4.3 Die gesetzlichen Grundlagen des E-Government

Neben dem EGovG, zuletzt geändert im Jahre 2008 (EGovG-Novelle 2007)[111], sind für die Umstellung des Verkehrs mit den Behörden auf elektronische Kommunikation eine Reihe weiterer gesetzlicher Regelungen erforderlich. Zu nennen ist dabei zunächst das **Signaturgesetz**[112], das -in Übereinstimmung mit der Signaturrichtlinie- die Rahmenbedingungen der elektronischen Signaturen regelt.

Das **Allgemeine Verwaltungsverfahrensgesetz**[113] hat die Grundlagen des Verwaltungsverfahrens zum Gegenstand. Für den Bereich des E-Government ist § 13 AVG einschlägig, der die Möglichkeiten der Kontaktaufnahme zwischen Bürger und Behörde regelt.

Das **Zustellgesetz** (ZustG)[114] beschreibt die Zustellung der von Verwaltungsbehörden in Vollziehung der Gesetze zu übermittelnden Dokumente (z.B. Bescheide). Eine nachweisliche elektronische Zustellung (§ 35 ZustG) wird über einen elektronischen Zustelldienst bewirkt.

---

[110] EU-Kommission, Information Society, Digital Agenda Scoreboard 2011, Austria: **eGovernment:** The full range of basic public services for citizens and enterprises are now available online. Take-up of eGovernment services by businesses, at 75%, is relatively good. However, this displays a slight fall compared to 2009. Take-up by citizens is significantly lower, though at 51%, it is higher than the EU average (41%), http://ec.europa.eu/information_society/digital-agenda/scoreboard/countries/at/index_en.htm, letzte Abfrage 20.12.2011.
[111] BGBl. I Nr. 10/2004 zuletzt geändert durch BGBl. I Nr. 7/2008.
[112] BGBl. I Nr. 190/1999 zuletzt geändert 2008, BGBl. I Nr. 59/2008 (VFB).
[113] BGBl.Nr. 51/1991, zuletzt geändert in 2009, BGBl. I Nr. 20/2009.
[114] BGBl. Nr. 200/1982 zuletzt geändert 2008, BGBl. I Nr. 5/2008.

Die **Stammzahlenregisterverordnung**[115] bestimmt die Tätigkeiten der Stammzahlenregisterbehörde, die für die Umsetzung des Bürgerkartenkonzepts und ihr Zusammenwirken mit ihren Dienstleistern notwendig sind. Zur Errechnung des bereichsspezifischen Personenkennzeichens muss jede Datenanwendung eines Auftraggebers des öffentlichen Bereichs einem staatlichen Tätigkeitsbereich zugeordnet werden.

Die **E-Government Bereichsabgrenzungsverordnung**[116] enthält die Bezeichnung jedes Tätigkeitsbereichs samt Bereichskennung.

Die **Ergänzungsregisterverordnung**[117] ist neben der Stammzahlen-Registerverordnung und der E-Government-Bereichsabgrenzungsverordnung ein wichtiger Bestandteil der Durchführungsvorschriften zum E-Government-Gesetz. Das Ergänzungsregister wird getrennt in zwei Teilen geführt. Im Teil für natürliche Personen können sich alle natürlichen Personen eintragen lassen, die nicht im Zentralen Melderegister eingetragen sind. Im Teil für sonstige Betroffene können sich die nichtnatürlichen Personen eintragen lassen, die nicht im Firmenbuch oder im Vereinsregister eingetragen sein müssen.

Die elektronische Zustellung ist im Zustellgesetz geregelt, in dem vor allem die Aufgaben und Zulassung elektronischer Zustelldienste, die näheren Umstände der Leistungserbringung und die Aufsicht über die elektronischen Zustelldienste festlegt sind. Die **Zustelldiensteverordnung**[118] bestimmt im Einzelnen die Zulassungskriterien, nach denen die notwendige technische und organisatorische Leistungsfähigkeit sowie die rechtliche, insbesondere datenschutzrechtliche Verlässlichkeit der elektronischen Zustelldienste im Hinblick auf die ordnungsgemäße Erfüllung der von ihnen zu erbringenden Leistungen beurteilt werden kann.

Die **Zustellformularverordnung**[119] legt unter anderem die Verständigungsformulare für die erste und zweite Verständigung fest, die elektronisch an den Empfänger gesendet werden, sowie für die dritte Verständigung, die in Papierform ergeht, sofern

---

[115] BGBl. II Nr. 57/2005, Änderung 2009, BGBl. II Nr. 330/2009.
[116] BGBl. II Nr. 289/2004.
[117] BGBl. II Nr. 241/2005.
[118] BGBl. II Nr. 233/2005 idF: BGBl. II Nr. 354/2008.
[119] BGBl. Nr. 600/1982 idF. BGBl. II Nr. 152/2008.

der Empfänger eine Abgabestelle (z.B. die Wohnadresse) beim Zustelldienst bekannt gegeben hat.

4.4 Das Konzept des Datenschutzes im E-Government, Identifizierung, Bürgerkarte

Grundsätzlich dürfen Behörden Bürger im elektronischen Verkehr nur identifizieren, wenn dies im überwiegenden öffentlichen Interesse geboten ist, insbesondere wenn dies eine wesentliche Voraussetzung für die Erfüllung der gesetzlich übertragenen Aufgaben ist, § 3 Abs. 2 EgovG. Ein Zugriff auf personenbezogene Daten darf auch nur erfolgen, wenn die Authenzität des Ersuchens in elektronisch nachprüfbarer Form nachgewiesen wird, § 3 Abs. 1 EGovG. Die Identität einer Person wird regelmäßig mit der Bürgerkarte und der in ihr verkörperten Personenbindung nachgewiesen, § 4 Abs. 1 EGovG. Der in der Bürgerkarte bezeichneten Person wird durch die Stammzahlenregisterbehörde, das ist die DSK (§ 7 Abs. 1 EGovG), in elektronisch signierter Form bestätigt, dass der in der Bürgerkarte bezeichneten natürlichen Person eine bestimmte Stammzahl zur eindeutigen Identifikation zugewiesen ist, § 4 Abs. 2 EGovG. Gemäß § 6 Abs. 2 EGovG werden die Stammzahlen für natürliche im Melderegister eingetragene Personen durch eine mit starker Verschlüsselung gesicherte Ableitung aus ihrer ZMZ-Zahl, § 16 Abs. 1 Meldegesetz 1991 [120] gebildet. Bei allen anderen Personen wird ihre Ordnungsnummer im Ergänzungsregister für die Ableitung genutzt. Die DSK als Stammzahlenregisterbehörde kann für diese Aufgabe andere Dienstleister einsetzen. In der Regel wird die Berechnung der Stammzahl vom zentralen Melderegister durchgeführt, das dem BMI untersteht. Bei anderen Betroffenen werden die Berechnungen vom BMF vorgenommen.[121]

Gemäß § 8 EGovG darf zur eindeutigen Identifizierung einer natürlichen Person in den Datenanwendungen öffentlicher Auftraggeber nur ein bereichsspezifisches Personenkennzeichen, bPK, verwendet werden. Damit soll aus datenschutzrechtlichen Gründen vermieden werden, dass im österreichischen E-Government-Konzept einheitliche und flächendeckend geltende Personenkennzeichen entstehen.[122] Das bPK wird in der bürgerkartentauglichen DV-Umgebung der jeweiligen Behörde automa-

---

[120] BGBl. 1992 Nr. 9
[121] EGovG, Texte und Materialien, Pro Libris Verlagsgesellschaft (Hrsg.) Linz 2009, Seite 25
[122] Siehe vorstehende Fußnote, Seite 27

tisch – unterschiedlich für die einzelnen Bereiche staatlicher Tätigkeit – durch Ableitung aus der Stammzahl gebildet. Dabei handelt es sich um kryptographische Einwegableitungen, also nicht umkehrbare Ableitungen, § 10 Abs. 1 EGovG. Damit können zwar mittels der Stammzahl die bPKs aller Bereiche erzeugt werden, aber nicht die Stammzahl und auch nicht die Ableitung für einen anderen Bereich.[123] Die Begründung des Gesetzgebers, warum nicht von vornherein unterschiedliche Personenkennzeichen verwendet werden, besteht darin, dass es in ganz bestimmten gesetzlich geregelten Situationen möglich bleiben müsse, Daten aus verschiedenen Bereichen zusammenzuführen, z.B. bei Amtshilfe im Rahmen insbesondere datenschutzrechtlicher Voraussetzungen. Zwar wäre dies wie bisher auch mit Hilfe des Namens möglich. Die Möglichkeit der eindeutigen Identifikation in den einzelnen Bereichen mit der bPK sollte jedoch im Interesse des Datenschutzes genutzt werden, weil damit das Zusammenführen von Daten unterschiedlicher Personen mit gleichem Namen vermieden werde.[124]

4.5 Zweckbindung im Datenschutz und Amtshilfe

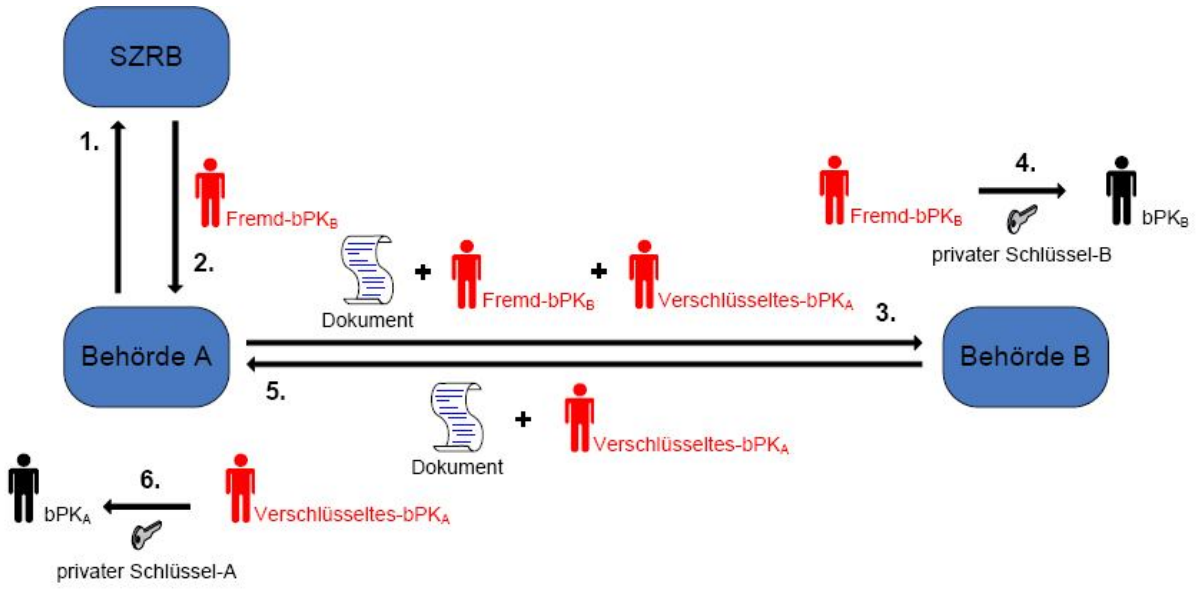
Entsprechend der Vorgabe in Art. 6 Abs. 1 Ziffer 2 DS-RL bestimmt § 6 Abs. 1 Ziffer 2 DSG 2000, dass Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden dürfen. Die Übermittlung von personenbezogenen Daten ist nach § 7 Abs. 2 DSG 2000 nur zulässig, wenn die Daten aus einer zulässigen Datenanwendung stammen, der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder seine rechtliche Befugnis im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und durch den Zweck und den Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden. Damit sind datenschutzrechtliche Rahmenbedingungen für Auskünfte und Amtshilfe der Behörden untereinander festgelegt. Nach Art. 20 Abs. 3 B-VG sind alle Behörden grundsätzlich auch zur Amtsverschwiegenheit verpflichtet. Soweit diese gesetzliche Verschwiegenheitspflicht nicht entgegensteht, sind aber alle Behörden des Bundes und der Länder und Organe anderer Körperschaften des öffentlichen Rechts nach Art. 22 B-VG im Rahmen ihres gesetzlichen Wirkungskreises zur wechselseitigen

---

[123] Siehe vorstehende Fußnote, Seite 27
[124] EGovG, Texte und Materialien, Pro Libris Verlagsgesellschaft (Hrsg.) Linz 2009, Seite 27

Hilfeleistung verpflichtet. Auch im DSG 2000 ist in § 8 Abs. 3 Ziffer 2 und in § 9 Ziffer 4 die Amtshilfe ausdrücklich vorgesehen und festgelegt, dass insoweit schutzwürdige Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.
Das bedeutet jedoch nicht, dass Behörden einander uneingeschränkt zur Auskunft und Amtshilfe verpflichtet sind. Die weiteren Bestimmungen des DSG 2000, insbesondere § 7 Abs. 2 , sind zu beachten.

Rein technisch läuft die Amtshilfe im Rahmen des EGovG so ab, dass die ersuchende Behörde von der Stammzahlenregisterbehörde ein bPK für den Bereich anfordert, an den das Ersuchen gestellt werden soll (ein so genanntes Fremd-bPK). Gemäß § 13 Abs. 2 EGovG wird dabei das bPK so verschlüsselt, dass nur die die Behörde, in deren Bereich das bPK zulässigerweise verarbeitet werden darf, die Entschlüsselung vornehmen kann.



Quelle: EGIZ E-Government Informationszentrum

1. Behörde A fordert von der Stammzahlenregisterbehörde ein Fremd-bPk für eine Anfrage an Behörde B an,
2. Behörde B erhält Fremd-bPk von der Stammzahlenregisterbehörde,
3. Behörde A sendet Dokument mit ihrem verschlüsselten bPk und Fremd-bPk an Behörde B,

4. Behörde entschlüsselt mit ihrem privaten Schlüssel Fremd-bPk und kann dann das Dokument einer Person zuordnen und bearbeitet die Anfrage der Behörde A,
5. Behörde B sendet das bearbeitete Dokument mit dem verschlüsselten Fremd-bPk wieder an Behörde A,
6. Behörde kann ihr verschlüsseltes bPk mit ihrem privaten Schlüssel entschlüsseln und so das Dokument der betroffenen Person zuordnen.

Mit dieser technischen Abwicklung ist zunächst nur gewährleistet, dass die ausgetauschten Daten die richtige Person betreffen. Über den zulässigen Inhalt der Übermittlung und Amtshilfe ist damit noch nichts gesagt. Ein uneingeschränkte Übermittlung würde die Zweckbindung der ursprünglichen Datenverwendung unterlaufen und u. U. im Widerspruch zu § 7 Abs. 2 DSG 2000 stehen.

In diesem Zusammenhang ist eine Entscheidung der DSK aus dem Jahre 2006 von Interesse[125]. Ein Bürger sollte im Rahmen eines waffenrechtlichen Verfahrens auf seine Zulässigkeit hin überprüft werden. Die zuständige Behörde richtete eine Anfrage an die Wohnsitzgemeinde, welche dieser daraufhin eine Reihe von Unterlagen übermittelte, die auch bei großzügiger Betrachtung kaum etwas mit dem Gegenstand des Verfahrens zu tun hatten.[126] In ihrer Entscheidung über die Zulässigkeit der Übermittlung vertrat die DSK die Auffassung, aus § 55 Abs. 1 AVG, der auch eine einfach-gesetzliche Präzisierung des Art. 22 B-VG darstelle, ergebe sich, dass eine Behörde Beweisaufnahmen auch durch ersuchte oder beauftragte Behörden vornehmen lassen kann. Umso mehr seien bloße Ersuchen um Akten- oder Urkundenübersendungen im Verwaltungsverfahren möglich. Nach der Rechtsprechung des Verwaltungsgerichtshofes zu § 46 AVG könne die Behörde ohne weiteres das Beweis- und Erhebungsmaterial anderer Verfahren und anderer Behörden zu Beweiszwecken

---

[125] http://www.ris.bka.gv.at/Dokumente/Dsk/DSKTE_20061129_K121229_0006-DSK_2006_00/DSKTE_20061129_K121229_0006-DSK_2006_00.pdf, letzte Abfrage 29.12.2011

126 Folgende Schriftstücke wurden übermittelt: - vom 27. Juni 2005: Anzeige gegen V. B*** wegen behaupteten Verstoßes gegen § 91 StVO und den „Bebauungsplan und Bauplatzerklärung“ sowie „Hinweis und Säumnisbeschwerde“ wegen „Überschreitung“ des Abstandes der Pflanzen von der 5m-Grundstücksgrenze.
- vom 8. September 2005: Ersuchen an die Gemeinde, die Bestätigung und Übergabe eines (beiliegenden Schreibens) an den Beschwerdeführer vorzunehmen.
- vom 23. Oktober 2005: Rechnung für Abwehrmaßnahmen gegen die „verleumderische Anzeige der Gemeindebediensteten ...“ bzw. des Beschwerdegegners wg. „nicht erfolgte(r) Sachbeschädigung“ bzw. „nicht erfolgte(r) Störung“ sowie Mahnung offener Beträge.
- und vom 26. Dezember 2005: Ersuchen an die Gemeindevertretung, die Kanalgebühren des Beschwerdeführers „im Sinne des Gleichheitsrechtes“ auszusetzen

heranziehen. Solche Ersuchen müssten im Hinblick auf das Ziel des Verwaltungs-(beweis)verfahren – Feststellung des für einen Bescheid maßgeblichen Sachverhaltes von Amts wegen – siehe §§ 37 und 39 Abs. 2 AVG – auch weit gefasst sein können. Würde man an ein Amtshilfeersuchen strengere Anforderungen stellen, würde diese Aufgabe des Verwaltungsverfahrens vereitelt. Eine Begründung, die die Rechtsgrundlage oder zumindest das Ziel des konkret geführten Verwaltungsverfahrens und darauf bezogen das Beweisthema benenne, müsse daher als ausreichend angesehen werden.

Die DSK habe wiederholt ausgesprochen, dass sie nicht befugt sei, die Zulässigkeit von (Beweismittel-)Erhebungen im Verwaltungsverfahren im Detail zu prüfen. Dafür bestehe ein in den Bestimmungen über das Ermittlungsverfahren(§§ 37 ff. AVG) zum Ausdruck kommendes überwiegendes berechtigtes Interesse. Als Abgrenzungskriterium werde jedoch die Denkmöglichkeit als Ausdruck des in § 1 Abs. 2 DSG 2000 normierten Verhältnismäßigkeitsgrundsatzes herangezogen: Wenn es denkmöglich sei, dass die von einer Behörde in einer Sache ermittelten Daten nach Art und Inhalt für die Feststellung des relevanten Sachverhaltes geeignet seien, sei die Zulässigkeit der Ermittlung aus datenschutzrechtlicher Sicht gegeben.

In der praktischen Auswirkung bedeutet diese Auffassung, dass eine Behörde personenbezogene Daten, die für einen bestimmten Zweck bei ihr gespeichert worden sind, an eine andere weitergeben darf, wenn es denkmöglich erscheint, dass diese Daten für die Erledigung der Aufgabe der anfragenden Behörde geeignet erscheinen. Die ersuchte Behörde dürfte also nicht näher prüfen, ob die Verwendung der Daten bei der anfragenden Behörde mit den ursprünglichen Erhebungszwecken vereinbar ist.

Dabei stellt sich die Frage, ob dieses Vorgehen mit den Anforderungen des § 7 Abs. 2 Ziffer 1 bis 3 DSG 2000 übereinstimmt, der der ersuchten Behörde Prüfpflichten auferlegt. Nach § 6 Abs. 1 Ziffer 2 DSG 2000 darf die Weiterverwendung t mit den ursprünglichen Zwecken nicht unvereinbar sein. Art. 6 Abs. 1 Buchst. B DS-RL legt ebenso fest, dass die Weiterverarbeitung nur in einer mit der ursprünglichen Zweckbestimmung zu vereinbarenden Art und Weise erfolgen darf.

4.5.1 Der Begriff der Zweckbindung

Das Thema Zweckbindung wird hier so breit behandelt, weil ohne Beachtung dieses Grundsatzes für Betroffene nicht mehr feststellbar ist, wer, welche Daten über ihn gespeichert hat, und damit das Grundrecht auf Datenschutz ausgehöhlt wird.

Zweckbindung kann so verstanden werden, dass personenbezogene Daten ausschließlich zu dem Zweck verwendet werden dürfen, zu dem sie erhoben worden sind und eine anderweitige Verwendung damit ausgeschlossen wird. Diesen engen Begriff der Zweckbindung vertritt das deutsche BVerfG u. a. in seinem bekannten Volkszählungsurteil[127] aus dem Jahre 1983. Der Zwang zur Abgabe personenbezogener Daten setzt danach voraus, dass der Verwendungszweck im Voraus bereichsspezifisch präzise festgelegt wird. Eine davon abweichende Verwendung für eine andere Behörde sei grundsätzlich nicht zulässig.[128] Diese strenge Auffassung vom Zweckbindungsprinzip ist für den Datenschutz optimal und sie ist auch in das deutsche BDSG in § 14 Abs. 1 übernommen worden. Das enge Verständnis der Zweckbindung wird aber in der Literatur im Interesse einer funktionierenden und effizienten Verwaltung kritisiert. Die vom BVerfG vorgegebene Definition der informationellen Selbstbestimmung werde zunehmend nicht mehr als dem Wandel zu einer Informationsgesellschaft angemessen empfunden. Es gelte daher die Reichweite und den Inhalt der informationellen Selbstbestimmung in einer Weise zu überdenken, die den Anforderungen auch in Zeiten vernetzter Verwaltungsorganisationen gerecht werde.[129] Eine ausschließlich bereichsorientierte Betrachtung der Zweckbindung sei praktisch kaum möglich. Unter Berücksichtigung einer zunehmenden Medienkompetenz der Bevölkerung wird für eine subjektive Bestimmung der Zwecksetzung plädiert. In dem Anstoßen einer Datenverarbeitung durch den Bürger liege eine individuelle Konkretisierung des Zwe-

---

[127] BVerfGE 65, 1 ff

[128] BVerfGE 65, S. 46, *„Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren. Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen. Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein - amtshilfefester - Schutz gegen Zweckentfremdung durch Weitergabeverbote und Verwertungsverbote erforderlich. Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungspflichten, Auskunftspflichten und Löschungspflichten wesentlich.“*

[129] Forgó, Krügel, Rapp, Zwecksetzung und informationelle Gewaltenteilung, Nomos Verlagsgesellschaft Baden-Baden,1. Aufl. 2006, Seite 21.

ckes. Diese Auffassung von der Zwecksetzung durch den Bürger entspreche weit mehr dem Anspruch auf informationelle Selbstbestimmung.[130]

Die Rechtslage in Österreich entspricht jedoch nicht der in Deutschland. Wie sich aus der zitierten Rechtsprechung des deutschen BVerfG ergibt, ist in Deutschland das informationelle Selbstbestimmungsrecht auf der Grundlage von einzelnen Bestimmungen des deutschen Grundgesetzes als subjektives Recht ausgestaltet. In Österreich steht unter Berücksichtigung von Art. 8 EMRK, Art. 1 DS-RL und §1 DSG 2000 mehr der Schutz der Privatsphäre nach objektiven Kriterien im Vordergrund. Art. 6 Abs. 1 Buchst. b DS-RL und § 6 Abs. 1 Ziffer 2 DSG 2000 lassen eine Verwendung von personenbezogenen Daten zu anderen Zwecken grundsätzlich zu, wenn diese mit dem Zweck der ursprünglichen Erhebung vereinbar sind.

„Vereinbarkeit“ ist ein unbestimmter Begriff, der im Interesse einer sicheren Rechtsanwendung näher erläutert werden soll. Dabei ist zu beachten, dass nach der Definition in § 4 Ziffer 12 DSG 2000 in einer Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers bereits eine Datenübermittlung zu sehen ist, nicht erst in der Weitergabe von Daten an einen anderen Auftraggeber. Die Übermittlung ist an die Voraussetzungen des § 7 Abs. 2 DSG 2000 gebunden.[131] Eine anderweitige Nutzung von Daten und eine Weitergabe von Daten an einen anderen Auftraggeber ist also grundsätzlich nur zulässig, wenn die Daten aus einer zulässigen Verarbeitung stammen, der Empfänger aufgrund entsprechender gesetzlicher Bestimmungen berechtigt ist, diese zu verwenden, seine Berechtigung dem Übermittelnden glaubhaft gemacht hat und schutzwürdige Geheimhaltungsinteressen des Betroffenen nicht verletzt werden. Unabhängig davon ist nach § 6 Abs. 1 Ziffer 2 DSG 2000 auch zu prüfen, ob die neue Verwendung zu anderen Zwecken erhobener Daten mit dem ursprünglichen Erhebungszweck unvereinbar ist. Das ergibt sich auch aus § 7 Abs. 3 DSG 2000, der festlegt, dass bei einer Datenverwendung die Grundsätze des § 6 DSG 2000 einzuhalten sind. Dabei dürfte es, anders als die DSK vertritt, nicht ausreichend sein, dass eine Eignung der Daten für die anfordernde Behörde denkmöglich erscheint, sie muss mit dem ursprünglichen Zweck vereinbar sein. Ob dieses Kriteri-

---

[130] Forgó, Krügel, Rapp aaO., Seite 38
[131] Dohr/Pollirer/Weiss,/Knyrim, Kommentar Datenschutzrecht, Stand Dezember 2011, § 4 Anm. zu Abs. 1

um gegeben ist, hängt von einem Zweckvergleich im Einzelfall und auch von der Art der Daten ab. Bei sensiblen Daten im Sinne von § 4 Ziffer 2 DSG 2000 wird eine stärkere Bindung an den ursprünglichen Erhebungszweck geboten sein als bei nicht sensiblen. Wenngleich der Zweckbindungsgrundsatz in der DS-RL und im DSG nur in abgeschwächter Form realisiert worden ist, bedeutet dies keineswegs, dass die öffentliche Verwaltung in ihrer Gesamtheit als ein Informationsverbund zu betrachten ist, in dem personenbezogene Daten beliebig oder auch nur bei denkmöglicher Eignung für den Verwender ausgetauscht werden können. Eine Behörde, die personenbezogene Daten an andere abgibt, hat sich nach § 7 Abs. 2 DSG 2000 im Rahmen einer Plausibilitätsprüfung zu vergewissern, ob für die Verarbeitung durch den Empfänger eine gesetzliche Grundlage besteht und der Verarbeitungszweck mit dem ursprünglichen vereinbar ist.

Der EuGH hat sich in der Entscheidung Huber gegen Deutschland[132] mit der Frage der Zweckbindung befasst. Die Daten des österreichischen Staatsbürgers Huber waren in Deutschland im Ausländerzentralregister gespeichert worden. Zugang zu den Daten hatten nicht nur die Ausländerbehörden, sondern auch die Sicherheits,- Justiz- und Polizeibehörden. Das Gericht sah es in erster Linie als einen Verstoß gegen das Diskriminierungsverbot des Art. 12 Abs. 1 des damaligen EG-Vertrages an, dass EU-Bürger in Deutschland anders behandelt werden als inländische Bürger. Er hat aber auch ausgeführt, dass ein Ausländerzentralregister nicht zur Kriminalitätsbekämpfung genutzt werden und keine entsprechenden Daten enthalten darf. Was die die Modalitäten der Nutzung eines solchen Registers im Hinblick auf die Behandlung aufenthaltsrechtlicher Fragen betreffe, könne nur ein Zugang von Behörden mit Befugnissen in diesem Bereich als erforderlich im Sinne von Art. 7 Buchst. e DS-RL angesehen werden. Nach der genannten Bestimmung ist die Verarbeitung personenbezogener Daten nur unter der Voraussetzung zulässig, dass die Verarbeitung im Interesse der Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erfolgt, die dem für Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde. Auch diese Entscheidung verdeutlicht, dass die öffentliche Verwaltung kein Informationsverbund ist und eine Verwendung

---

[132] Urteil des EuGH vom 16.12.2008, Rs. C-524/06, insbes. Rd-Nr. 59, 61, http://curia.europa.eu/juris/celex.jsf?celex=62006CJ0524&lang1=de&type=NOT&ancre=, letzter Abruf 16.04.2012.

von personenbezogenen Daten, die für einen bestimmten Zweck erhoben worden sind, nicht ohne weiteres für andere Zwecke zulässig ist. Der Verwender muss aufgrund einer ihm gesetzlich übertragenen Aufgabe zur Nutzung der Daten berechtigt sein, unabhängig davon, ob er die betreffenden Daten selbst erhoben oder übermittelt erhalten hat. Dass eine Eignung von Daten für die Verwendung durch eine andere Behörde denkmöglich erscheint, wie es die DSK vertritt, reicht nach Rechtsprechung des EuGH für die Weitergabe nicht aus.

Zusammenfassend ist bei einer Weitergabe zunächst festzustellen, ob ein Eingriff in das Grundrecht auf Datenschutz bzw. die Privatsphäre vorliegt. Jede Weitergabe von Daten ist mit einer Erweiterung des Kreises der Kenner dieser Daten erhöht, so dass darin bereits eine Beschwer liegt.[133] Auch der EuGH ist dieser Auffassung. In dem Urteil Rechnungshof gegen Österreichischen Rundfunk und andere führt er aus, dass bereits die Weitergabe von Daten unabhängig von der späteren Verwendung eine Beeinträchtigung des durch Art. 8 EMRK gewährleisteten Rechts auf Privatsphäre darstelle.[134]

Wenn jede Übermittlung bereits einen Eingriff darstellt, ist jeweils zu prüfen, ob Vorschriften bestehen, die diesen zulassen und rechtfertigen. Im Rahmen der Amtshilfe ist die anfordernde Behörde gemäß § 7 Abs. 2 Ziffer 2 DSG 2000 verpflichtet, der übermittelnden Behörde ihre Zuständigkeit und rechtliche Befugnis glaubhaft zu machen. Die übermittelnde Behörde hat diese Kriterien und die weiteren Voraussetzungen einer Übermittlung in § 7 Abs. 2 DSG 2000 zu prüfen. Als gesetzliche Grundlage ist nicht jede beliebige Vorschrift geeignet. Aufgrund des Eingriffscharakters einer Datenübermittlung müssen die diese rechtfertigenden Bestimmungen den Anforderungen des § 1 Abs. 2 DSG 2000 und Art. 8 Abs.2 EMRK entsprechen.[135] Die Regelung muss ausreichend klar und bestimmt, erforderlich und verhältnismäßig sein. Im DSG 2000 wird allerdings in den §§ 8 Abs. 3 Ziffer 2 und 9 Ziffer 4 festgestellt, dass durch eine Datenverwendung in Erfüllung einer Verpflichtung zur Amtshilfe keine

---

[133] Wettner , Die Amtshilfe im Europäischen Verwaltungsrecht, Mohr Siebeck, Tübingen 2005, S. 323
[134] Urteil des EuGH vom 20.05.2003 Rechnungshof gegen Österreichischen Rundfunk und andere, C-465/00, und Christa Neumann,C-138/01, und Josef Lauermann, C-139/01 gegen Österreichischen Rundfunk, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000CJ0465:DE:HTML, letzter Abruf 16.04.2012.
[135] Duschanek in Korinek/Holoubek (Hrsg.), Österreichisches Bundesverfassungsrecht, Bd. III, Komm. zu den Grundrechten, Springer Verlag Wien, 7. Lief. 2005, § 1 DSG, Rz. 57.

schutzwürdigen Interessen verletzt werden. Das mit einer Amtshilfe verbundene öffentliche Interesse allein reicht als Rechtfertigung im Sinne von der Verfassungsbestimmung von § 1 Abs.2 iVm. Art. 8 Abs. 2 EMRK nicht aus. Es besteht kein sachlicher Grund dafür, warum bei Eingriffen im Zusammenhang mit einer Amtshilfe geringere Anforderungen gelten sollen als bei sonstigen Eingriffen. Auch die Tatsache, dass Behörden nach der Verfassungsbestimmung des Art. 22 B-VG einander zur Amtshilfe verpflichtet sind, führt nicht zu einer anderen Beurteilung. Die Bestimmung hat zwar Verfassungscharakter, ist jedoch als interne Verpflichtungsnorm und nicht als Befugnisnorm zu bewerten[136], so dass für jeden Amtshilfefall nicht nur formal die Zulässigkeit, sondern das Bestehen einer spezifischen gesetzlichen Ermächtigung nach § 1 Abs. 2 DSG 2000 iVm. Art 8 Abs. 2 EMRK zu prüfen ist. [137] Das gilt auch dann, wenn der Zweck der Datenverwendung bei der empfangenden Behörde mit dem bei der übermittelnden Behörde vergleichbar ist. Bei der Amtshilfe sind also die Voraussetzungen für eine Datenübermittlung nach § 7 Abs. 2 DSG 2000 zu beachten, das Bestehen einer Ermächtigungsgrundlage nach § 1 Abs. 2 DSG 2000 iVm. Art. 8 Abs. 2 EMRK und die Vereinbarkeit des Zwecks der geplanten Verwendung nach § 6 Abs. 1 Ziffer 2 DSG 2000 mit dem der ursprünglichen Verwendung bei der übermittelnden Behörde. Die Beurteilung ob die Voraussetzungen für eine Übermittlung glaubhaft gegeben sind, obliegt dem Übermittler.[138]

In dem letzten Punkt ist in Zukunft eine Änderung denkbar. Wie bereits erwähnt, plant die EU im Interesse einheitlicher Datenschutzstandards in der EU die Verabschiedung einer Datenschutz-Grundverordnung[139], die unmittelbar in den Mitgliedstaaten gelten würde. In Art. 6 Ziffer 4 des Entwurfs ist vorgesehen, dass personenbezogene Daten auch zu anderen Zwecken als die mit Ihrer Erhebung verbundenen verwendet werden dürfen, wenn mindestens eine der in Art. 6 Ziffer 1 des Entwurfs genannten Voraussetzungen für die Rechtmäßigkeit der Verarbeitung vorliegt. Dazu gehört u. a. die unter Art. 6 Ziffer 1 c des Entwurfs genannte Voraussetzung, dass die Verarbei-

---

[136] Wiederin in Korinek/Holoubek (Hrsg.), Österreichisches Bundesverfassungsrecht Bd.II 1. Halbbd., Springer Wien 1999, Art. 22 Rz. 51; Adamovic/Funk/Holzinger Österreichisches Staatsrecht, Bd. 2 , Springer Wien 1998, Rz. 27.077.
[137] Duschanek aaO.
[138] Jahnel, Handbuch Datenschutzrecht, Jan Smarek Vverlag, Wien 2010, Kapitel 4/122, S. 270
[139] Entwurf einer Datenschutz-Grundverordnung, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, letzter Abruf 19.04.2012.

tung zur Erfüllung einer gesetzlichen Verpflichtung erforderlich ist, der der für die Verarbeitung Verantwortliche unterliegt. Damit wird der Zweckbindungsgrundsatz weiter eingeschränkt. Eine Vereinbarkeit mit dem Zweck der ursprünglichen Datenerhebung wäre nicht mehr erforderlich. Es würde ausreichen, wenn die Daten zur Erfüllung einer gesetzlichen Aufgabe bestimmt sind. Mit der geplanten Neuregelung sollen offenbar die Möglichkeiten des Informationsaustausches zwischen den Behörden verbessert werden. Auch die Verordnung würde aber nichts an dem Eingriffscharakter einer Übermittlung von personenbezogenen Daten ändern, so dass auch in Zukunft die Voraussetzungen für einen Eingriff nach Art. 8 Abs.2 EMRK zu prüfen wären.

Zu ergänzen ist noch, dass eine Behörde, an die im Wege der Amtshilfe personenbezogene Daten übermittelt werden, grundsätzlich (Ausnahmen § 24 Abs. 3 DSG 2000) gemäß § 24 Abs. 1 DSG 2000 und entsprechend Art. 11 Abs. 1 DS-RL gehalten ist, den Betroffenen über ihre Identität, die an sie übermittelten Daten und den Zweck der Verarbeitung zu unterrichten. Damit wird der Betroffene in die Lage versetzt, seine Rechte wahrzunehmen, u. a. sein Recht auf Auskunft nach § 26 DSG 2000 und seinen Anspruch auf Richtigstellung oder Löschung gemäß § 27 DSG 2000. Auch die geplante Datenschutz-Grundverordnung sieht in Art. 7 Abs. 1 Ziffer 4 b eine Unterrichtung des Betroffenen für den Fall vor, dass die Daten nicht bei ihm erhoben werden.[140]

Die Datenübermittlung im Wege der Amtshilfe ist also an bestimmte Voraussetzungen gebunden. Eine uneingeschränkte und dem Betroffenen nicht zur Kenntnis gelangende Übermittlung im Wege der Auskunfts- oder Amtshilfe würde den Datenschutz aushöhlen. Es erschiene auch widersprüchlich, wenn im EGovG einerseits besondere Vorkehrungen zur Vertraulichkeit im Form verschlüsselter bPK getroffen werden, andererseits nachsuchenden Behörden bei nur denkmöglicher Eignung für den Empfänger personenbezogene Daten zur Verfügung gestellt werden, wie es die Auffassung der DSK ist.

---

[140] Entwurf einer Datenschutz-Grundverordnung, http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_de.pdf , letzte Abfrage 16.04.2012.

4.6 Kritische Betrachtung des Datenschutzkonzeptes im EGovG

Die Aufteilung in einzelne Bereiche, nach denen die bPK gebildet werden, ist in Anlage 1 zur E-Government-Bereichsabgrenzungsverordnung[141] vorgenommen worden. Nach § 9 Abs. 2 EGovG sollte die Abgrenzung der staatlichen Tätigkeitsbereiche so vorgenommen werden, dass zusammengehörende Lebenssachverhalte in ein und demselben Bereich zusammengefasst werden und miteinander unvereinbare Datenanwendungen innerhalb desselben Bereiches nicht vorgesehen sind. Es fällt jedoch auf, dass zum Teil Behörden mit sehr unterschiedlichen Aufgabenstellungen zu einem Bereich zusammengefasst worden sind. So sind im Bereich „Bauen und Wohnen“ die „Schlichtungsstelle nach MRG“, die „Energiesparförderung“ und der „Grundverkehr“ enthalten, im Bereich „Gesundheit“ neben der „Krankenpflege“ die „Überwachung des Giftverkehrs“, das „Bestattungswesen“ und die „Überwachung und Bekämpfung des Drogenmissbrauchs“. Unter der „Vermögensverwaltung“ sind auch „Fuhrpark“ und „Amtswirtschaft“ aufgeführt. Es erscheint etwas widersprüchlich, wenn einerseits im EGovG ein hoher Aufwand betrieben wird, um eine Zusammenführung von Daten aus verschiedenen Bereichen zu verhindern, andererseits bei der Bildung der Bereich zum Teil eine recht grobe Zuordnung vorgenommen wurde. Die Wirkung des EGovG, mit dem u. a. auch eine Profilbildung über einzelne Bürger verhindert werden soll, wird in seiner Wirkung auch dadurch eingeschränkt, dass große und wichtige Bereiche andere Identifizierungsverfahren verwenden, z. B. das Finanzwesen die Steuer-und Sozialversicherungsnummer und auch das Gesundheitswesen die Sozialversicherungsnummer. Da die Bereiche nach der Bereichsabgrenzungsverordnung zum Teil recht groß sind, werden für interne Bearbeitung in einem Bereich zusätzliche Identifizierungsmerkmale in Form von Geschäftszahlen verwendet, § 11 EGovG. Da diese auf den Dokumenten aufgeführt werden, können auf diese Weise doch Zusammenhänge sichtbar werden. In der Literatur wird aus diesen Gründen das mit dem EGovG verbundene Bestreben, den „gläsernen Menschen“ zu verhindern, als Illusion bezeichnet.[142]

---

[141] http://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40054144/NOR40054144.pdf, letze Abfrage 19.04.2012.

[142] Priglinger, Auswirkungen der EU-DL-Richtlinie auf die E-Gov-Welt, in Jahnel (Hrsg.) Jahrbuch Datenschutzrecht und E-Government 08, S. 269 ff. (275).

Schwierigkeiten, das Konzept des EGovG durchzuhalten, entstehen auch aus einer anderen Richtung. Auf der E-Government-Konferenz an der Donau-Universität Krems im Jahre 2008 wurde bereits über die Europäisierung des E-Government diskutiert. Diese zunehmende Entwicklung des Verwaltungshandeln über die die Grenzen hinweg, z. B. durch die EU-Dienstleistungsrichtlinie, das Internal Market System und das Pan-European E-Procurement-System zwinge zu einer Neugestaltung des E-Government-Konzeptes. Die Verwaltungsprozesse entwickelten sich zunehmend in behörden- und ebenenübergreifende Aktivitäten.[143]

Die Aufteilung in einzelne Bereiche gemäß der Bereichsabgrenzungsverordnung führt dazu, dass in jedem Bereich gesonderte Datensammlungen mit zum Teil identischen Daten entstehen, was organisatorisch und wirtschaftlich nicht sehr sinnvoll erscheint. So wird dann auch kritisiert, dass das EGovG mit einer Abgrenzung der Dienstleistungen und Daten die Silosicht unterstütze. Das Gesetz schließe andere Möglichkeiten, das Problem des Datenschutzes zu lösen, auf unbestimmte Zeit aus.[144] Das dem EGovG zugrunde liegende Konzept ist auf die bestehende Hierarchie der Verwaltung ausgerichtet und nicht auf die Verwaltungsprozesse, die behörden- und zunehmend auch länderübergreifend gestaltet werden müssen. Mit der Speicherung von häufig identischen Daten in verschiedenen Bereichen der Verwaltung ist ein erhöhter Pflegeaufwand sowie ein erhöhtes Risiko für Fehler und Missbräuche verbunden. Außerdem wird dadurch die Zusammenarbeit zwischen verschiedenen Bereich erschwert. Der Umweg über die Stammzahlenregisterbehörde und verschlüsselte Fremd-bPK ist ein zusätzlicher Aufwand.

Einen weiteren Nachteil bedeutet der Umstand, dass das Konzept des EGovG in wichtigen Bereichen wie Finanz-, Gesundheits- und Bildungswesen nicht umgesetzt ist und statt dessen eine einheitliche Personenkennziffer, die Sozialversicherungsnummer, verwendet wird, so dass Daten aus diesen Bereichen leicht zusammengeführt werden können.

---

[143] Digitales Österreich: E-Government-Konferenz 2008 , http://www.donau-uni.ac.at/de/department/gpa/verwaltung/news/id/11871/index.php, letzte Abfrage 17.04.2012.
[144] Priglinger, Auswirkungen der EU-DL-Richtlinie auf die E-Gov-Welt,in Jahnel (Hrsg.) Jahrbuch Datenschutzrecht und E-Government 08, S. 269 ff. (275).

Nicht sehr vorteilhaft ist auch der Umstand, dass die DSK, deren eigentliche Aufgabe es ist, die Einhaltung der auf der Grundlage der DS-RL erlassenen Datenschutzbestimmungen zu überwachen, gemäß § 7 Abs. 1 EGovG auch Stammzahlenregisterbehörde eingesetzt worden ist. In dieser Funktion muss sie sich gewissermaßen selbst überwachen und kann in einen Interessenkonflikt geraten. Die Unabhängigkeit der DSK steht auch bereits im Rahmen ihrer traditionellen Aufgabe in der Kritik. Mit Rücksicht auf die Eingliederung in das Bundeskanzleramt und die Personenauswahl gemäß § 36 DSG 2000 und die Abhängigkeit vom Bundeskanzler in Bezug auf die sachliche und personelle Ausstattung der Geschäftsstelle, § 38 Abs. DSG 2000 wird die Unabhängigkeit der DSK in Zweifel gezogen.[145] Seitens der EU-Kommission ist deshalb bereits ein Vertragsverletzungsverfahren gegen Österreich eingeleitet worden.[146]

Unabhängig von der Stellung der DSK im Rahmen des E-Government stellt sich die Frage, ob es Alternativen zum Konzept des EGovG gibt, die einerseits die Zusammenarbeit zwischen verschiedenen Behörden fördern, aber andererseits auch den Anforderungen des Datenschutzes Rechnung tragen. Wie in der Wirtschaft schon in großem Umfang üblich sollte auch die DV-Unterstützung in den Behörden an den Arbeitsabläufen, d. h. an der logischen und zeitlichen Abfolge von einzelnen Arbeitsschritten bis zur Erledigung eines Vorgangs ggf. unter Einbindung mehrerer Behörden ausgerichtet werden.

4.7 Datenschutz bei ämterübergreifenden Verwaltungshandeln

Die Regeln des Datenschutzes mit Beachtung der Erforderlichkeit, Verhältnismäßigkeit, Zweckbindung und Transparenz vertragen sich nicht ohne weiteres mit dem Streben nach einer effektiven Verwaltung mit möglichst uneingeschränkten Zugriff auf alle für die Bearbeitung eines Vorgangs erforderlichen Daten. Die Zusammenarbeit zwischen Behörden in vertikaler Richtung (EU, Bund, Länder, Gemeinden) und in horizontaler Ebene zwischen Behörden mit unterschiedlichen Aufgabenstellungen erfordert eine entsprechende Vernetzung. Angestrebt wird dabei eine Integration der Verwaltungsdienstleistungen in Form eines One-Stop-Governments, d. h. das Ziel,

---

[145] Mayer- Schönberger/Brandl, Datenschutzgesetz, 2. Aufl., Linde Verlag Wien 2006, S. 40
[146] Meldung Datenschutzforum vom 10.11.2009, https://www.bfdi.bund.de/bfdi_forum/archive/index.php/t-702.html.

für einheitliche Lebenssachverhalte für die Bürger von einer Stelle aus behördenübergreifend bearbeiten und erledigen zu lassen, so dass die Bürger auch für die Erledigung komplexer Vorgänge nur einen Ansprechpartner haben.[147]
Ein Ansatz, den Datenschutz auch in einer Welt zunehmenden Datenanwendungen zu realisieren, besteht darin, diesen bereits durch entsprechende Gestaltung der der Informationstechnik zu implementieren. Rechtliche Anforderungen müssen in eine rechtskonforme insbesondere datenschutzgerechte Technikgestaltung umgesetzt werden.[148] An der Universität Kassel ist im Rahmen des Projektes *Verfassungsverträgliche Technikgestaltung* (provet) eine Methode (KORA)entwickelt worden, die in einem vierstufigen Verfahren abstrakte rechtliche Vorgaben in konkrete technische Gestaltungsvorschläge übersetzt.[149] Diese Methode sei auf alle Informations- und Kommunikationstechniken übertragbar, so dass auch in E-Government-Anwendungen mit KORA Technik rechtskonform gestaltet werden könne.[150]

Als Ergebnis eines Entwicklungsprozesses der letzten 15 Jahre werden in der gewerblichen Wirtschaft DV-Anwendungen nicht mehr isoliert für einzelne Funktionsbereiche (z. B. Vertrieb, Produktion Buchhaltung, Personalwesen) entwickelt, sondern prozessorientiert. D. h. Sie werden an den einzelnen Arbeitsabläufen, die in der Regel mehrerer Funktionsbereich berühren, ausgerichtet. Um die mehrfache Haltung von Daten zu verbunden mit entsprechendem Pflegeaufwand und erhöhtem Fehlerrisiko zu vermeiden, wird eine einheitliche Datenbasis angestrebt. Der Zugriff auf die Daten läuft dabei über die jeweilige Anwendung, so dass auf diese Weise eine Steuerung der Zugriffsberechtigungen möglich wird.

Auch der öffentlichen Verwaltung werden DV-Anwendungen immer mehr nach diesen Grundsätzen entwickelt. Zu der Vorgehensweise für die Einführung des Geschäftsprozessmanagements in der öffentlichen Verwaltung gibt es seit 2008 auch

---

[147] Yildirim, Datenschutz und E-Government, Deutscher Universitäts-Verlag, 1 Aufl. 2004, S. 313/314.
[148] Roßnagel, Verantwortung für Datenschutz, Informatik_Spektrum_1_Dezember_2005, S. 462 ff (471, 472), http://www.springerlink.com/content/f414801348142428/fulltext.pdf, letzte Abfrage 30.12.2011.
[149] Hammer,Pordesch,Roßnagel, KORA. Eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für Informations- und Kommunikationssysteme, Infotech 1/1993, S. 21 ff.
[150] Yildirim aaO. Seite 287.

eine DIN-Empfehlung.[151] Für die Entwicklung kennzeichnend ist eine Stellungnahme des österreichischen Städtebundes, in der die wesentlichen Gesichtspunkte für echtes (true) E-Government zusammengefasst sind. [152]

Voraussetzung für eine Behörden- und länderübergreifende Zusammenarbeit ist die Standardisierung der eingesetzten Technik und einheitliche Datenstrukturen sowie Softwarearchitekturen. Wichtig ist, dass Anwendungen an der Folge der Arbeitsschritte (work flow, Prozesse) ausgerichtet und nötigenfalls ämterübegreifend ausgestaltet werden. Die jeweilige Aufgabenstellung ist auch für den Zugriff auf personenbezogene Daten maßgeblich und wird durch geeignete informationstechnische Mechanismen (z. B. mehrstufige Verschlüsselung[153] oder Metadatenmanagement[154]) realisiert. Wesentlich erscheint, dass bei der Gestaltung der Prozesse und der dafür eingesetzten DV-Instrumente darauf geachtet wird, dass die beteiligten Behörden nur auf die Daten zugreifen können, die sie für die Erledigung von Aufgaben in ihrem Zuständigkeitsbereich benötigen. Wirksamer Zugriffschutz ist also das wesentliche Kriterium, um einerseits eine zweckgebundene Verwendung von Daten sicherzustellen und andererseits eine eine ämterübergreifen Zusammenarbeit zu ermöglichen.[155]

Das deutsche Bundesamt für Sicherheit in der Informationstechnik hat ein E-Government-Handbuch mit Empfehlungen für die erforderlichen organisatorischen

---

[151] DIN-Fachbericht 158, http://www.nia.din.de/sixcms_upload/media/2397/Kurzuebersicht_Final.pdf, Abfrage 01.03.2012.

[152] *„Echtes (true) E-Government erhebt den Anspruch einer durchgängigen elektronischen Bearbeitung entlang der Prozesskette, also von der Antragstellung bis hin zur (nach Möglichkeit) elektronischen Erledigung. Eine verwaltungsinterne Vernetzung -und zwar nicht nur hardwareseitig, sondern auch bei den operativen Bearbeitungssystemen (z.B. Dokumentenmanagement, elektronische Aktenverwaltung, Verwaltungsfachanwendungen)- stellt daher eine Grundvoraussetzung dar..... Für eine verwaltungsübergreifende Zusammenarbeit ist es manchmal notwendig, Organisationseinheiten der Verwaltung eindeutig zu identifizieren und über diese Identifikation auch (elektronisch) ansprechen zu können."* aus Priglinger, Auswirkungen der EU-DL-Richtlinie auf die E-Government-Welt, in Jahnel (Hrsg.) Datenschutzrecht und E-Government , Jahrbuch 08, S. 270/271.

[153] Laue, Maidl, Peters, Zweckbindung in ämterübergreifenden Verwaltungswokflows, DuD 2007, S. 810 ff (812): Peters, Audersch, Laue, Datenschutzgerechte Vorgangsbearbeitung im eGovernment, in Horster, Patrick (Hrsg.): D-A-CH Security 2007 Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven. Klagenfurt, Austria, Juni 2007, S. 166 ff; Audersch, Laue, Datenschutzgerechtes Workflow-Management bei Mehrfachanträgen in ämterübergreifenden Verwaltungsprozessen, in Hochberger/Liskowsky (Hrsg.) Informatik 2006, Informatik für Menschen Bd. 2, S. 422 ff..

[154] Priglinger in Jahnel (Hrsg.), Datenschutzrecht und E-Government, Jahrbuch 08, Auswirkungen der EU-DL-Richtlinie auf die E-Gov-Welt, S. 267 ff (279).

[155] Laue,Maidl,Peters aaO. Seite 811.

Maßnahmen für die Gestaltung von E-Government-Prozessen herausgegeben.[156] Im Hinblick auf eine europaweite Zusammenarbeit der Verwaltungen hat auch die EU-Kommission Initiativen für eine Standardisierung der IT-Umgebungen im Bereich E-Government ergriffen. In einem Weißbuch zur ITK-Normung werden auch für das E-Government relevante Empfehlungen gegeben.[157]

Auch aktuelle IT-Technologien wie Wissensmanagement und semantische Web-Dienste werden für E-Government-Anwendungen eingesetzt.[158] Aus dem juristischen

---

[156] Datenschutzgerechtes E-Government, S. 37/38, https://www.bsi.bund.de/cae/servlet/contentblob/476812/publicationFile/28294/2_Daten_pdf.pdf, letzter Abruf 18.04.2012: „*• Es muss sichergestellt sein, dass nur berechtigte Nutzer den Zugang zu den Daten haben. Die Identifizierung und Authentisierung sollte an zentraler Stelle durchgeführt werden (Authentifizierungsserver) bzw. über das jeweilige Betriebssystem erfolgen.*

• Rechte sind sowohl benutzerbezogen als auch datei- oder programmbezogen zu vergeben, um die Zugriffsmöglichkeiten zweckgebunden zu begrenzen. Dabei ist der Maßstab immer das fachliche Anforderungsprofil und die Arbeitsaufgabe des einzelnen Benutzers.

• Arbeitsschritte, die im Hinblick auf die Einhaltung der Zweckbindung besonders sensibel sind, sind zu Zwecken der Beweissicherung, soweit notwendig, zu protokollieren. Beweissicherung bedeutet in diesem Zusammenhang, dass es im Nachhinein möglich sein muss, den Missbrauch zugestandener Rechte nachzuweisen oder die versuchte Ausübung von nicht zugestandenen Rechten aufzudecken.

• Daten sind logisch getrennt zu speichern. In diesem Fall ist eine gegenseitige Abschottung der zweckgebundenen Datenbestände am einfachsten und am datenschutzfreundlichsten zu realisieren.

• Moderne Datenverarbeitungsanlagen bieten die Möglichkeit, gleichzeitig mehrere Anwendungen abzuarbeiten. Hier ist darauf zu achten, dass die einzelnen Anwendungen und ihre jeweils zweckgebundenen Daten gegenseitig voneinander abgeschottet verarbeitet werden. Dies kann in der Praxis durch den Einsatz technischer Zusatzsysteme erreicht werden, die beispielsweise auf einem Prozessor mehrere virtuelle Maschinen simulieren, welche die jeweiligen Anwendungen einschließlich deren Daten gegeneinander abgekapselt verarbeiten.

• Sensible Daten sind verschlüsselt zu speichern und zu übertragen, damit eine inhaltliche Kenntnisnahme der Daten durch Unbefugte verwehrt wird. Die Prozeduren der Verschlüsselung sind für die Benutzer transparent zu halten.

• Für besondere Zwecke erhobene Daten sollten mit einem spezifischen Kennzeichen versehen werden, welches den Zweck ihrer Erhebung sowie einer eventuellen Verarbeitung und Übermittlung spezifiziert, sodass eine Verwendung für einen anderen Zweck kontrolliert werden kann. Die Vergabe solcher Kennzeichen und die Sicherung der Zweckbindung anhand der Auswertung dieser Kennzeichen stellt eine elegante und zukunftsorientierte Sicherheitstechnologie dar. Für ihre technische Realisierung wären allerdings erhebliche Änderungen bzw. Erweiterungen der bestehenden Betriebs- und Datenbanksysteme sowie Anwendungsprogramme erforderlich, die derzeit noch nicht über solche Funktionalitäten verfügen.“

[157] KOM(2009) 324 endgültig,WEISSBUCH Modernisierung der IKT-Normung in der EU, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0324:FIN:DE:PDF , letzte Abfrage 30.12.2011

[158] Sabol, Access to E-Government Services by Employing semantic Technologies, http://www.epractice.eu/en/cases/accessegov , letzte Abfrage 30.12.2011; http://www.accessegov.org/acegov/web/uk/index.jsp?id=50024, letzte Abfrage 30.12.2011 *“By employing semantic technologies the Access-eGov project will support semantic interoperability among e-government services across organizational, regional and linguistic borders. For service providers (on all levels of public administration - local, regional, national, and European) Access-eGov will enable introduction of a (new) e-service to the world of e-government interoperability in an easy way. The government service registered in the Access-eGov may be localized, contracted and used auto-*

Strukturdenken und der juristischen Methodenlehre Konzepte zu entwickeln, die sich für eine informatorische Formalisierung eignen, wie z. B. Normen, die richterliche Rechtsanwendung und das Begriffsdenken im Recht, gehört zu den Aufgabenstellungen der Rechtsinformatik. Ausgangspunkt ist dabei die Rechtsordnung in ihrer Erscheinungsform als Textkorpus in Rechtsinformationssystemen, was jedoch für eine automatisierte Unterstützung der Rechtsanwendung nicht ausreicht. Dafür sind das Erkennen, Beschreiben, und Prognostizieren von Umwelt und Realität in Strukturen und Prozessen in Form von Modellen erforderlich.[159] Die öffentliche Verwaltung erweist sich dabei als besonders für die Rechtsinformatik geeignet, weil zwar nicht alle, aber viele Fallgestaltungen anders als bei der richterlichen Urteilsfindung gleich oder ähnlich sind.

4.8 Die Europäisierung der Amtshilfe

Bedingt durch die Entwicklung des Binnenmarktes ist die Notwendigkeit einer verstärkten Zusammenarbeit zwischen den Behörden verschiedener Mitgliedstaaten in der EU entstanden. Als Folge davon hat die EU im Rahmen ihrer Lissabon-Strategie Pläne für länderübergreifende Konzepte des E-Government entwickelt. Die ersten Projekte gehen auf einen Beschluss des Europäischen Parlaments und des Rates vom 21. 04. 2004[160] über Interoperable Delivery of European E-Government Services to public Administrations, Businesses and Citizens (IDABC) zurück. Bezüglich des

---

matically through agents and other IT components. For citizens and business users the Access-eGov will provide two basic categories of services. Firstly, it will provide a meta-service - depending on the needs and context of the user Access-eGov will find (identify) traditional and/or e-government services relevant to the given life event or business episode. Secondly, once the relevant services are found, Access-eGov will generate a scenario consisting of elementary government services. Usually these scenarios will be of "hybrid" nature - i.e. combination of elementary traditional and e-services - realization of which leads to a requested outcome (e.g. to get a new driving license, if you lost both your ID and the old driving license etc.).At the realisation of the scenario the user will be guided by a virtual personal assistant. Access-eGov is built on peer-to-peer and service-oriented architecture. Component-based security infrastructure provides a complete portfolio of necessary security services (authentication, authorization, attribute management, access control, data protection, auditing) that are accessible through web service interfaces. All the Access-eGov components will be delivered as an open source solution. The system developed will be validated also by the non EU project partner (GUC, Egypt), which will lead to increased employability of the system due to taking into account cross-cultural and language issues."

[159] Schweighofer , „Strukturdenken und Modellbildung im Recht" in Traumüller/Wimmers (Hrsg.), Informatik in Recht und Verwaltung Gestern-Heute-Morgen, Ehrenband für Prof. Fiedler zum Achtzigsten Geburtstag, 2009, S.. 89 ff. (90-92).

[160] ABl. 2004, L 181/25, Beschluss 2004/387/EG des Europäischen Parlamentes und des Rates vom 21. April 2004 über die interoperable Erbringung elektronischer Behördendienste (E-Government-Dienste) für öffentliche Verwaltungen, Unternehmen und Bürger (IDABC), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:181:0025:0035:DE:PDF, letzte Abfrage 30.12.2011.

Datenschutzes wird auf die Richtlinien 95/48/ EG und 2002/58EG, also die DS-RL und die Kommunikations-Datenschutzrichtlinie verwiesen.[161] Das IDABC-Programm ist inzwischen ausgelaufen und durch das ISA-Programm 2010-2015[162] ersetzt worden. Das Ziel des ISA (Interoperability Solutions for European Public Administrations Programme) ist es, die die grenzüberschreitende elektronische Zusammenarbeit zwischen Verwaltungen in den Mitgliedstaaten innerhalb der EU zu ermöglichen.

Ein Hauptproblem ist die Identifizierung einzelner Bürger und juristischer Personen über Ländergrenzen hinweg. Anstelle der Einführung einheitlicher Identifizierungsmerkmale in der EU wird in dem gemischten Konsortium aus privaten und öffentlichen Einheiten STORK (Secure Identity across Border linked)[163] an einem Konzept gearbeitet, ein System zu implementieren, das es Bürgern, Unternehmen und Behörden länderübergreifend ermöglichen soll, auf der Basis nationaler Identitätsmerkmale mit Behörden in anderen Ländern zu kommunizieren.

Ein weiteres Projekt PEPPOL[164], das Pan European Public Procurement Online, ist ein von der EU unterstütztes Projekt zur Förderung der Interoperabilität im öffentlichen Beschaffungswesen. Dafür werden in Pilotprojekten entsprechende Module entwickelt.

Die Vielzahl der von der EU geförderten oder selbst betrieben Projekte verdeutlicht die zunehmende europäische Integration im Bereich des E-Government. Im aktuellen Aktionsplan für das E-Government[165] wird angestrebt, einen Übergang von derzeiti-

---

[161] Ziffer 15 der Begründung zum Beschlusses 2004/387/EG

[162] ISA (Interoperability Solutions for European Public Administrations programme), http://ec.europa.eu/isa/, Abfrage 27.03.2012

[163] STORK Overview for new Member States "handout at the 5th STORK Industry Group Meeting 16.11.2011, S. 6 https://www.eid-stork.eu/index.php?option=com_processes&Itemid=60&act=streamDocument&did=1704, Seite 6 : "*In 2008 a consortium of 29 participants of 14 European countries was founded, to execute the STORK project. The project had as main objective to establish a European eID interoperability platform, within existing legal restrictions, respectful with all national cultures and complying with the requirements of scalability, trust and security, especially the privacy*." Letzte Abfrage 18.04.2012.

[164] Peppol, Pan European Public Procurement Online, http://www.peppol.eu/events/event_repository/files-for-promotion-and-publication/peppol_kompetenzprofil_final.pdf, letzte Abfrage 30.03.2012

[165] Europäischer eGovernment-Aktionsplan 2011-2015 – Einsatz der ITK zur Förderung intelligent, nachhaltig und innovativ handelnder Behörden, http://ec.europa.eu/information_society/activities/egovernment/action_plan_2011_2015/docs/action_plan_de_act_part1_v1.pdf, letzte Abfrage 30.03.2012.

gen elektronischen Behördendiensten zu einer neuen Generation offener, flexibler und kooperativer sowie nahtlos funktionierender Behördendienste zu fördern, die auf regionaler, nationaler und europäischer Ebene erbracht werden.[166] Dazu hat die EU-Kommission zusammen mit Vertretern der Mitgliedstaaten eine Europäische Interoperabilitätsstrategie (EIS) erstellt und gleichzeitig, nach Konsultation mit den Mitgliedstaaten, einen Europäischen Interoperabilitätsrahmen für Europäische öffentliche Dienste (EIF) erstellt.[167] Mit der EIS wird das Ziel verfolgt, europäische öffentliche Dienste durch bessere Interoperabilität deutlich zu verbessern und mit dem EIF wird angestrebt, einen Rahmen für öffentliche europäische Dienste einzurichten. Der EIF soll europäischen öffentlichen Verwaltungen Orientierung in Bezug auf die Definition, Ausgestaltung und Durchführung europäischer öffentlicher Dienste bieten. Beide Programme sollen im Rahmen des ISA, Interoperability Solutions for European Public Administrations Programme, weitergeführt werden.

Die ämter- und länderübergreifende Zusammenarbeit wird auch durch den Beschluss der EU-Kommission zur Errichtung eines Binnenmarktinformationsystems (Internal Market Information System, IMI)[168] für den grenzüberschreitenden Datenaustausch zwischen Behörden verschiedener Mitgliedstaaten gefördert. IMI wird gegenwärtig hauptsächlich für die Anerkennung von Berufsqualifikationen[169] und die Anwendung der Dienstleistungsrichtlinie[170] in Anspruch genommen. Der Beschluss berücksichtigt in seinem Art. 5 auch Gesichtspunkte des Datenschutzes. Insoweit wird auf die DS-

---

[166] Siehe Aktionsplan in vorstehender Fußnote, Seite 5

[167] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen -Interoperabilisierung europäischer öffentlicher Dienste-, Seite 8 und 9, http://www.parlament.gv.at/PAKT/EU/XXIV/EU/04/31/EU_43117/imfname_10008671.pdf , Abfrage 30.03.2012.

[168] 2009/739/EG: Entscheidung der Kommission vom 2. Oktober 2009 zur Festlegung der praktischen Regelungen für den Informationsaustausch auf elektronischem Wege zwischen den Mitgliedstaaten gemäß Kapitel VI der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt (Bekannt gegeben unter Aktenzeichen K(2009) 7493) (Text von Bedeutung für den EWR**)** http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:263:0032:0034:DE:PDF, letzte Abfrage 30.12.2011.

[169] Richtlinie 2005/36/EG über die Anerkennung von Berufsqualifikationen (ABl. L 255 vom 30.9.2005, S. 22), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2005L0036:20110324:DE:PDF, letzte Abfrage 10.12.2011.

[170] Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt (ABl. L 376 vom 27.12.2006, S. 36), http://www.llv.li/pdf-llv-sewr-32006l0123.pdf, letzte Abfrage 10.12.2011

RL und die Kommunikationsdatenschutzrichtlinie 2002/58/EG[171] Bezug genommen. Die Kommission hat aber die Vorsorge für den Datenschutz im Rahmen des IMI noch durch eine gesonderte Entscheidung über den Schutz personenbezogener Daten bei der Umsetzung des Binnenmarktinformationssystems ergänzt.[172] Nach Art. 4 dieser Entscheidung werden alle personenbezogenen Daten, die sich auf die betroffenen Personen eines Informationsaustauschs beziehen und die zwischen zuständigen Behörden ausgetauscht und in IMI verarbeitet werden, sechs Monate nach formellem Abschluss des Informationsaustauschs gelöscht, es sei denn, eine zuständige Behörde beantragt bei der Kommission ausdrücklich das Löschen der Daten vor dieser Frist. Die IMI-Nutzer haben nur insoweit Zugriff auf personenbezogene Daten Betroffener, wie dies für die Bearbeitung des Vorganges erforderlich ist. Einzelheiten dazu sind Art. 12 des Beschlusses geregelt.

Die Einführung des IMI wird unter Gesichtspunkten des Datenschutzes kritisch gesehen. Die erwähnte Berufsanerkennungsrichtlinie sieht in den Art. 8, 50 und 56 Verpflichtungen zur Amtshilfe vor, ebenso Art. 28 der Dienstleistungsrichtlinie. Amtshilfe für sich genommen begründe keine rechtliche Befugnis zu personenbezogener Informationshilfe und Eingriffe in Grundrechtspositionen. Die Verwendung personenbezogener Daten durch öffentliche Stellen sei grundsätzlich nur zulässig, soweit dies zur Erfüllung der ihnen durch Gesetz zugewiesenen und in ihre Zuständigkeit fallenden Aufgaben erforderlich ist.[173] Die zentrale Datenhaltung des IMI bei der EU-Kommission wird gleichfalls kritisch betrachtet, weil dafür keine Rechtsgrundlage be-

---

[171] 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 S. 0031 – 0050, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML, letzte Abfrage 30.12.2011; Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl . L 201 vom 31/07/2002 S. 0037 – 0047, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:DE:HTML, letzte Abfrage 30.12.2011.

[172] 2008/49/EG: Entscheidung der Kommission vom 12. Dezember 2007 über den Schutz personenbezogener Daten bei der Umsetzung des Binnenmarktinformationssystems (IMI) (Bekannt gegeben unter Aktenzeichen K(2007) 6306) (Text von Bedeutung für den EWR), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D0049:DE:NOT, letzte Abfrage am 30.12.2011.

[173] Scholz, Das neue Binnenmarkt -Informationssystem der EU, DuD 2007, S. 411 ff (413).

stehe und darin auch Risiken für Missbrauch liegen.[174] Länderübergreifende Zusammenarbeit und wirksamer Datenschutz sind offenbar nicht leicht vereinbar.

Dabei ist erkennbar, dass die unmittelbare Zusammenarbeit von Behörden in verschiedenen Mitgliedsländern der EU ständig zunimmt, so dass auch von einer Europäisierung der Amtshilfe gesprochen wird.[175] Wenngleich eine dem Art. 22 B-VG vergleichbare Bestimmung auf europäischer Ebene nicht besteht, ist auch in der Zusammenarbeit der Behörden verschiedener Mitgliedstaaten aufgrund von allgemeinen Rechtsgrundsätzen der EU von einer Verpflichtung zur Amtshilfe auszugehen.[176] Darüber hinaus bestehen auf verschiedenen Gebieten bereichsspezifische Bestimmungen, die eine enge Zusammenarbeit von Behörden verschiedener Mitgliedstaaten und wechselseitige Unterstützung vorsehen. Zu nennen ist dabei für den Bereich der Steuern das EG-Amtshilfegesetz,[177] für das Sozialrecht Art. 76 Abs. 2 Satz 1 der VO 883/2004/EG[178], für das Lebensmittelrecht die Richtlinie 89/608/EWG[179] vom 21.11.1989. Für das Wettbewerbsrecht enthält Art 105 Abs. 1 AEUV eine primärrechtliche Verpflichtung zur Amtshilfe. Schließlich ist die Zusammenarbeit der Mitgliedstaaten im Bereich der inneren Sicherheit, der früheren dritten Säule, zu erwähnen, die in Kapitel 9 ausführlich beschrieben wird. Ausführliche Vorschriften über die Amtshilfe enthält auch die Dienstleistungsrichtlinie 2006/23/EG180 in den Art 28 ff. Mit der fortschreitenden auch elektronischen Vernetzung über Ländergrenzen hinweg und der damit erstrebten Verwaltungseffizienz sind auch Gefahren für den Rechtsschutz der Bürger verbunden[181], insbesondere den Datenschutz. Einschlägig sind insoweit bei der Ausführung von EU-Recht die Art 7 und 8 GRCh,

---

[174] Scholz aaO. S. 415.
[175] Schliesky, Die Europäisierung der Amtshilfe, Boorberg-Verlag Stuttgart 2008, S. 47/48.
[176] Wettner, Die Amtshilfe im europäischen Verwaltungsrecht, Mohr Siebek-Verlag Tübingen 2005, S. 303.
[177] Gesetz zur Durchführung der EG-Richtlinie über die gegenseitige Amtshilfe im Bereich der direkten Steuern, bestimmter Verbrauchsteuern und der Steuern auf Versicherungsprämien (EG-Amtshilfe-Gesetz), deutsches BGBl. vom 19.12.1985 Teil I, Seite 2436 ff (2441), http://www.gesetze-im-internet.de/egahig/BJNR024410985.html, letzte Abfrage 10.12.2011
178 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:166:0001:0123:de:PDF, letzte Abfrage 10.12.2011.
[179] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31989L0608:DE:NOT, letzte Abfrage 10.12.2011.
[180] RICHTLINIE 2006/123/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt, http://www.llv.li/pdf-llv-sewr-32006l0123.pdf, letzte Abfrage 10.12.2011.
[181] Wetter, Die Amtshilfe im europäischen Verwaltungsrecht, 2005, S. 305.

die DS-RL sowie Art. 8 EMRK. In der bereits mehrfach zitierten Entscheidung[182] Rechnungshof . /. ORF hat der EuGH in der Übermittlung von Daten, also deren Weitergabe an einen Dritten, einen Eingriff im Sinne von Art 8 EMRK gesehen. Allein die Erweiterung des Kreises der Kenntnisinhaber konstituiert dabei die Eingriffsqualität, unabhängig davon, ob die Weitergabe von Privaten an Behörden oder umgekehrt verläuft oder ob mit der Weitergabe eine Zweckänderung verbunden ist.[183] Auch in der erwähnten Entscheidung des EuGH wird in der schlichten Weitergabe von Daten ein Eingriff, also eine Verletzung des Grundrechtes auf Datenschutz, gesehen, dessen Zulässigkeit unter dem gemeinschaftsrechtlichen Vorbehalt einer entsprechenden Rechtsgrundlage steht, Art 52 Abs.1 GRCh. An eine derartige Rechtsgrundlage sind nach der Rechtsprechung des EGMR und EuGH bestimmte Anforderungen zu stellen, insbesondere die Bestimmtheit einer Ermächtigung zu Eingriffen, so dass diese für Betroffene vorhersehbar sind.[184] Weiter stehen hoheitliche Eingriffe in die Rechte Betroffener unter dem Vorbehalt der Erforderlichkeit, so dass willkürliche Maßnahmen unzulässig sind.[185] Außerdem ist der Grundsatz der Verhältnismäßigkeit zu beachten.[186] Zusammenfassend ist deshalb festzustellen, dass für länderübergrei-

---

[182] Urteil des EuGH vom 20.05.2003, Verb. Rs. C-465, C-138, C-139, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000J0465:DE:HTML, letzte Abfrage 10.12.2011.

[183] Wetter aaO., S.323.

[184] EGMR Urteil vom 20.05.1999, Rekvényi gg. Ungarn**,** ÖJZ 2000, S. 235, Rd.-Nr.: „*34. According to the Court's well-established case-law, one of the requirements flowing from the expression "prescribed by law" is foreseeability. Thus, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.".*

[185] Urteil des EuGH vom 21.09.1989 - Aktenzeichen Rs C-46/87 - Aktenzeichen Rs C-227/88, Rd.-Nr.: *19] Indessen bedürfen in allen Rechtsordnungen der Mitgliedstaaten Eingriffe der öffentlichen Gewalt in die Sphäre der privaten Betätigung jeder - natürlichen oder juristischen - Person einer Rechtsgrundlage und müssen aus den gesetzlich vorgesehenen Gründen gerechtfertigt sein; diese Rechtsordnungen sehen daher, wenn auch in unterschiedlichen Ausgestaltung, einen Schutz gegen willkürliche oder unverhältnismäßige Eingriffe vor. Das Erfordernis eines solchen Schutzes ist folglich als allgemeiner Grundsatz des Gemeinschaftsrechts anzuerkennen.*

[186] Urteil des EuGH vom 20.05.2003, Verb. Rs. C-465, C-138, C-139, Rd.-Nr.: *82 Es bleibt zu prüfen, ob der fragliche Eingriff in einer demokratischen Gesellschaft für die Erreichung des mit ihm verfolgten berechtigten Zweckes notwendig ist.83 Nach der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte bedeutet das Eigenschaftswort notwendig" in Artikel 8 Absatz 2 EMRK, dass ein zwingendes gesellschaftliches Bedürfnis" bestehen und die Maßnahme in einem angemessenen Verhältnis zu dem verfolgten berechtigten Zweck" stehen muss (vgl. u. a. EGMR, Urteil Gillow/Vereinigtes Königreich vom 24. November 1986, Série A, Nr. 109, § 55). Die nationalen Behörden verfügen zudem über ein Ermessen, dessen Umfang nicht nur von der Zielsetzung, sondern auch vom Wesen des Eingriffs abhängig ist" (vgl. EGMR, Urteil Leander/Schweden vom 26. März 1987, Série A, Nr. 116, § 59).*

fende Amtshilfe innerhalb der EU letztendlich dieselben Maßstäbe gelten wie für die Amtshilfe innerhalb Österreichs.

4.9 Zusammenfassung zum EGovG und Datenschutz

Der im EGovG realisierte Datenschutz ist wirksam. Die Stammzahlenregisterbehörde könnte zwar durch Generierung von bPKs auf personenbezogene Daten in verschiedenen Verwaltungsbereichen zugreifen und so Profile einzelner erstellen. Das wäre technisch wohl möglich. Aber das wäre rechtswidrig und mit derartigen Handlungen könnte man jede wohl jede Sicherheitsbarriere unterlaufen. Die Methode der Identifizierung durch bPKs ist zwar einzigartig und wird von keinem anderen Land verwendet.[187] Aber sie verhindert nicht die Zusammenarbeit zwischen verschiedenen Behörden, auch nicht mit Behörden im Ausland, wenngleich der Umstand, bei der Stammzahlenregisterbehörde Fremd-pPKs zu beantragen, zusätzlichen Aufwand bedeutet. Auch für die Zusammenarbeit mit dem Ausland stellt das einzigartige österreichische Konzept keinen Hinderungsgrund dar. Wird im Rahmen eines transaktionsorientierten Onlinedienstes eine Identifizierung des Nutzers notwendig, so könnte der Anbieter auf der Grundlage des öffentlichen Signaturschlüssels der Bürgerkarte eine Anfrage beim zentralen Melderegister tätigen, und ihm würden dann die benötigten Identitätsdaten, nicht aber ZMR- und Stammnummer, übermittelt werden.[188] Auch dieses bedeutet natürlich zusätzlichen Aufwand. Es wäre also von Vorteil, wenn die Systeme den Behörden einerseits einen unmittelbaren Zugriff auf die personenbezogenen Daten im Rahmen ihrer Zuständigkeit ermöglichen aber unzulässige Zugriffe verhindern würde. Es ist denkbar, dass die Entwicklung in diese Richtung verläuft, und der Zwang zur Zusammenarbeit in der EU und die damit verbundene Standardisierung wird diese fördern.

Nachteilig erscheint, dass das Konzept der Identifizierung und Authentifizierung des EGovG nicht durchgängig für alle Bereiche der öffentlichen Verwaltung verwendet wird. Die wichtigen Bereiche Finanzwesen, Gesundheits- und Bildungswesen und

---

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000J0465:DE:HTML, letzte Abfrage 10.12.2011

[187] STORK; D2.2- Report on Legal Interoperability, S.40 , http://www.epractice.eu/files/STORK%20Deliverable%20D2.2,%20Report%20on%20Legal%20Interoperability.pdf , letzte Abfrage am 30.12.2011 :"*In Austria, the base identifier (sourcePIN) may not be used at all. Instead derived ssPINs may be used, but only within Austria."*

[188] Hoye, Digitale Identitäten im Kontext von E-Government-Anwendungen, Diplomica Verlag Hamburg 2010, Seite 51/52

haben gesonderte Regelungen. Sie verwenden die Sozialversicherungsnummer als Identifizierungsmerkmal.

Im Hinblick auf zunehmende länderübergreifende Verwaltungsabwicklungen in der EU und im Interesse einer effizienten und wirtschaftlichen Abwicklung von Verwaltungsvorgängen wäre eine Anpassung des E-Government-Konzeptes an europäische Standards wünschenswert.

Das Handeln der Verwaltung ist nicht auf die z. Zt. vom EGovG erfassten Bereiche beschränkt. Wie sich aus der unter Abschnitt 4.1 beschriebenen Definition ergibt, erstreckt sich das Thema auf alle Bereiche der öffentlichen Verwaltung. Die Frage des Datenschutzes wird deshalb in den folgenden Kapiteln in weiteren Gebieten untersucht.

5. Bildungsdokumentation

Seit dem Jahre 2003 besteht in Österreich ein Bildungsdokumentationsgesetz (BilDokG), zu dem allerdings zu Beginn des Jahres 2008 wesentliche Änderungen in Kraft getreten sind. Wesentliches Ziel des Gesetzes ist es, den bildungspolitischen Entscheidungsträgern die für das Gestalten von Bildung notwendigen Grundlagen an die Hand zu geben. Das betrifft die Gesetzgebung ebenso wie die Verwaltung. Dieser Zielsetzung dienen die im BilDokG vorgesehene Gesamtevidenz der Schüler und Studierenden (§§ 5 bis 7) sowie die darin gleichfalls geregelte, von der Bundesanstalt „Statistik Österreich“ jährlich zu erstellende Bundesstatistik zum Bildungswesen (§ 9) und das ebenfalls von dieser Einrichtung zu schaffende Bildungsstandregister (§ 10).[189]

Das zuständige Ministerium rechtfertigte die Schaffung dieses Gesetzes bei dem Inkrafttreten im Jahre 2003 u.a. auch damit, dass nach der letzten Volkszählung im Jahre 2001 keine weiteren Zählungen dieser Art mehr geplant seien und deshalb Daten aus der Auswertung von Volkszählungen nicht mehr zur Verfügung stünden. An ihre Stelle treten Register und Dateien von Behörden, auf die unter genau geregelten Bedingungen, die in erster Linie dem Datenschutz dienen, zugegriffen werden könne. Diese Entwicklung sei keine österreichische Besonderheit. Eine Reihe europäischer Staaten mit anerkannt hohem Rechtsschutzstandard habe diesen Weg bereits beschritten. Dänemark, Schweden, Finnland oder Norwegen seien nur einige von ihnen. Hätte der Gesetzgeber auf das Auslaufen der Volkszählungen nicht reagiert, wären große Datenlücken im Bildungsbereich die Folge. Für den Ausbau und die weitere Entwicklung des Bildungswesens bedeutsame Informationen wären unwiederbringlich verloren gegangen. Das BilDokG verhindere das Entstehen solcher nicht mehr schließbarer Datenlücken. Es gewährleiste, dass für das Gestalten von Bildung entscheidende soziale Entwicklungen auch weiter statistisch erfasst und ausgewertet werden können.[190]

---

[189] Bundesministerium für Unterricht Kunst und Kultur (früher Bundesministerium für Bildung, Wissenschaft und Kultur, BMBWK, Rundschreiben Nr. 7/2004, Ziffer 1.1, http://www.bmukk.gv.at/ministerium/rs/2004_07.xml, letzte Abfrage 30.12.2011.

[190] BMKWK-Rundschreiben Nr. 7/2004 vom 21.04.2004 aaO., Ziffern 1.2 und 1.3.

5.1 Identifizierung und Nummerierung

Nach § 3 Abs. 6 BilDokG sind die Schüler und Studierenden gehalten, den Leitern einer Bildungseinrichtung neben anderen Daten ihre Sozialversicherungsnummer bekannt zu geben, § 3 Abs. 6 Satz 1 BilDokG. Für die Erstellung der Gesamtevidenzen sind einmal Daten an das Bundesministerium für Unterricht, Kunst und Kultur (BMUKK) zu melden, §§ 5 bis 7 BilDokG, und für die Erstellung der Statistiken und die Erstellung und Führung eines Bildungsregisters an die Bundesanstalt „Statistik Österreich", §§ 9, 10 BilDokG. Gemäß § 6 Abs. 2 BilDokG sind die Daten der Schüler und Studierenden in den Gesamtevidenzen nur indirekt personenbezogen zu speichern. Zu diesem Zweck übermitteln die jeweiligen die Bildungseinrichtungen die im Gesetz im Einzelnen spezifizierten Daten einschließlich der Sozialversicherungsnummern zunächst an die Bundesanstalt „Statistik Österreich", § 6 Abs. 2 BilDokG. Sofern eine österreichische Sozialversicherungsnummer nicht besteht, sind der Bundesanstalt Namen, Vornamen, Geschlecht, Geburtsdatum und Anschrift am Heimatort bzw. Wohnanschrift im Inland zu übermitteln, damit diese sich von der zuständigen Behörde ein Ersatzkennzeichen zuweisen lassen kann, § 3 Abs. 6 Satz 2 BilDokG. Die Bundesanstalt „Statistik Österreich" verschlüsselt die Sozialversicherungsnummer bzw. das Ersatzkennzeichen in nicht-rückführbarer Weise und erzeugt daraus eine Bildungsevidenz-Kennzahl (BEKZ). Anschließend übermittelt sie dann die für die Gesamtevidenzen vorgesehenen Daten[191] ohne die Namen der Betroffenen an das Bundesministerium für Unterricht, Kunst und Kultur (BMUKK), §§ 5 Abs. 2, 6 Abs. 3 BilDokG.

Hinsichtlich der Daten der Studierenden ist das Gesetz nicht ganz klar. Während in § 6 Abs. 2 für die Gesamtevidenzen der Schüler eindeutig gesagt wird, dass die Daten zunächst an die Bundesanstalt „Statistik Österreich" als die für die Bildung der BEKZ zuständigen Stelle geleitet werden, heißt es für die Gesamtevidenzen der Studieren-

---

[191] 1. Monat und Jahr der Geburt, 2. das Geschlecht, die Staatsangehörigkeit, Bezeichnung der Ausbildung und Datum des Beginns, Postleitzahl der Anschrift am Heimatort und Information, ob am Ort der Bildungseinrichtung eine weitere Anschrift besteht, 3. Die Bildungsevidenzkennzahl (BEKZ) und 4. das erste Jahr der allgemeinen Schulpflicht, einen festgestellten sonderpädagogischen Förderbedarf, die Eigenschaft als ordentlicher oder außerordentlicher Schüler, die Schulkennzahl, die Schulformkennzahl und andere mit dem Schulbesuch zusammenhängende Daten über die Teilnahme an Unterrichts- und Betreuungsangeboten, den Schulerfolg, die Schul-und Unterrichtsorganisation, den Bildungsverlauf sowie die Inanspruchnahme von Transferleistungen aus dem Familienlastenausgleich nach Maßgabe der Anlage 1.

den in § 7 Abs. 2 BilDokG, dass die erforderlichen Daten einschließlich Sozialversicherungsnummer aber ohne Angabe der Namen an das BMUKK zu übermitteln sind. Offenbar kann bei den Studierenden der Universitäten gemäß Universitätsgesetz 2002 (BGBl. I Nr. 120), der Universität für Weiterbildung Krems sowie den Fachhochschulen gemäß Fachhochschul-Studiengesetz (BGBl. Nr. 340/1993) und den Pädagogischen Hochschulen die nicht-rückführbare Verschlüsselung der Sozialversicherungsnummer in eine BEKZ durch eine andere Einrichtung als die „Statistik Österreich" vorgenommen werden. Dafür spricht die Wortfolge „hinsichtlich der Bildungseinrichtungen gemäß § 2 Abs. 1 Ziffer 2 lit. a, c, und f auch durch eine andere (als die „Statistik Österreich")[192] geeignete Einrichtung, die den Anforderungen des § 14 des Datenschutzgesetzes 2000 entspricht…" in § 5 Abs. 2 BilDokG. Eine Unklarheit bleibt insofern bestehen, dass nach § 5 Abs. 2 BilDokG die Daten der Studierenden an den Pädagogischen Hochschulen (§ 2 Abs. 1 Ziffer 2 lit. b BilDokG) von der Bundesanstalt „Statistik Österreich" zu verschlüsseln sind, während nach § 7 Abs. 2 BilDokG auch die Leiter der Pädagogischen Hochschulen gehalten sind, die relevanten Daten unmittelbar an das BMUKK zu melden.

In § 5 Abs. 2 BilDokG heißt es ausdrücklich: „*(2) In den Gesamtevidenzen sind die Daten der Schüler bzw. Studierenden nur indirekt personenbezogen zu speichern. Zu diesem Zweck ist vorzusorgen, dass die Datensätze gemäß § 6 Abs. 3 und § 7 Abs. 2 und 3, unbeschadet der Übermittlung gemäß § 9 Abs. 2 an die Bundesanstalt „Statistik Österreich", übermittelt werden. Vor Eingang eines derartigen Datensatzes beim zuständigen Bundesminister sind jedenfalls ….durch die Bundesanstalt „Statistik Österreich", …. auch durch eine andere geeignete Einrichtung, die den Anforderungen an die Datensicherheitsmaßnahmen gemäß § 14 des Datenschutzgesetzes 2000 entspricht, die Datensätze auf Vollständigkeit und Schlüssigkeit zu überprüfen bzw. richtig zu stellen und es ist die Sozialversicherungsnummer bzw. das Ersatzkennzeichen im jeweiligen Datensatz nicht-rückführbar so zu verschlüsseln, dass eine Bildungsevidenz-Kennzahl (BEKZ) gewonnen wird und ein- und dieselbe Sozialversicherungsnummer bzw. ein und dasselbe Ersatzkennzeichen bei der Verschlüsselung jeweils dieselbe BEKZ ergibt. Eine Speicherung der Datensätze durch*

[192] Einschub des Verfassers

den zuständigen Bundesminister unter der Sozialversicherungsnummer und/oder dem Namen des Betroffenen ist für Zwecke der Gesamtevidenzen unzulässig."

Unter Berücksichtigung von § 5 Abs. 2 BilDokG ist das Gesetz also insgesamt so auszulegen, dass auch bei den Studierenden eine Übermittlung von Daten an den BMUKK nicht unmittelbar, sondern erst nach Verschlüsselung durch die „Statistik Österreich" oder eine andere Einrichtung erfolgt, die die Anforderungen von §14 DSG erfüllt.

Nach § 3 Abs. 1 der ursprünglichen Fassung des Gesetzes waren die Leiter aller Bildungseinrichtungen verpflichtet, von den Schülern bzw. Studierenden erhobene persönliche Daten gemäß § 6 Abs. 2 bzw. § 7 Abs. 2 BilDokG a.F. unmittelbar an das Bundesministerium zu übermitteln. Dabei handelte es sich u.a. um das Geburtsdatum, die Sozialversicherungsnummer, das Geschlecht die Staatsangehörigkeit, Beginn und Ende der Ausbildung mit Angabe der Art des Abschlusses, das Personenkennzeichen der jeweiligen Bildungseinrichtung sowie Angaben zum Wohnort. Die Namen der Schüler und Studenten wurden nicht an das BMUKK übermittelt und auch nicht in den Gesamtevidenzen gespeichert. Das BMUKK war gemäß § 5 Abs. 2 BilDokG aF. und § 8 BilDokV aF. wie jetzt die Bundesanstalt „Statistik Österreich" gehalten, den Datensatz vor einer Speicherung in den Gesamtevidenzen zu verschlüsseln und dabei an Stelle der Sozialversicherungsnummer eine BEKZ zu ermitteln, aus der die Sozialversicherungsnummer nicht mehr generiert werden kann. Damit entstehen letztendlich mit der Bildungsdokumentation lediglich indirekt personenbezogene Daten im Sinne von § 4 Abs. 1 2. Halbs. DSG 2000, bei denen die Identität des Betroffen nicht mit rechtlich zulässigen Mitteln bestimmbar ist und daher ein (aus Sicht des österreichischen Gesetzgebers) schutzwürdiges Geheimhaltungsinteresse nicht besteht.

Dazu ist anzumerken, dass die Datenschutzrichtlinie der EU (95/46/EG) nur zwei Arten von Personaldaten, nämlich personenbezogene Daten (Art. 1 Buchst. a) und besondere personenbezogene Daten (Art. 8 Abs. 1) unterscheidet und auch Informationen, durch die eine Person nur indirekt bestimmbar ist, als personenbezogene Daten definiert, Art. 2 Buchst. a der Richtlinie. Daher wird die Konformität mit europäi-

schem Recht bezweifelt.[193] Weiter sind seitens der ARGE DATEN die Auskunftsrechte anderer Behörden nach § 8 BilDokG (alt) und die Möglichkeit kritisiert worden, mit Hilfe der Bildungsevidenzkennzahl und der Sozialversicherungsnummer doch die individuellen Daten einzelner Personen zu ermitteln.[194] Ungeachtet dessen wurde auch im Rahmen der Novelle 2008[195] an der Verwendung der Sozialversicherungsnummer festgehalten, aber dem BMUKK die gesetzliche Verpflichtung auferlegt, dem Nationalrat bis Ende 2009 einen Bericht über Alternativen zur Verwendung der Sozialversicherungsnummer vorzulegen.[196]

Nach der im in 2008 Jahre erfolgten Änderung des Gesetzes[197] werden die Daten nicht mehr unmittelbar von den Leitern der jeweiligen Institute an das BMUKK übermittelt, sondern an die Bundesanstalt „Statistik Österreich“ oder eine andere Einrichtung nach § 14 DSG, die dann die Sozialversicherungsnummer oder das Ersatzkennzeichen zur Bildungsevidenz-Kennziffer verschlüsselt und die auf diese Weise pseudonymisierten Daten an das BMUKK übermittelt. Damit erhält das Ministerium keine Kenntnis von der Sozialversicherungsnummer oder dem Ersatzkennzeichen. Ebenso sind die Abfragemöglichkeiten durch andere Behörden stark eingeschränkt worden, § 8 Abs. 1 und 2 BilDokG. In der Literatur werden die Änderungen positiv aufgenommen.[198] Die Weiterverwendung der Sozialversicherungsnummer als Identifikationsmerkmal ist aber auch nach der Novelle 2008 des BilDokG wie schon bei der Erstfassung des Gesetzes kritisiert worden. [199] Grundsätzlich wäre es möglich, mit Hilfe der Sozialversicherungsnummer die passende Bildungsevidenzkennziffer zu generieren und damit die betreffende Person zu identifizieren. Die beibehaltene Verwendung der Sozialversicherungsnummer wird vom Gesetzgeber damit begrün-

---

[193] Arning,Forgó,Krügel, Bildungsdokumentationen: Es geht auch datenschutzfreundlich, DuD 2008, S. 13ff (15).
[194] 2005/04/30 Was sind die zentralen Einwände der ARGE DATEN gegen das Bildungsdokumentationsgesetz? http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=52357ibol, letzte Abfrage 30.12.2011.
[195] BGBl I 2008/24.
[196] Wohlkinger in Bauer/Reimer (Hrsg.), Handbuch Datenschutzrecht, 2009, S. 278.
[197] Bundesgesetz, mit dem das Bildungsdokumentationsgesetz geändert wird, 259 d.P. (XXIII. GP), wurde am 05.12.2007 vom Nationalrat und am 20.12.2007 von Bundesrat beschlossen. Es wurde am 9. Januar 2008 im Bundesgesetzblatt verkündet (BGBl. I 24/2008; abrufbar unter: http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2008_I_24/BGBLA_2008_I_24.pdf, letzte Abfrage 30.12.2011.
[198] Arning,Forgó,Krügel, DuD 2008, S. 13ff, (S. 17).
[199] http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=19898ulr , letzte Abfrage 21.04,2012.

det, dass es der „Statistik Österreich“ sonst nicht möglich wäre, Verknüpfungen zu anderen Statistiken herzustellen. Das widerspricht aber dem E-Government-Gesetz, §§ 8,9 E-GovG,[200] das bereichsspezifische und keine übergreifenden Kennziffern vorsieht.[201]

Im Hinblick auf diese Kritik und die erwähnte Aufforderung des Gesetzgebers, dem Nationalrat bis Ende 2009 einen Bericht über Alternativen zur Verwendung der Sozialversicherungsnummer als bildungsspezifisches Personenkennzeichen vorzulegen, hat das BMUKK beim Institut für Rechtsinformatik der Leibniz Universität Hannover ein Gutachten in Auftrag gegeben, in dem mögliche Alternativen zur Sozialversicherungsnummer insbesondere unter datenschutzrechtlichen Aspekten ausführlich untersucht worden sind.[202]

Neben der Variante „Weiterverwendung der Sozialversicherungsnummer“ wurden die Verwendung eines bereichsspezifischen Personenkennzeicherns entsprechend dem EGovG, die Verwendung einer Schülermatrikelnummer sowie die Nutzung der ZMR-Zahl als Identifikationsmerkmal geprüft.

Im Falle der Nutzung eines bPK müsste dieses entweder bei den Schulen und/oder Universitäten vor Ort oder der Bundesanstalt „Statistik Österreich“ generiert werden. Im letzteren Falle würden die jeweiligen Datensätze unter Beteiligung der DSK als Stammzahlenregisterbehörde mit einen bPK ausgestattet werden. Da die Bundesanstalt Statistik Österreich das Kennzeichen „AS“ (Amtliche Statistik) verwendet, müsste die Weiterleitung der pseudonymisierten Datensätze an das BMUKK nach den Regeln des EGovG mittels dem Fremd-bPK „BF“ (Bildung und Forschung) erfolgen. Diese Variante wird von den Verfassern der Untersuchung vor allem deshalb als wenig geeignet angesehen, weil entsprechend weit verbreiteter Kritik die Aufgabenzuweisung als Stammzahlenregisterbehörde an die DSK mit deren sonstiger Funktion als unabhängiger Kontrollbehörde im Sinne von Art. 28 Abs. 1 DSRL für unvereinbar erachtet wird. Bei der Einführung der bPK in den Bildungseinrichtungen würden dort

---

[200] BGBl I 2008/7.
[201] Arning,Forgó,Krügel, aaO, S. 17.
[202] Egermann, Forgó, Kastelitz, Krügel, Reiners, Untersuchung von Alternativen zur Sozialversicherungsnummer in der Bildungsdokumentation, http://www.parlament.gv.at/PG/DE/XXIV/III/III_00102/imfname_176139.pdf, letzter Abruf 30.12.2011.

ein erheblicher Implementierungsaufwand und komplexe Fragen der Datensicherheit entstehen. Bei der Verbindung der Datensätze mit einer bPK erst bei der Bundesanstalt „Statistik Österreich“ sei weiterhin die Verwendung der Sozialversicherungsnummer am Schulstandort erforderlich. Insgesamt sei deshalb mit dieser Variante keine Verbesserung der datenschutzrechtlichen Situation gegenüber dem Status Quo zu erreichen.[203]

Weiter ist die Verwendung einer Schülermatrikelnummer untersucht worden. Dabei ist die Vergabe der Nummern durch eine Zentralstelle denkbar. Mit Rücksicht auf das Erfordernis der Kompatibilität mit den Registerzahldaten nach dem Registerzählungsgesetz müsste eine bPK-Zuordnungstabelle für die Statistik Österreich erstellt werden. Bei einer getrennten Erhebung der Daten für die Bildungsstatistik und die Registerzählung würden Matrikelnummern durch die jeweilige Bildungseinrichtung vergeben werden. Es wäre aber eine zusätzliche Datenerhebung der Bundesanstalt „Statistik Österreich“ für Zwecke der Registerzählung, der Bildungsstatistik und der jährlichen Feststellung der Volkszahl gemäß Finanzausgleichsgesetz mit der Sozialversicherungsnummer als Identifikator erforderlich. Nach Ansicht der Verfasser wäre bei Verwendung einer unabhängigen Schülermatrikelnummer zwar eine Verknüpfung mit anderen personenbezogenen Daten praktisch ausgeschlossen. Da aber eine Kompatibilität zur Registerzählung durch Matching-Tables oder eine Doppelzählung unter Verwendung der Sozialversicherungsnummer hergestellt werden müsse, ginge dieser Vorteil wieder verloren.[204]

Als weitere Variante wurde der unmittelbare Einsatz der ZMR-Zahl untersucht. Dagegen sprechen aber wegen der vielfältigen Möglichkeiten der Verknüpfung datenschutzrechtliche Gründe, aufgrund derer auch bereits im EGovG auf die unmittelbare Verwendung der ZMR-Zahl verzichtet wurde.

Bei der Variante Sozialversicherungsnummer als Identifikator ergibt sich, wie bereits oben ausgeführt, nach der Novellierung des Gesetzes im Jahre 2008 insofern eine Änderung als Daten der Schüler und Studenten von den Bildungseinrichtungen nicht mehr unmittelbar an das BMUKK übermittelt werden, sondern an die Bundesanstalt

---

[203] Egermann, Forgó u.a. aaO., S. 5, 22 ff.
[204] Egermann, Forgó u.a. aaO., S. 6/7, 37 ff.

“Statistik Österreich”, die die Daten dann ohne Namen und pseudonymisiert an das Ministerium für die Erstellung der Gesamtevidenzen weiterleitet. Die Sozialversicherungsnummer wird dabei in nicht-rückführbarer Weise in eine (BEKZ) umgeschlüsselt. Eine Verknüpfung der mit einer BEKZ codierten Daten mit anderen personenbezogenen Daten sei deshalb kaum denkbar, da dieser Indentifikator außerhalb des Bildungsbereiches nicht verwendet werde. Da die anderen beschriebenen Varianten unter datenschutzrechtlichen Gesichtspunkten keine Vorteile bieten, seien keine zwingenden Gründe für einen Wechsel gegeben. [205]

Das BMUKK hat sich das Ergebnis der beschriebenen Untersuchung zu Eigen gemacht und die Beibehaltung der Sozialversicherungsnummer als Identifikator auch im Bildungswesen verteidigt.[206]

5.2 Zusammenfassende Betrachtung der Identifizierung nach dem BilDokG

Es erscheint zunächst einmal verwunderlich, dass der Gesetzgeber einerseits mit dem EGovG im Interesse des Datenschutzes ein komplexes System der Identitätsfeststellung eingeführt hat, mit der eine bereichsübergreifende Zusammenführung von Daten einer Person verhindert werden soll und andererseits dann mit dem BilDokG eine Regelung verwirklicht, mit der eine für einen ganz anderen Bereich geschaffene, aber in vielen öffentlichen und privaten Einrichtungen eingesetzte Kennziffer, nämlich die Sozialversicherungsnummer, für die Identifizierung von Personen verwendet wird. Zwar wird die Sozialversicherungsnummer vor der Speicherung in Evidenzen in eine BEKZ verschlüsselt; für den, der den Schlüssel kennt, also z.B. die Bundesanstalt „Statistik Österreich“ und das BMUKK, ist es aber grundsätzlich möglich, eine Verbindung von bildungsrelevanten Daten einer Person mit anderen personenbezogenen Daten dieser Person über die Sozialversicherungsnummer herzustellen. Der Ordnung halber muss man einräumen, dass zum Zeitpunkt des Inkrafttretens des BilDokG im Jahre 2002 das EGovG noch nicht existierte, das erst 2004 in Kraft gesetzt wurde. Dennoch stellt sich die Frage, ob es im Interesse des Datenschutzes und der Einheitlichkeit des Identifizierungsverfahrens in Österreich nicht sinnvoll ist, auch für den Bildungsbereich, dem das bPK „Bildung und Forschung

---

[205] Egermann, Forgó u.a. aaO., S. 5, 53.
[206] http://www.parlament.gv.at/PG/DE/XXIV/III/III_00102/imfname_176139.pdf, letzter Abruf 30.12.2011.

(BF)“ zugeordnet ist, das Identifizierungsverfahren nach dem EGovG einzuführen. Die Sozialversicherungsnummer ist ursprünglich ausschließlich für den Bereich der Sozialversicherung als Kontonummer für Sozialversicherungsdaten eingeführt worden. Sie besteht aus einer vierstelligen Nummer, die durch das Geburtsdatum mit sechs Stellen ergänzt wird.[207] Sie wurde und wird nach wie vor bei einer Vielzahl von Verwaltungsaufgaben eingesetzt. Neben den bereits genannten Einrichtungen Sozialversicherung, BMUKK, „Statistik Österreich“, wird diese Kennzeichnung u.a. von den Gesundheitsdiensten, den Finanzbehörden, den Bausparkassen und den Arbeitgebern verwendet.

Der Hauptverband der Sozialversicherungsträger hat darauf aufmerksam gemacht, dass die Kennzeichnung als Identifikator wenig geeignet ist, weil nicht alle natürlichen Personen in Österreich eine Sozialversicherungsnummer haben (u.a. nicht die Beamten, Lehrer und ausländische Schüler und Studenten), manchmal mehrfach Nummern vergeben werden und die Bildung von Ersatzkennzeichen sich nicht bewährt habe. Durch das E-Government-Gesetz, BGBl. I Nr. 10/2004, sei ein neues Konzept für die Verwaltung von Personendaten eingeführt worden. Das Bildungsdokumentationsgesetz sollte sich nach dem E-Government richten, wie es ansatzweise bereits im § 3 Abs. 7 des Entwurfes in die Wege geleitet sei.[208] Bei Kenntnis des Geburtsdatums einer Person kann auch leicht eine Sozialversicherungsnummer gefälscht werden, da die entsprechenden Algorithmen im Internet zugänglich sind.[209]

In dem erwähnten Gutachten des Institutes für Rechtsinformatik der Leibniz Universität Hannover wird zwar die Verwendung einer ausschließlich für den Bildungsbereich eingesetzten Kennung als die datenschutzrechtlich optimale Lösung bezeichnet, weil damit ein technisch völlig unabhängiges, mit der Kennzeichnung in anderen Verwaltungsbereichen nicht kompatibles Kennzeichen verwendet und auch eine Zusam-

---

[207] Egermann, Forgó u.a. aaO., S.16.

[208] Stellungnahme des Hauptverbandes der Sozialversicherungsträger zum Entwurf eines Bundesgesetzes über die Dokumentation im Bildungswesen, 7/SN-236/ME 21. GP, 1 f, http://www.parlament.gv.at/PG/DE/XXI/ME/ME_00236_07/fname_000000.pdf, letzte Abfrage 30.12.2011; Stellungnahme des Hauptverbandes der Österreichischen Sozialversicherungsträger zu dem Ministerialentwurf betreffend ein Bundesgesetz, mit dem das Bildungsdokumentationsgesetz geändert wird, abrufbar unter http://www.parlament.gv.at/PG/DE/XXIII/ME/ME_00080_30/fname_087015.pdf, letzte Abfrage 30.12.2011.

[209] Egermann, Forgó u.a. aaO., S. 17.

menführung von Daten aus anderen Bereich unterbunden werden würde.[210] Im Hinblick auf die Anforderungen des Registerzählungsgesetzes, durch das regelmäßige Volkszählungen vermieden werden sollen, und die Notwendigkeit der Verknüpfung mit Altdaten bei der Verlaufsstatistik werden jedoch praktische Schwierigkeiten gesehen. Es müssten zusätzliche Identifikatoren eingeführt werden, um die Anforderungen der Registerzählung und der Statistik zu erfüllen. Damit würden jedoch unerwünschte Datenverknüpfungen möglich werden, so dass aus datenschutzrechtlicher Sicht keine Verbesserung im Vergleich zum bestehenden System eintreten würde.[211]

Die Verwendung von bereichsspezifischen Personenkennzeichen wird zwar als datenschutzrechtlich zulässig, aber im Vergleich zu einer unabhängigen eigenständigen Nummerierung für das Bildungswesen als weniger datenschutzfreundlich angesehen. Durch die einheitliche Verwendung der Stammzahl sei die Zusammenführung von Daten aus verschiedenen Verwaltungsbereichen im Vergleich zu der letztgenannten Option nicht völlig ausgeschlossen, so dass bei einer solchen Lösung im Vergleich zum Status Quo möglicherweise mehr Nachteile als Vorteile entstünden. Es sei auch zu bedenken, dass das BMI derzeit als Dienstleister für die Stammzahlenregisterbehörde DSK fungiere.[212]

Der Datenschutzrat hat sich in seiner Sitzung am 22.02.2010 mit der zitierten Untersuchung von Alternativen zur Sozialversicherungsnummer in der Bildungsdokumentation befasst. Er vertritt die Ansicht, dass in der Bildungsdokumentation bereichsspezifische Personenkenzeichen, bPKs, vorgesehen werden sollten, was auch der E-Government-Strategie des Bundes entsprechen würde. Die in dem Gutachten geäußerten datenschutzrechtlichen Bedenken gegen bPKs im Hinblick auf Datenverknüpfungen mit anderen Bereichen sowie die Möglichkeit einer Reidentifizierung über die DSK hält er nicht für gerechtfertigt. Die Probleme lägen in der Verwendung der Sozialversicherungsnummer in der Bildungsdokumentation. Die Sozialversicherungsnummer sei kein sicherer Schlüssel und eine Vielzahl von Personen könne auf „legaler“ Grundlage darauf zugreifen. Bei dem Inkrafttreten des BilDokG existierte das EGovG noch nicht. Nunmehr seien aber in Österreich E-Government-Lösungen ent-

---

[210] Egermann, Forgó u.a. aaO., S. 52.
[211] Egermann, Forgó u.a. aaO., S. 40/41.
[212] Egermann, Forgó u.a. aaO., S. 52.

wickelt worden, um die Sozialversicherungsnummer nicht als universelles Personenkennzeichen für Bereiche zu verwenden, die keinen Bezug zur Sozialversicherung haben. Aus diesen Gründen ersuche der Datenschutzrat das BMUKK, ein Konzept für eine mittelfristige Umsetzung der Verwendung bereichsspezifischer Personenkennzeichen in der Bildungsdokumentation vorzubereiten und dieses dem Datenschutzrat zukommen zu lassen.[213] Auch im Nationalrat selbst geht die Diskussion über die Frage weiter. In einem Entschließungsantrag vom 24.03.2010 haben mehrere Abgeordnete das BMUKK aufgefordert, dem Nationalrat einen Gesetzesvorschlag vorzulegen, der die Einführung einer bereichsspezifischen Bildungskennzahl in der Bildungsdokumentation vorsieht.[214]

Die von den Gutachtern gegen die Verwendung von bereichsspezifischen Personenkennzeichen vorgebrachten Bedenken stellen im Grunde das gesamte Konzept des EGovG in Frage. Wenn aufgrund der technischen Konstruktion, der Doppelfunktion der DSK und der Tätigkeit des BMI als Dienstleister für die DSK in ihrer Funktion als Stammzahlenregisterbehörde die Gefahr einer unzulässigen Zusammenführung von Daten gesehen wird, dann müsste man wohl die E-Government-Strategie der Bundesregierung anzweifeln.

Das Grundkonzept, durch eine „unabhängige Behörde“ aus der ZMR-Nummer eine virtuelle Stammzahl zu generieren, zu verschlüsseln und daraus bereichsspezifische Personenkennzeichen zu bilden, um eine Zusammenführung von Daten aus verschiedenen Bereichen zu vermeiden, erscheint schlüssig. Problematisch erscheint der Umstand, dass die Datenschutzkommission, deren Unabhängigkeit wegen ihrer organisatorischen Einbindung in das Bundeskanzleramt ohnehin kritisiert wird, als Stammzahlenregisterbehörde fungiert und sich in Bezug auf diese Funktion gewissermaßen selbst kontrolliert. Wie bereits in Kapitel 4.5 dargestellt, erscheint auch der Zuschnitt der Bereiche nach der BereichsabgrenzungsVO zum Teil recht grob, so dass in gewissen Umfang eine Verknüpfungsmöglichkeit von Daten aus Verwaltungsbereichen entsteht, die unterschiedliche Aufgaben wahrnehmen. Weiter können

---

[213] Stellungnahme des Datenschutzrates zur Untersuchung von Alternativen zur Sozialversicherungsnummer in der Bildungsdokumentation, http://www.bka.gv.at/DocView.axd?CobId=38592, letzte Abfrage 30.12.2011.

[214] http://www.parlament.gv.at/PG/DE/XXIV/A/A_01031/fname_182182.pdf, letzte Abfrage 30.12.2011.

sich bPKs, die bereichsübergreifend verwendet werden (wie z.B. das bPK für den Bereich Zustellung), zu einem alle Bereiche umfassenden Personenkennzeichen entwickeln. [215]

Diese Kritiken sind berechtigt. Aber sie betreffen nicht den Kern der österreichischen E-Goverment-Strategie im EGovG für die Identifizierung der Bürger. Diese ist, wie erwähnt, dadurch gekennzeichnet, dass aus der Nummer im Zentralen Melderegister (ZMR-Zahl) bzw. einer Nummer im Ergänzungsregister, wenn keine ZMR-Zahl besteht, mittels Verschlüsselung eine Stammzahl abgeleitet wird, die jedoch nicht gespeichert wird. Aus ihr wird mittels einer nicht-rückführbarer Einwegfunktion ein bPK errechnet. Wenn eine Verwaltungsbehörde für ihre gesetzlichen Aufgaben personenbezogene Daten aus einem anderen Bereich benötigt, muss sie von der Stammzahlenregisterbehörde ein sogenanntes Fremd-bPK anfordern, das jedoch verschlüsselt wird und nur von der anzufragenden Behörde entschlüsselt werden kann. Diese hat dann zu prüfen, ob die anfragende Behörde legitimiert ist und der mit der Anfrage verfolgte Zweck mit dem der ursprünglichen Erhebung der relevanten Daten vereinbar ist, §§ 6 Abs. 1 Ziffer 2, 7 Abs. 2 DSG 2000.

Wenn diese Kernbedingungen eingehalten und die beschriebenen Schwachpunkte beseitigt werden, bestehen gegen Verwendung von bPKs im Bildungsbereich keine datenschutzrechtlichen Bedenken. Erforderlich ist jedoch eine verbesserte Zuweisung von bPKs in der BereichsabgrenzungsVO, durch die nicht unterschiedliche Funktionen in einem Bereich zusammengefasst werden. Außerdem sollte die bereichsübergreifende Nutzung von pPks für eine Datenverkettung verhindert werden. Der Gesetzgeber ist dazu aufgerufen, entsprechende Verbesserungen des Konzeptes umzusetzen. Außerdem wäre es sinnvoll, die DSK nicht mit der Verwaltung der Stammzahlen zu betrauen, sondern eine selbständige und unabhängige Behörde. In jedem Fall müsste die Unabhängigkeit der DSK gestärkt werden. U.U. Vollzieht sich insoweit durch Druck seitens der Europäischen Kommission oder des EuGH im Rahmen der laufenden Verfahren eine Änderung.

---

[215] Straus, Datenschutzimplikationen staatlicher Identitätsmanagement-Systeme, DuD 2010, S. 99 ff. (102).

Die Verfasser des Gutachtens des Institutes der Leibniz Universität Hannover begründen ihr Votum für die Beibehaltung der Sozialversicherungsnummer als Identifkationsmerkmal im Bildungswesen u.a. auch mit dem Umsetzungsaufwand, der mit einer Umstellung auf bPKs verbunden wäre, weil der Behörde, die diese Aufgabe übernimmt, ein zusätzlicher Aufwand durch Ermittlung der bPKs bei der Stammzahlenregisterbehörde entsteht.[216] Dieser Einwand ist sicher zutreffend. Auf der anderen Seite würde die weitere Nutzung der Sozialversicherungsnummer die Fehlentwicklung fortsetzen, die mit dem Einsatz dieses Kennzeichens außerhalb des Bereiches der Sozialversicherung verbunden ist und deren immanente Schwächen fortschreiben. Soweit bekannt, soll die Anwendung des EGovG nicht auf die derzeit von der BereichsabgrenzungsVO erfassten 26 Bereiche beschränkt bleiben, sondern allmählich ausgedehnt werden. Es wird also ein einheitliches Konzept der Identifizierung in der öffentlichen Verwaltung in Österreich angestrebt. In dem erwähnten Gutachten wird ungeachtet gewisser datenschutzrechtlicher Bedenken auch eingeräumt, dass für die Verwendung von bPks auch im Bildungswesen im Interesse einer Vereinheitlichung des E-Government in Österreich gute Gründe sprechen können.[217]

Ein weiterer Punkt ist die Kompatibilität des österreichischen Identifizierungssystems mit Systemen der EU oder anderer Mitgliedsländer. Nach bisherigem Kenntnisstand verwendet kein anderes Land ein vergleichbares System, so dass sich die Frage stellt, ob im Rahmen länderübergreifender transaktionsorientierter Onlineanwendungen eine eindeutige Identifizierung österreichischer Bürger möglich ist. Dabei hilft die Funktionalität der Bürgerkarte, die die Stammnummer der betreffenden Person enthält, welche aus Sicherheitsgründen mit einer Signatur der Melderegisterbehörde versehen ist. Die Stammnummer wird bei der Registrierungsstelle mit dem Signaturzertifikat der Bürgerkarte verknüpft. Wenn im Rahmen eines transaktionsorientierten Onlinedienstes eine eindeutige Identifizierung des Nutzers notwendig wird, so kann der Anbieter beim zentralen Melderegister auf der Basis des öffentlichen Signaturschlüssels der Bürgerkarte eine entsprechende Abfrage tätigen. Ihm werden dann die benötigten Identitätsdaten (nicht aber Stammnummer und ZMR-Nummer) übermittelt. Somit kann das Signaturzertifikat der Bürgerkarte sowohl zur Authentifizie-

---

216 Egermann, Forgó u.a. aaO., S. 26 f..

217 Egermann, Forgó u.a. aaO., S. 53.

rung als auch zur Signatur verwendet werden.[218] Allerdings ist die Bürgerkarte noch nicht allgemein verbreitet, weil ihre Nutzung freiwillig ist. Mit zunehmender Inanspruchnahme gewinnt sie jedoch auch an Bedeutung für die Identifizierung bei länderübergreifende Anwendungen.

5.3 Beachtung datenschutzrechtlicher Kriterien

Nach Art. 1 Abs. 2 DSG 2000 ist für jede Verwendung personenbezogener Daten durch eine Behörde, die ohne Einwilligung des Betroffenen erfolgt, eine gesetzliche Grundlage erforderlich, die den Anforderungen von Art. 8 Abs. 2 EMRK genügt. Danach muss der Eingriff einer Behörde eine Maßnahme darstellen, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.
Mit dem Gebot der Erforderlichkeit bei der Verarbeitung personenbezogener Daten hat sich der EuGH u.a. in einer Entscheidung zum deutschen Ausländerzentralregister mit Bezug auf Art. 7 Buchst. e DSRL auseinandergesetzt.[219] Nach dieser Bestimmung der Richtlinie ist die Verarbeitung personenbezogener Daten nur zulässig, wenn sie für die Wahrnehmung einer Aufgabe erfolgt, die in öffentlichem Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde. Er hat dazu weiter ausgeführt, dass der Begriff der „Erforderlichkeit“ mit Rücksicht auf die Gewährleistung eines einheitlichen Schutzniveaus in der EU in den einzelnen Mitgliedstaaten keinen variablen Inhalt haben könne. Es handele sich um einen autonomen Begriff des Gemeinschaftsrechts, der so auszulegen sei, dass er in vollem Umfang dem Ziel dieser Richtlinie, wie in ihrem Art. 1 Abs. 1 definiert wird, entspreche.

Es erscheint allerdings fraglich, ob EU-Recht für die Beurteilung der datenschutzrechtlichen Zulässigkeit des BilDokG zu berücksichtigen ist, weil dieses Gesetz Be-

---

[218] Hoye, Digitale Identitäten im Kontext von E-Government-Anwendungen, 2010, S. 51 f..
[219] Urteil des EuGH vom 20.05.2003 C-524/06, ABl. C 171/ vom 19.07.2003, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006CJ0524:DE:HTML, letzte Abfrage 30.12.2011.

standteil des nationalen Rechts ist und auch nicht in Umsetzung von Gemeinschaftsrecht erlassen wurde. Zwar hat der EuGH den Anwendungsbereich der DSRL in der Vergangenheit weit ausgelegt und auch auf Sachverhalte angewendet, bei denen kein unmittelbarer Zusammenhang mit den durch den EG-Vertrag garantierten Grundfreiheiten besteht.[220] Mit Inkrafttreten des Lissabon-Vertrages und der GRCh am 01.12.2009 gilt auch die ausdrückliche Schrankenregelung gemäß Art. 51 Abs.1 GRCh, nach der die Grundrechte der Charta, u.a. auch das Grundrecht auf Datenschutz gemäß Art. 8 der Charta, nur für die Organe der Union und die Mitgliedstaaten ausschließlich bei der Durchführung von Gesetzen der Union Anwendung findet. Das Recht auf Datenschutz ergibt sich auch aus Art. 16 Abs. 1 AEUV. Insoweit gilt die Schrankenregelung des Art.16 Abs. 2 AEUV.

Uneingeschränkt anwendbar ist jedoch die EMRK. Darüber hinaus wird in § 1 Abs. 2 DSG ausdrücklich auf Art 8 Abs. 2 EMRK Bezug genommen. Anders als die GRCh enthält die EGMK keine ausdrückliche Regelung zum Datenschutz. Der EGMR hat den Datenschutz in seiner Rechtsprechung auf der Grundlage von Art. 8 Abs. 1 EMRK als spezifisch ausgestalteten Teilbereich des Rechts auf Achtung der Privatsphäre entwickelt.[221] In dem Urteil Marper gg. Vereinigtes Königreich[222] sind die Datenschutzprinzipien der Verhältnismäßigkeit der Erforderlichkeit und der Zweckbindung noch einmal betont worden. Danach muss die Aufbewahrung von Daten zu dem Zweck, zu dem sie angelegt wurden, verhältnismäßig und zudem zeitlich begrenzt sein. Der EGMR räumt den Staaten bei Eingriffen in die Privatsphäre einen gewissen Ermessenspielraum ein und prüft jeweils, ob im konkreten Fall die Gründe, die zur Rechtfertigung des Eingriffs angeführt werden, maßgeblich und ausreichend sind und ob die Maßnahme gegenüber dem verfolgten Ziel angemessen ist.[223] Nach der Rechtsprechung des EGMR bedeutet das Wort „notwendig“ in Art. 8 Abs. 2 EMRK, dass ein zwingendes gesellschaftliches Bedürfnis besteht und die Maßnahme

---

[220] zuletzt im Fall der vom österreichischen Rechnungshof veröffentlichten Gehaltsdaten, EuGH C-465/00, C-138/01, C-139/01

[221] EGMR, Urteil vom 26.03.1987, Leander gegen Schweden, Nr. 10/1985/96/144 Serie A 116, EGMR-E 3 , S. 430.

[222] EGMR Urteil vom 04.12.2008, EuGRZ 2009, S 299.

[223] EGMR, Urteil vom 02.08.2001, Nr. 54273/00 (Boultif), InfAuslR 2001, S. 476; EGMR Urteil vom 05.07.2005, Nr. 46410/99 (Üner), DVBl. 2006, S. 688.

in angemessenem Verhältnis zum dem verfolgten Zweck stehen muss.[224] Gesetzliche Bestimmungen, die Eingriffe nach Art. 8 Abs. 2 EMRK zulassen, müssen hinreichend bestimmt sein. Bei einer Datei ist zu regeln, unter welchen Umständen sie angelegt wird. Das Verfahren und die Informationen, die gesammelt werden, müssen bestimmt sein, ebenso die Dauer der Aufbewahrung und die Löschung der Daten.[225]

Bei der Prüfung, inwieweit das BilDokG diese Anforderungen erfüllt, wird zunächst der mit dem Gesetz verfolgte Zweck betrachtet. Nach § 1 Ziff. 1 BilDokG soll das Gesetz die Verwendung von Daten der Schüler und Studierenden durch die jeweiligen Bildungseinrichtungen entsprechend dem DSG 2000 regeln, nach der Ziffer 2 dieser Bestimmung die Führung der Gesamtevidenzen der Schüler bzw. der Studierenden für ausschließlich statistisch-planerische und steuernde Zwecke, nach Ziffer 3 die Verwendung der Daten aus den Evidenzen der Bildungseinrichtungen für Zwecke der Bundesstatistik zum Bildungswesen und des Bildungsstandsregisters, die von der Bundesanstalt „Statistik Österreich“ besorgt werden.

5.3.1 Erforderlichkeit der Datenverwendung

Bei der Prüfung der Erforderlichkeit ist zwischen der Speicherung in den Bildungseinrichtungen, im BMUKK und bei der Bundesanstalt „Statistik Österreich“ zu differenzieren.

Da sensible Daten und die Sozialversicherungsnummer nach zwei Jahren in den lokalen Evidenzen gelöscht werden, erscheint die lange Speicherdauer der weiteren personenbezogenen Daten, die bis zur Pensionierungsgrenze der betreffenden Personen andauern kann, im Hinblick auf die verfolgten Zwecke, z.B. die Ausstellung von Zweitschriften von Zeugnissen bei einem Verlust der Urschrift, vertretbar. Dabei ist auch zu berücksichtigen, dass die einzelnen Bildungseinrichtungen mangels Zugang zu anderen Datenquellen kaum die Möglichkeit haben, ihre Daten mit anderen zu verknüpfen und Profile zu bilden.

---

[224] EMRK, Urteil vom 24.11.1986 (Gillow gg. Vereinigtes Königreich), Serie A Nr. 109, § 55, EGMR-E 3, 306.
[225] EMRK, Urteil vom 16.02.2000, Amann gegen Schweiz, Slg. 2000 – II Nr. 76 ff, ÖJZ 2001, S. 71.

Eine andere Frage ist, ob der Umfang der für die Gesamtevidenzen im BMUKK erhobenen Daten in einer demokratischen Gesellschaft für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist. Wie erwähnt, räumt der EGMR den Nationalstaaten bei der Anwendung dieser Vorschrift einen gewissen Ermessensspielraum ein, der umso größer ist, je geringer der staatliche Eingriff in die Privatsphäre durch die Datenerhebung ausfällt. Aber nicht nur die Intensität des Eingriffs und die Bedeutung der Daten für den Kern der Persönlichkeit ist maßgeblich, sondern auch das vom Konventionsstaat verfolgte Ziel. Bei Maßnahmen zur nationalen Sicherheit gesteht der Gerichtshof den Konventionalstaaten einen weiten Ermessensspielraum zu.[226] Letztendlich geht es um die Frage, ob die staatlichen Maßnahmen, hier die Datenerhebungen für die Gesamtevidenzen im Rahmen der Bildungsdokumentation, im Hinblick auf die verfolgten Ziele verhältnismäßig sind. Der Begriff der Notwendigkeit in einer demokratischen Gesellschaft ist in diesem Zusammenhang einerseits nicht so zu verstehen, dass der nationale Gesetzgeber nur eine bestimmte Lösung wählen darf. Andererseits darf die Lösung nicht nur angemessen oder nützlich erscheinen, sondern die zu beurteilende Notwendigkeit setzt das Vorliegen eines dringenden sozialen Bedürfnisses für den fraglichen Eingriff und dessen Verhältnismäßigkeit in Bezug auf das verfolgte legitime Ziel voraus.[227] Dabei ist zu berücksichtigen, dass Art. 8 Abs. 2 EMRK eine Ausnahmeregelung zu Abs. 1 darstellt, die grundsätzlich eng auszulegen ist. Dies ist bei der Prüfung der Verhältnismäßigkeit zu berücksichtigen. U. a. dürfte die Verhältnismäßigkeit dann nicht gegeben sein, wenn die mit dem Eingriff verfolgten Ziele sich mit anderen weniger eingriffsintensiven Maßnahmen erreichen lassen. Nach der Rechtsprechung des Verfassungsgerichtshofes zur Verhältnismäßigkeit müssen folgende Voraussetzungen erfüllt sein: Das Ziel der Regelung muss im öffentlichen Interesse liegen. Die Regelung muss zur Erreichung des Zieles geeignet sein. Zur Verfolgung des Zieles muss ein möglichst schonendes Mittel eingesetzt werden. Zwischen öffentlichem Interesse

---

[226] Grote/Maraun EMRK/GG Konkordanzkommentar zum europäischen Grundrechtsschutz, 2006, § 8 Anm. 92.
[227] Wildhaber/Breitenmoser in Karl (Hrsg.) Internationaler Kommentar zur Europäischen Menschenrechtskonvention Stand 2010, Art. 8 Anm. 711.

und der durch einen Eingriff verkürzten Grundrechtsposition des Betroffenen muss eine angemessene Relation bestehen.[228]

Das BMUKK hat die aufwendige und umfangreiche Datensammlung für die Gesamtevidenzen in allen Bildungseinrichtungen damit gerechtfertigt, dass den Entscheidungsträgern für das Gestalten von Bildung die notwendigen Grundlagen an die Hand gegeben werden müssten. Für bildungsbezogene Steuerungs- und Planungsaufgaben seien in der Vergangenheit immer auch Daten verwendet worden, die aus den Auswertungen von Volkszählungen stammten. Solche Zählungen werde es nach der Volkszählung im Jahre 2001 nicht mehr geben. Das Auslaufen der Volkszählungen sei eine Folge der technischen Entwicklung der letzten Jahre. Sie mache es nicht länger erforderlich, Daten über periodisch wiederkehrende, aufwendig zu organisierende und letztlich auch teure Befragungen von auskunftspflichtigen Personen mittels umfangreicher Fragebögen zu erheben. An ihre Stelle treten Register und Dateien von Behörden, auf die unter genau geregelten Bedingungen, die in erster Linie dem Datenschutz dienten, zugegriffen werden könne. Die im BilDokG vorgesehene Gesamtevidenz der Schüler sei ein solches Register.[229] Ungeachtet dieser Argumente ist zu prüfen, ob für die Erreichung der im BilDokG genannten Ziele nicht gelindere Mittel im Sinne von § 1 Abs. 2 DSG 2000, letzter Satz, zur Verfügung stehen

Bei der Frage, ob weniger eingriffsintensive und weniger aufwendige Maßnahmen denkbar sind, soll ein Blick auf europäische Vorgaben und Vorschläge gerichtet werden. Insoweit ist die Verordnung (EG) Nr. 452/2008 des Europäischen Parlaments und des Rates vom 23. 04. 2008 über die Erstellung und die Entwicklung von Statistiken über Bildung und lebenslanges Lernen von Interesse. Mit dieser Verordnung wird ein gemeinsamer Rahmen für die systematische Erstellung von gemeinschaftlichen Statistiken über Bildung und lebenslanges Lernen geschaffen, § 1 der genannten VO. Die Maßnahmen zur Durchführung der Verordnung sind in einem Anhang

---

[228] VfGH vom 16.03.2001, Az.: G 94/00, Sammlungsnummer 16150.
[229] Rundschreiben Nr. 7/2004, 1. Die Zielsetzung des Bildungsdokumentationsgesetzes (BilDokG), http://www.bmukk.gv.at/ministerium/rs/2004_07.xml, letzte Abfrage 16.01.2012.

dazu beschrieben. Danach sind neben der Nutzung von vorhandenen Verwaltungsdaten Stichprobenerhebungen mit maximal 5000 Beteiligten vorgesehen.[230]

Wenn man berücksichtigt, dass derartige Erhebungen nicht unbedingt alle Jahre zu erfolgen haben und welcher Umfang an Daten nach dem BilDokG alljährlich in allen österreichischen Bildungseinrichtungen erfasst und übermittelt werden muss (siehe dazu §§ 6 Abs. 2 und 3, 7 Abs. 2 und 3 BilDokG, Anhang 1 zum BilDokG) erscheint eine Stichprobenerhebung nach europäischen Vorgaben als weniger eingriffsintensiv und weniger aufwendig. Es sind also Zweifel angebracht, ob die Vorschriften über die Erhebung der Daten für die Gesamtevidenzen der Schüler-innen und Student-innen mit den österreichischen Verfassungsbestimmungen zum Datenschutz in Einklang stehen. Diese Zweifel werden auch nicht dadurch relativiert, dass es sich bei den in den Daten für die Gesamtevidenzen lediglich um indirekt-personenbezogene Daten im Sinne von § 4 Ziff. 1 DSG 2000 handelt. Einmal erscheint es, wie oben erläutert, zweifelhaft, ob die Vorschrift des § 8 Abs. 2 DSG 2000, der für diese Art von Daten ein Geheimhaltungsinteresse verneint, europarechtskonform ist. Die Differenzierung zwischen personenbezogenen Daten und indirekt personenbezogenen Daten in § 4 Ziffer 1 DSG 2000 ist kritisch zu sehen, weil nach der Datenschutzrichtlinie (siehe Art. 2 Buchst. a DSRL) auch indirekt personenbezogene Daten vom Datenbegriff der Richtlinie erfasst werden. Wie sich aus Erwägungsgrund Nr. 26 der DSRL ergibt, gelten die Schutzprinzipien der Richtlinie für alle Informationen über eine bestimmte oder bestimmbare Person. Die Schutzprinzipien finden nur dann keine Anwendung, wenn die Daten derart anonymisiert (nicht nur pseudonymisiert, Anm. d. Verf.) sind, dass die betreffende Person nicht mehr identifizierbar ist. Die Einschränkung der mangelnden Bestimmbarkeit mit rechtlich zulässigen Mitteln, wie in § 4 Ziffer 1 DSG 2000 geschehen, wird in der Richtlinie nicht vorgenommen, so dass die Bestimmungen des DSG 2000 in Bezug auf den verminderten Schutz von nur indirekt personenbezogenen Daten für den Anwendungsbereich der Richtlinie unbeachtlich sind. Unter Berücksichtigung der neuen Schrankenbestimmungen des Lissabon-Vertrages könnte man argumentieren, dass diese Schlussfolgerungen nicht für reine nationalstaatliche Regelungen wie das BilDokG gelten. Es handelt sich dabei jedoch um

---

[230] ABl. 2008 L 145/233.

grundsätzliche Überlegungen zum Begriff der Personaldaten, die auf einem allgemeinen europäischen Verständnis des Grundrechts auf Datenschutz beruhen und auch bei der Anwendung und Auslegung des Art. 8 EMRK zu berücksichtigen sind.

Zum anderen ist es bei Kenntnis des betreffenden Algorithmus leicht möglich, aus der Sozialversicherungsnummer die BEKZ zu generieren und Verknüpfungen herzustellen. Außerdem erfolgt bei jeder neuen Datenerhebung in jedem Jahr eine Reidentifikation, weil jedes Mal aus der Sozialversicherungsnummer die bereits bekannte BEKZ neu generiert wird.

Das BMUKK argumentiert u.a. auch mit Notwendigkeit, Daten für die Registerzählung an Stelle der weggefallenen Volkszählung schaffen zu müssen. Von einer Verwendung der Daten der Gesamtevidenzen für die Registerzählung ist im BilDokG bei der Beschreibung des Gesetzeszweckes aber keine Rede. Hier ergeben sich auch Fragen einer (un)zulässigen Verknüpfung bzw. Übermittlung, weil die Daten außerhalb der ursprünglichen Zweckbestimmung verwendet werden. Im Rahmen eines grundgesetzlich gewährten Schutzes dürfen aber verwaltungstechnische Opportunitätsüberlegungen nicht in den Vordergrund gestellt werden. Die Lösung muss nicht nur sinnvoll, sondern zwingend erforderlich sein.

5.3.2 Löschung von personenbezogenen Daten

Nach § 8 Abs. 5 BilDokG sind die in den lokalen Evidenzen enthaltenen Sozialversicherungsnummern bzw. Ersatzkennzeichen und eine Reihe anderer personenbezogener Daten spätestens zwei Jahre nach dem Abgang der betreffenden Schüler oder Studenten von der Bildungseinrichtung zu löschen, die restlichen nach Maßgabe der schul- bzw. hochschulrechtlichen Bestimmungen zu einem späteren Zeitpunkt. Dies betrifft beispielsweise personenbezogene Daten, die für die Ausstellung von Zweitschriften der Zeugnisse benötigt werden. Sie sind so lange zu speichern wie dies durch die Verordnung über die Aufbewahrungsfristen von in den Schulen zu führenden Aufzeichnungen[231] vorgesehen ist. Für einen Teil der Daten kann die Speicherung also bis zur Pensionierung andauern. Im Hinblick auf das Erfordernis, auch

[231] Verordnung über die Aufbewahrungsfristen von in den Schulen zu führenden Aufzeichnungen, BGBl. I 1978, 419.

nach längerer Zeit Zweitschriften von Zeugnissen erstellen zu können, erscheinen die Aufbewahrungsfristen für den genannten Zweck vertretbar.
Hinsichtlich der in den Gesamtevidenzen verarbeiteten Daten ist keine gesetzliche Höchstgrenze der Aufbewahrung vorgesehen. Das wird nicht für notwendig erachtet, weil es sich bei diesen Daten um indirekt personenbezogene Daten handele. Da die Datensätze durch die Bundesanstalt „Statistik Österreich“ mittels BEKZ nicht rückführbar verschlüsselt werden, werden lediglich pseudonymisierte Daten verarbeitet und gespeichert.[232] Unter europarechtlichen Gesichtspunkten führt die Pseudonymisierung aber nicht zu einer Einschränkung des Schutzes, weil es sich um personenbezogene Daten einer bestimmbaren Person handelt. Unabhängig davon kann man davon ausgehen, dass der mit dem Gesetz angestrebte Zweck erfüllt ist, wenn die einzelnen Datensätze zu Gesamtevidenzen verarbeitet worden sind. Unter Berücksichtigung des strengen Zweckprinzips besteht aufgrund § 1 Abs. 3 Ziffer und Abs. 4 DSG ein Anspruch auf Löschung von personenbezogenen Daten, wenn sie für die Verfolgung des ursprünglichen Zweckes nicht mehr erforderlich sind.[233] Auch nach der Rechtsprechung des VfGH sind personenbezogene Daten zu löschen, sobald sie für die Erfüllung der Aufgabe, für die sie verwendet worden sind, nicht mehr benötigt werden, es sei denn, für ihre Löschung wäre eine besondere Regelung getroffen worden.[234]

Bei den für die Erstellung der Gesamtevidenzen im BMUKK gespeicherten Daten ist im Übrigen auch unter Berücksichtigung der Abfragemöglichkeiten gemäß § 8 Abs. 1 BilDokG nicht erkennbar, warum diese praktisch unbegrenzt aufbewahrt werden müssen. In dieser Bestimmung ist zwar vorgesehen, dass der BMUKK Schulbehörden des Bundes zum Zwecke der Erfüllung der ihnen gesetzlich übertragenen Aufgaben Abfrageberechtigungen auf die in den Gesamtevidenzen verarbeiteten Daten in der Weise erteilen kann, dass ein Rückschluss auf Angaben zu einzelnen Personen nicht möglich ist. Aber es ist kein Grund ersichtlich, weshalb Daten für derartige

---

[232] Arning, Forgó, Krügel, Bildungsdokumentationen: Es geht auch datenschutzfreundlich, DuD 2008, S. 17.
[233] Jahnel, Handbuch Datenschutzrecht, 2010, Kapitel 7, Rd.-Nr. 65; Mayer-Schönberger/Bradl, Datenschutzgesetz, 2. Auflage 2005, S. 39.
[234] VfGH vom 16.03.2001, Az.: G 94/00, Sammlungsnummer 16150, http://www.ris.bka.gv.at/Dokumente/Vfgh/JFR_09989684_00G00094_01/JFR_09989684_00G00094_01.pdf, letzte Abfrage 16.01.2012.

Abfragen Jahrzehnte vorgehalten werden müssen. Datensammlungen auf Vorrat sind grundsätzlich unzulässig. Mit zunehmender Dauer der Aufbewahrung verringert sich auch der Erkenntniswert der Daten für die gesetzlich vorgesehenen Zwecke der statistischen Planung und Steuerung im Sinne von § 1 Ziffer 2 BilDokG. Zu dem Argument des BMUKK, im Rahmen der Verteidigung des Gesetzesvorhabens bestehe auch die Notwendigkeit, Daten für die Registerzählung nach Abschaffung der traditionellen Volkszählung verfügbar zu machen, ist zu sagen, dass die Nützlichkeit der Datenerhebung im Rahmen einer Verhältnismäßigkeitsprüfung nicht allein für eine Rechtfertigung nach Art. 8 Abs.2 EMRK ausreicht. Die vom Gesetz verfolgten Ziele dürften sich durch weniger eingriffsintensive Maßnahmen erreichen lassen, was entsprechend den von der EU gegebenen Vorgaben möglich erscheint.

Die Bundesanstalt „Statistik Österreich“ hat gemäß § 8 Abs. 6 BilDokG Daten über einen festgestellten sonderpädagogischen Förderbedarf spätestens sechs Monate nach Veröffentlichung der Statistik und spätestens 20 Jahre nach der letzten Datenmeldung den Personenbezug zu den betreffenden Schülern und / oder Studierenden zu löschen. Das bedeutet, dass die Daten spätestens nach 20 Jahren vollständig anonymisiert sind. Die „Statistik Österreich“ ist an sich gemäß § 15 Abs. 1 Bundesstatistikgesetz 2000 gehalten, die Identitätsdaten bei der Verarbeitung von personenbezogenen Daten unverzüglich zu beseitigen und durch das bereichsspezifischen Personenkennzeichen Amtliche Statistik (bPk-AS) zu ersetzen. Es gibt jedoch zahlreiche Ausnahmen. Für den Fall, dass der Personenbezug aus gesetzlichen Gründen erhalten bleiben muss, sind die Identitätsdaten unmittelbar nach der Verarbeitung zu verschlüsseln, wobei Daten und Schlüssel getrennt aufzubewahren sind, § 15 Abs. 2 Bundesstatistikgesetz 2000.

5.4 Zusammenfassung zum BilDokG

Die Verwendung der Sozialversicherungsnummer als Identifikationsmerkmal steht in Widerspruch zu der allgemeinen E-Government-Strategie im EGovG. Außerdem ist die Sozialversicherungsnummer wegen ihres Aufbaus unter Verwendung des Geburtsdatums leicht zu fälschen, also unsicher. Da die Sozialversicherungsnummer z.Zt. nicht nur in dem Bereich verwendet wird, für den sie geschaffen worden ist, sondern noch in vielen anderen Bereichen, u.a. der Finanzverwaltung, wird die Gefährdung durch Datenverknüpfungen erhöht, insbesondere bei Verbindungen mit

sensiblen Gesundheitsdaten. Es erscheint daher sinnvoll, die Sozialversicherungsnummer als Identifikationsmerkmal im Bildungsbereich nicht unbegrenzt fortzuführen, sondern in absehbarer Zeit durch ein bPK zu ersetzen.

Das mit dem BilDokG verfolgte Ziel, Daten für die Entscheidungsträger im Bildungsbereich zur Planung und Steuerung des Bildungswesens zu erhalten, lässt mit weniger aufwendigen und weniger eingriffsintensiven Maßnahmen als durch eine alljährliche Totalerfassung der Daten aller Schüler und Studierenden erreichen. Praktisch veranstaltet das BMUKK jedes Jahr im Bildungsbereich eine dem Aufwand für eine Volkszählung vergleichbare Sammlung von Daten. Die im Gesetz für die Gesamtevidenzen und die Bundesstatistik vorgesehenen Maßnahmen erscheinen daher unverhältnismäßig, d.h. nicht notwendig im Sinne von § 1 Abs. 2 DSG 2000 und Art. 8 Abs. 2 EMRK .

6. Registerzählungsgesetz

Der Gesetzgeber hat sich aufgrund der EU-Verordnung Nr. 763/2008 EG vom 9.Juli 2008 über die Volks- und Wohnungszählungen[235] und der Richtlinie 2002/91/EG vom 16. Dezember 2002 über die Gesamtenergieeffizienz von Gebäuden[236] veranlasst gesehen, das Registerzählungsgesetz zu überarbeiten[237] und zum 31.10.2011 eine Registerzählung durchzuführen.

Nach diesem Gesetz ist die Bundesanstalt Statistik Österreich verpflichtet, an der Wende eines jeden Jahrzehnts, erstmals zum 31.10.2011 eine Volks-, Arbeitsstätten, Gebäude- und Wohnungszählung durchzuführen, § 1 Abs. 1 Registerzählungsgesetz. Die erforderlichen Daten werden unter Verwendung bereichsspezifischer Personenkenzeichen gemäß § 9 EGovG ohne Namensnennung der Betroffenen erhoben, § 4 Abs. 1 Registerzählungsgesetz. Die zu erhebenden personenbezogenen Daten sind in einer Anlage zum Registerzählungsgesetz aufgelistet. Sie umfassen im Wesentlichen folgende Merkmale:

Hauptwohnsitz und ggfs. weitere Wohnsitze, Geburtsdatum, Geschlecht Staatsangehörigkeit, Geburtsort, Familienstand, Stellung in der Familie, Geburtsdaten der Kinder, höchster Ausbildungsstand, Erwerbsstatus mit Stellung im Beruf , zeitliches Ausmaß einer unselbständigen Tätigkeit (Vollzeit, Teilzeit, geringfügig beschäftigt), Arbeitsstätte, Dienstgeber und Beitragskontonummer bei der Sozialversicherung, Steuernummer, Angaben zu Arbeitslosigkeit (Dauer, ggf. Schulungen), bei Schülern und Studenten Ausbildungsart, -form und -fachrichtung sowie Adresse der Bildungseinrichtung, Angabe zum Präsenz- oder Zivildienst, Eigenschaft als Pensionist, Privat- oder Anstaltshaushalt.

Sie werden hauptsächlich durch Zusammenführung von Daten aus folgenden Registern generiert:

- Zentrales Melderegister,
- Daten bei den Sozialversicherungsträgern,

---

[235] ABl. L 213 vom13.08.2008, S. 14 ff..
[236] ABl.- L1 vom 04.01.2003, S. 65 ff..
[237] BGBl. I Nr. 125/2009.

- Daten bei den Krankenfürsorgeanstalten der Länder und Gemeinden,
- Daten bei den Kammern der freien Berufe,
- Bildungsstandregister,
- Steuerregister,
- Daten des Arbeitsmarktservices Österreich,
- Unternehmensregister,
- Gebäude- und Wohnungsregister.

Gemäß § 5 Registerzählungsgesetz ist eine Qualitätssicherung der Basisdaten aus den genannten Registern durch Vergleich mit Auskünften aus der Kfz-Zulassungsevidenz, dem Familienbeihilferegister, dem zentralen Fremdenregister, dem Asylbewerberinformationssystem, dem Register der Sozialhilfeempfänger und dem Dienstgeberregister des Bundes durchzuführen. Bei Widersprüchen sind die Ursachen aufzuklären und die Daten entsprechend zu berichtigen.

Um sicherzustellen, dass die aus verschiedenen Registern stammenden Daten ein und derselben Person zuzuordnen sind, erfolgt die Erhebung der genannten Daten in der Form, dass die jeweiligen Registerbehörden verpflichtet sind, für die Personen, deren Daten zu übermitteln sind, bereichsspezifische Personenkennzeichen entsprechend § 7 EGovG bei der Stammzahlenregisterbehörde anzufordern sowie die Erzeugung der bereichsspezifischen Kennziffer für die Statistik, bPK-AS als so genannte Fremd- bPK[238] zu beantragen, § 6 Abs. 1 Registerzählungsgesetz. Mit den Übermittlungen von personenbezogenen Daten seitens der Registerbehörden an die Bundesanstalt sind die verschlüsselten bPk der liefernden Behörde sowie das verschlüsselte bPK-AS zu verknüpfen.

Mit der Änderung des Registerzählgesetzes sind auch Bestimmungen des Bundesstatistikgesetzes[239] angepasst worden, u.a. dessen § 15 Abs. 1. In der ursprünglichen Fassung war eine Beseitigung des Personenbezuges nach der Auswertung der Daten geregelt. In der Neufassung ist jedoch lediglich der Ersatz der Identitätsdaten des Betroffenen durch das bPk-AS vorgesehen, so dass entgegen der Überschrift der Bestimmung „Anonymisierung personenbezogener Daten“ lediglich eine

[238] Zur Fremd-bPk siehe die Ausführungen unter Kapitel 4.5.
[239] BGBl. I 1999, Nr. 163, Bundesstatistikgesetz 2000 in der Fassung vom 11.03.2012.

Pseudonymisierung stattfindet und der Personenbezug sich jederzeit über das bPK-AS und auch das bPK der jeweiligen Registerbehörde wieder herstellen lässt.

Mit der Zusammenführung der genannten Daten in einem zentralen Register ist eine neue, die Daten aller Bürger umfassende Datensammlung, entstanden, die dadurch gekennzeichnet ist, dass im Grundsatz jederzeit auf die Daten eines bestimmten Bürgers zurückgegriffen werden kann. Da die einzelnen Personen ggf. bestimmbar sind, handelt es sich bei dieser Datei um eine Sammlung personenbezogener Daten. Nach der Definition der DS-RL in Art. 2 gelten als personenbezogene Daten alle Informationen über eine bestimmte oder bestimmbare Person. Als bestimmbar wird gemäß Buchst. a der genannten Bestimmung eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. Das DSG 2000 hat diese Definition in verkürzter Form in § 4 Ziffer 1 übernommen.

Mit dem Registerzählgesetz ist eine Sammlung der wesentlichen Lebensmerkmale aller österreichischen Bürger entstanden, also ein Profil aller Bürger. Diese Datensammlung, die mit einer Prüfung und Korrektur aller erfassten Daten verbunden gewesen ist, zeichnet sich dadurch aus, dass sie vollständig, auf Dauer angelegt und jederzeit bis auf Datensatzebene auswertbar ist.

Der Gesetzgeber rechtfertigt sein Vorgehen mit den Verpflichtungen aus der Verordnung der EG Nr. 763/2008 vom 9. Juli 2008 über Volks- und Wohnungszählungen.[240] Die Verordnung sieht allerdings nur Auswertungen auf Gebiets-, Landes- und Bundesebene vor und verlangt keine individuellen Angaben zu einzelnen Personen. Zudem erfasst das Registerzählungsgesetz einen größeren Umfang an personenbezogenen Daten als in den Auswertungen für die EU-Verordnung verlangt wird. Die EU- Verordnung fordert nur Angaben über den höchsten Ausbildungsstand, nicht über die Art der Ausbildung und die Anschriften der Bildungsstäten, auch nicht Angaben über Präsenz- oder Zivildienst, Status als Pensionist. Es werden zwar die An-

[240] Abl. L 218 vom 13.08. 2008, S. 14 ff..

gaben zum Erwerbsstatus gefordert, nicht aber Informationen zur Art und Dauer einer Arbeitslosigkeit.

Auch die Art und Weise der Registerzählung mit der Zusammenfassung in einer Datei und Kontrolle der einzelnen Datensätze wird von der Verordnung nicht gefordert, eben so wenig die Möglichkeit des jederzeitigen Zugriffs auf einzelne Datensätze. Die Verordnung sieht mehrere Alternativen als Datenquellen vor: herkömmliche Zählungen, Registerzählungen, Stichprobenerhebungen sowie Kombinationen der einzelnen Alternativen. Für den Zweck der Verordnung hätte es ausgereicht, wenn die einzelnen Registerbehörden ihre Datenbestände nach den von der Verordnung geforderten Kriterien ausgewertet und dem Bundesamt für Statistik für eine Zusammenfassung zur Verfügung gestellt hätten. Auf diese Weise hätte die Anonymität der Bürger bei der Zählung gewahrt werden können. Statt dessen ist eine Generalinventur der wesentlichen Persönlichkeitsmerkmale der Bürger durchgeführt und in einer zentralen Datei zusammengefasst worden, ohne dass der Gesetzgeber nähere Gründe für diese Art der Erhebung und Speicherung genannt hätte. Die Umstände der Registerzählung lassen vielmehr den Schluss zu, dass der Gesetzgeber weitere nicht näher genannte Absichten mit dieser Art der Datenerhebung verfolgt.

Dabei stellt sich die Frage, ob das beschriebene Vorgehen des Gesetzgebers mit dem Grundrecht auf Datenschutz in Art 1 Abs.1 DSG 2000 und Art. 8 Abs.1 EMRK vereinbar ist und ob ggf. Rechtfertigungsgründe im Sinne von § 1 Abs. 2 DSG 2000 und Art. 8 Abs. 2 EMRK vorliegen.

Die beim Bundesamt für Statistik gespeicherten Daten sind zwar nicht direkt personenbezogen, aber die betroffenen Individuen sind über die bereichsspezifischen Personenkennzeichen bestimmbar, so dass die Daten gemäß Art. 2 DSRL und § 4 Abs. 1 DSG 2000 als personenbezogene Daten im Sinne dieser Gesetze anzusehen sind. Das DSG kennt zwar den Begriff der indirekt personenbezogenen Daten, §§ 4 Ziffer 1, 8 Abs.2 und 9 Ziffer 2 DSG 2000 und legt für diese Kategorie von Daten fest, dass bei deren Verwendung schutzwürdige Interessen im Sinne von § 1 Abs. 1 DSG 2000 nicht verletzt werden. Außerdem werden in § 29 DSG 2000 die Rechte Betroffener eingeschränkt.

Es ist bereits an anderer Stelle (Kap. 2.4) ausgeführt worden, das der im DSG 2000 eingeschränkte Schutz von indirekt personenbezogenen Daten nicht europäischen Vorgaben entspricht. In Art. 7 der DS-RL abschließend alle Fälle aufgelistet sind, in denen eine Verarbeitung personenbezogener Daten zulässig ist. Die in § 8 Abs. DSG 2000 genannten Kategorien „zulässigerweise veröffentlichte Daten“ und „indirekt personenbezogene Daten“ gemäß § 8 Abs. 2 DSG 2000 sind in Art. 7 DS-RL nicht aufgeführt. Daher widerspricht die Annahme, dass in diesen Fällen schutzwürdige Interessen nicht gegeben seien, europarechtlichen Vorgaben, so dass die gesetzlichen Privilegien im DSG 2000 für die Verwendung dieser Daten unter Berücksichtigung des im Konfliktfalle maßgeblichen Anwendungsvorranges der DS-RL nicht zu berücksichtigen sind.[241] Auch der EGMR lässt in seiner Rechtsprechung für die Personenbezogenheit die Bestimmbarkeit einer Person genügen.[242] Ebenso umfasst die Charta der Grundrechte der EU in Art. 8 GRCh als personenbezogene Daten alle Informationen über eine bestimmte oder bestimmbare Person.

Die filigrane Sammlung der Daten aus verschiedene Registern und deren Abgleich mit anderen ist eine Datenerhebung, durch die zunächst einmal das Grundrecht auf Datenschutz nach § 1 Abs. 1 DSG 2000 verletzt ist und ein Eingriff in die Privatsphäre im Sinne von Art. 8 Abs. 1 EMRK stattfindet. Deshalb bleibt zu prüfen, ob Rechtfertigungsgründe nach § 1 Abs. 2 DSG 2000 und Art. 8 Abs. 2 EMRK vorliegen.

Der Gesetzgeber nennt Zwecke der Registerzählung und des dafür geschaffenen Gesetzes für die Durchführung der EU-Verordnung Nr. 763/2008 als Gründe.[243] Dazu ist zu sagen, dass die Verordnung keine Erfassung und Speicherung von individuellen personenbezogenen Daten verlangt, sondern nur statistische Zusammenfassungen auf Gebiets-, Landes- und Bundesebene. Außerdem geht der Umfang der Datenerhebung über das von der Verordnung geforderte Ausmaß hinaus. Es bestehen deshalb Zweifel, ob mit dem Gesetz legitime Zwecke verfolgt werden, weil der Gesetzgeber keine Angaben darüber macht, warum im Gegensatz zu der früheren Regelung in § 15 Abs. 1 Bundesstatistikgesetz nach Auswertung der Daten aus der Re-

---

[241] Jahnel, Handbuch Datenschutzrecht, Salzburg 2010, Kap. 4 Anm. 27 und Kap. 1 Anm. 61
[242] Urteil des EGMR vom 16.02,2000, Amann gg. Schweiz, Rdnr. 65, ÖJZ 2001, S. 71
[243] Regierungsvorlage - Erläuterungen zum Registerzählgesetz, S. 1-16 (1), 320 der Beilagen XXIV. GP, http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_00320/fname_165758.pdf, Abfrage 04.04.2012

gisterzählung keine Löschung erfolgt. Wie oben erwähnt, hätten die Anforderungen der EU-Verordnung auch durch anonyme Auswertung der einzelnen Register und eine Zusammenfassung bei der „Bundesanstalt Statistik“ erfolgen können, so dass festzustellen ist, dass hier nicht das gelindeste Mittel zur Erfüllung des Zwecks der Verordnung gewählt worden ist.

Es bestehen also gewichtige Gründe, die gegen Grundrechtskonformität des Registerzählgesetzes sprechen.

7. Datenschutz im Gesundheitswesen

Im Jahre 2002 sind die §§ 31 a bis 31 d in das ASVG eingefügt worden, die die Grundlage für die Einführung der eCard als elektronischer Ausweis anstelle der papiergebundenen Krankenscheine bilden. Die eCard ist mittlerweile in ganz Österreich in Gebrauch. Auf der eCard sind derzeit keine Gesundheitsdaten gespeichert. Die Karte dient der Identifikation und als Schlüssel zum Gesundheitssystem. Sie ist mit einer Signaturfunktion versehen und kann daher grundsätzlich nach entsprechender Zertifizierung als Bürgerkarte eingesetzt werden.[244] Für das Jahr 2010 war die Einführung einer neuen eCard mit digitalem Foto zur Verbesserung der Authentifikation geplant. Das ist bisher noch nicht geschehen. Um Missbräuchen der eCard entgegenzuwirken hat der Nationalrat das BGM im März 2011 aufgefordert, nunmehr entsprechenden Initiativen zu entwickeln.[245] Ob auch ein digitaler Fingerabdruck gespeichert wird, ist noch offen[246]. Außerdem soll die eCard für die Medikamentenüberwachung eingesetzt werden, um Wechselwirkungen zwischen verschiedenen Medikamenten zu verringern. Dabei werden Rezeptdaten zentral gespeichert und können mittels eCard abgerufen werden. Bisher ist die Teilnahme freiwillig.[247] Ferner ist die Einführung von elektronischen Rezepten sowie die Überwachung von Impfdaten und die Verwaltung von Daten des Disease Management Programms (DMP) mittels eCard geplant.[248]

Unabhängig von der geplanten Erweiterung der Anwendungen insbesondere in Verbindung mit der lebenslangen elektronischen Gesundheitsakte ELGA werden schon heute nicht nur einfache Personaldaten, sondern auch sensible Daten in dem Verfahren erhoben und gespeichert, für das die eCard als Schlüssel dient. Zum Beispiel das Verfahren zur Bewilligung chefarztpflichtiger Medikamente wird beim behandelnden

---

[244] Daten auf der eCard, http://www.chipkarte.at/portal27/portal/ecardportal/channel_content/cmsWindow?action=2&p_menuid=51909&p_tabid=4 , letzte Abfrage 19.01.2012.

[245] Entschließung des Nationalrats vom 12. 03.2011 betreffend Umstellung auf e-Card mit Foto und Ausweispflicht für noch nicht umgestellte Karten, http://www.parlament.gv.at/PAKT/VHG/XXIV/E/E_00019/fname_153353.pdf , letzter Abruf 19.01.2012

[246] „Das Gesicht als Ausweis“,, http://futurezone.at/future/2443-face-moc-das-gesicht-als-ausweis.php ,letzte Abfrage 19.01.2012.

[247] „Pilotprojekte zur E-Medikation gestartet“, http://futurezone.at/future/2533-pilotprojekte-zur-e-medikation-gestartet.php , letzter Abruf 19.01.2012

[248] ELGA: Gesundheitssystem wird elektronisch, http://futurezone.at/future/2254-elga-gesundheitssystem-wird-elektronisch.php , letzte Abfrage 19.01.2012.

Arzt durch Datenverkehr mit der zuständigen Krankenkasse elektronisch abgewickelt, so dass dort auch die dafür erforderlichen Grundinformationen, also die relevanten Gesundheitsdaten abgespeichert werden. In diesem Zusammenhang ist es bedeutsam, dass die Ärzte seit dem Jahre 2003 verpflichtet sind, ihre Abrechnungen den Krankenversicherungsträgern auf elektronischem Wege zu übermitteln und zwar auch die jeweiligen Diagnosen auf der Grundlage von so genannten Diagnosecodes[249]. Das bedeutet, dass schon heute bei den Krankenversicherungsträgern unabhängig von der geplanten Gesundheitsakte ELGA vollständige Gesundheitsdaten der Versicherten vorliegen, die prinzipiell von allen abgerufen werden können, die unmittelbar oder mittelbar (z.B. im Wege der Amtshilfe) Zugang zu den Systemen haben.

7.1 Die Entwicklung der Elektronischen Gesundheitsakte (ELGA)

Im Jahre 2004 entwickelte die Europäische Kommission einen Aktionsplan[250], mit dem die Mitgliedstaaten aufgefordert wurden, Entwicklungsperspektiven für den Einsatz von Informations- und Kommunikationstechnologien im Gesundheitswesen festzulegen. Die Europäische Union hat zwar im Bereich des Gesundheitswesens keine ausschließliche Zuständigkeit, ist aber gemäß Art. 6 AEUV für die Durchführung von Maßnahmen zur Unterstützung, Koordinierung oder Ergänzung der Maßnahmen der Mitgliedstaaten zuständig. Einzelheiten sind in Art. 168 AEUV festgelegt.

Entsprechend den Empfehlungen der EU-Kommission im Aktionsplan wurden mit dem Gesundheitstelematikgesetz, GTelG, in Österreich u.a. die gesetzlichen Rahmenbedingungen für die Einführung des elektronischen Gesundheitsaktes, ELGA, geschaffen. Das GTelG ist als Bestandteil des am 1. Jänner 2005 in Kraft getretenen Gesundheitsreformgesetzes verabschiedet worden. Zur Umsetzung des Gesetzes hat das Bundesministeriums für Gesundheit und Frauen und unter Mitwirkung der Firma ADV (Arbeitsgemeinschaft für Datenverarbeitung) die österreichische E-Health Initiative (EHI) gegründet, die im November 2005 den Entwurf für eine E-Health-

---

[249] § 11 Abs. 2 der Einheitlichen Grundsätze gemäß § 340a ASVG über die EDV- Abrechnung der Vertragsärzte, verfügbar unter www.avsv.at, letzte Abfrage 19.01.2012.

[250] Mitteilung der Kommission an den Rat, das Europäische Parlament, den Europäischen wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Elektronische Gesundheitsdienste - eine bessere Gesundheitsfürsorge für Europas Bürger: Aktionsplan für einen europäischen Raum der elektronischen Gesundheitsdienste {SEC(2004)539}, s.a. (KOM (2004) 356, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0356:FIN:DE:PDF, letzte Abfrage 19.01.2012.

Strategie[251] in Österreich vorgelegt hat. Bestandteil dieser Strategie ist auch das Projekt ELGA. Die Bundesgesundheitsagentur hat zunächst eine Machbarkeitsstudie in Auftrag gegeben, die im November 2006 vorgelegt worden ist.[252] Für die Umsetzung des Projektes ELGA hat die Bundesgesundheitskommission auf der Grundlage einer Vereinbarung mit den Bundesländern gemäß Art. 15 a B-VG im Juli 2006 eine Arbeitsgemeinschaft errichtet. Diese hat am 1.September 2006 ihre Tätigkeit aufgenommen[253] und im August 2007 einen Masterplan vorgelegt[254]. Im Einzelnen sind folgende Kernanwendungen vorgesehen:

- e-Medikation
- e-Befund Labor
- e-Befund Radiologie
- e-Arztbrief/Patientenbrief

Die Arge hat 2007 mit der Umsetzung des Masterplanes begonnen. Die Errichtung eines Gesundheitsdienste-Registers sowie eines Patienten-Indexes, Vorarbeiten für die eMedication sowie erste Pilotversuche standen dabei im Vordergrund[255]. Zur Begründung der geplanten Gesundheitstelematik beruft sich der Gesetzgeber auf die zunehmende Verwendung von ITK in allen Lebensbereichen auf dem Weg in die Informationsgesellschaft. Mit der Nutzung dieser Technologien werde es möglich, expandierende Informationsmengen (medizinisches Wissen) und neue Möglichkeiten der Versorgung auf Grund des rasanten medizinischen und medizintechnischen Fortschritts zu erschließen. Der Zwang zu Effizienzsteigerungen werde nur mit Hilfe adäquater informations- und kommunikationstechnologischer Unterstützung zu bewältigen sein[256].

---

[251] http://ehi.adv.at/fileadmin/user_upload/adv_author/pdfs/konferenz20051202/Strategie_Empfehlung_der_e-Health-Initiative_Oesterreich_20051202.pdf ,letzte Abfrage 19.01.2012.

[252] http://www.arge-elga.at/fileadmin/user_upload/uploads/download_Papers/Arge_Papers/Machbarkeitsstudie_ELGA_Endbericht_21112006.pdf ,letzte Abfrage 19.01.2012.

[253] http://www.arge-elga.at/index.php?id=3 , letzter Abfrage 19.01.2012.

[254] http://www.arge-elga.at/fileadmin/user_upload/uploads/download_Papers/Arge_Papers/Endbericht_Folgeauftrag.pdf letzte Abfrage 19.01.2012.

[255] http://www.arge-elga.at/index.php?id=15 , letzte Abfrage 19.01.2012.

[256] Erläuterungen zur KAKuG-Novelle, http://www.parlament.gv.at/PG/DE/XXII/I/I_00693/fname_030666.pdf ,letzte Abfrage 19.01.2012.

7.2 Datenschutzrechtliche Rahmenbedingungen für ELGA

Bei der Verwendung personenbezogener Daten ist zwischen Eingriffen staatlicher Behörden, also hoheitlichen Akten, und sonstigen Eingriffen zu differenzieren. Grundsätzlich gilt, dass die Verwendung personenbezogener Daten nach § 1 Abs. 2 Satz 1 DSG 2000 nur aus lebenswichtigem Interesse des Betroffenen oder mit seiner Zustimmung erfolgen darf. Beschränkungen dieses Anspruchs auf Geheimhaltung sind nur zur Wahrung überwiegender Interessen eines anderen zulässig. Für die Abgrenzung zwischen schutzwürdigen Geheimhaltungsinteressen von Betroffenen und überwiegenden Interessen anderer sind die §§ 7 bis 9 DSG heranzuziehen.[257] Eine besondere rechtliche Grundlage für die Verwendung von personenbezogenen Daten ist, soweit diese nicht durch staatliche Behörden erfolgt, nach nationalem Recht nicht erforderlich, auch wenn es sich dabei um Gesundheitsdaten als sensible Daten im Sinne von § 4 Ziffer 2 DSG 2000 handelt.[258] Auf europäischer Ebene enthält Art. 8 Abs. 1 DS-RL ein grundsätzliches Verbot der Verwendung sensibler Daten, für das die in den nachfolgenden Absätzen geregelten Ausnahmen gelten. Art. 8 Abs. 3 DS-RL erlaubt die Verwendung im Rahmen der Gesundheitsvorsorge und medizinischen Behandlungen, soweit die Verarbeitung der Daten durch ärztliches Personal erfolgt, das der beruflichen Schweigepflicht unterliegt. Wenn eine Verwendung sensibler Daten für andere Aufgaben in Betracht kommt, müsste gemäß Art. 8 Abs. 4 DS-RL auch für nicht-staatliche Eingriffe eine besondere gesetzliche Grundlage geschaffen werden, für die ein wichtiges öffentliches Interesse bestehen muss und die angemessene Garantien für die Betroffenen enthält.

Bei Eingriffen staatlicher Behörden müssen gemäß § 1 Abs. 2 Satz 1 DSG 2000 die zusätzlichen Anforderungen von Art. 8 Abs. 2 EMRK erfüllt werden. Falls die betreffenden Gesetze die Verwendung sensibler Daten vorsehen, so darf dies nach § 1 Abs. 2 Satz 2 DSG 2000 nur zur Wahrung besonders wichtiger öffentlicher Interessen geschehen. Außerdem müssen angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festgelegt werden und die Eingriffe in das Grundrecht des § 1 Abs. 1 DSG 2000 müssen in der gelindesten möglichen Form erfolgen. In § 9 sind die Fälle geregelt, in denen auch bei Verwendung sensibler Daten ein schutzwürdiges Interesse im Sinne von § 1 Abs. 1 DSG 2000 und damit ein

---

[257] Mayer-Schönberger/Bradl, Datenschutzgesetz, 2. Auflage 2006, S. 65.
[258] Frohner in Bauer/ Reimer , Handbuch Datenschutzrecht, 2009, S. 268 f..

Geheimhaltungsanspruch nicht besteht. Nach § 9 Ziffer 12 DSG 2000 dürfen Gesundheitsdaten verwendet werden, wenn „*die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen".* § 9 Ziffer 3 ermöglicht die Verwendung besonders schutzwürdiger Daten auf der Grundlage von Vorschriften, die der Wahrung eines wichtigen öffentlichen Interesses dienen.

An den geplanten Anwendungen wurde in der Vergangenheit Kritik in erster Linie von Datenschützern und Ärzten geübt. Die Datenschützer haben vor allen die aus ihrer Sicht unklare Eingrenzung der Gesundheitsdiensteanbieter (GDA) als Zugangsberechtigte zu Gesundheitsdaten in § 2 Ziffer 2 GTelG bemängelt. Im Sinne des Gesetzes gelten als GDA Auftraggeberinnen/Auftraggeber und Dienstleisterinnen/Dienstleister gemäß DSG 2000, bei denen die regelmäßige Verwendung von Gesundheitsdaten Bestandteil ihrer Erwerbstätigkeit, ihres Betriebszwecks oder ihres Dienstleistungsangebotes ist. Die in der Anlage 1 zur Gesundheitstelematikverordnung, GTelV, aufgeführten Rollen verdeutlichen, dass nicht nur Anbieter ärztlicher Leistungen, die der ärztlichen Schweigepflicht unterliegen, Zugriff auf Gesundheitsdaten haben sollten, sondern zum Beispiel auch Versicherungsträger, der Hauptverband der österreichischen Sozialversicherungsträger und die Gesundheitsverwaltung. Zwar ist in § 10 GTelG eine rollenbasierte Identifizierung der GDA vorgesehen, die durch eine elektronische Bescheinigung oder Aufnahme in ein Verzeichnis gewährleistet werden soll, aber die Datenschutzkommission bemängelte, dass in der am 1. Jänner 2009 in Kraft getretenen GTelV diverse Abweichungen vom Regelfall des Nachweises vorgesehen sind und die in der GTelV geregelten Ausnahmen nicht mit denen in dem der Verordnung zugrunde liegenden Gesetz, dem GTelG, übereinstimmen[259]. Durch die große Zahl der Zugangsberechtigten sei für die Bürger nicht überschaubar, wer auf welche Daten zugreifen darf und wer tatsächlich zugegriffen hat, so dass im Nachhinein nicht feststellbar sei, wer Da-

[259] Brief des Datenschutzrates an das Bundesministerium für Gesundheit, Familie und Jugend vom 01.12.2008, http://www.austria.gv.at/DocView.axd?CobId=33058 ,letzte Abfrage 19.01.2012.

ten erhalten hat[260]. Nach den Regelungen im GTelG und in der GTelV sollen nicht nur Ärzte oder Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, Zugriff auf Gesundheitsdaten erhalten.[261] Zwar dürfen nach § 9 Ziffer 3 DSG 2000 auch Gesundheitsdaten verarbeitet werden, wenn sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen. Es wird jedoch bezweifelt, ob ein wichtiges öffentliches Interesse besteht. Eine angestrebte Verbesserung der Gesundheitsvorsorge liegt zwar in öffentlichem Interesse, es fragt sich jedoch, ob das öffentliche Interesse so wichtig erscheint, das es ausreicht, um einen Eingriff in das Grundrecht auf Datenschutz zu rechtfertigen.[262] Da die mit ELGA geplanten Eingriffe in das Grundrecht unter Datenschutzgesichtspunkten als kritisch betrachtet werden, wurde erwogen, dafür spezielle gesetzliche Regelungen zu schaffen,[263] bzw. wurde dies als wesentliche Voraussetzung für eine Einführung von ELGA angesehen.[264]

Auf Bedenken war auch die sehr weite Definition des Begriffs Gesundheitsdaten in § 2 Abs. 1 GTelG gestoßen. Dazu sollen neben der geistigen und körperlichen Verfassung (inklusive genetischer Informationen) auch gesundheitsrelevante Lebensgewohnheiten (inklusive Sexualverhalten) Umwelteinflüsse, Arzneimittel, Diagnose-, Therapie- und Pflegemethoden sowie Art und Kosten der konsumierten Gesundheitsleistungen gehören.[265]

Seitens der Ärzte, die von Gesetzes wegen dem Arztgeheimnis verpflichtet sind, § 54 Abs. 1 ÄrzteG, wurde insbesondere die drohende Aushöhlung dieser Verpflich-

---

[260] Arge Daten, Votum Separatum zum GTelG, http://www.argedaten.at/php/cms_monitor.php?q=PUBTEXT-ARGEDATEN&s=63469cza ,letzte Abfrage 19.01.2012.
[261] Löffler, Die elektronische Gesundheitsakte und der Datenschutz, Bakkalaureatsarbeit Tech. Uni Wien 2007, Seite 21 f.
[262] Löffler aaO. S. 23.
[263] IBM im Auftrag der Bundesgesundheitsagentur - Machbarkeitsstudie betreffend Einführung der elektronischen Gesundheitsakte (ELGA) im österreichischen Gesundheitswesen - 21.11. 2006, S. 64, http://www.arge-el-ga.at/fileadmin/user_upload/uploads/download_Papers/Arge_Papers/Machbarkeitsstudie_ELGA_Endbericht_21112006.pdf , letzte Abfrage 19.01.2012.
[264] Buchinger, Die Elektronische Gesundheitsakte in Österreich, in Jahnel (Hrsg.) Datenschutzrecht und E-Government, Jahrbuch 2008, S. 133- 160 (142).
[265] Ärztemagazin 5/2007, Seite 6.

tung und die damit verbundene Störung des Vertrauensverhältnisses Arzt/Patient beklagt.[266]

§ 9 Abs. 3 GTelG kennzeichnet, wie es bisher bei ELGA mit dem informationellen Selbstbestimmungsrecht der Bürger bestellt ist: „*Der Zugriff auf die im E-Health-Verzeichnisdienst enthaltenen Daten ist auf die im E-Health-Verzeichnisdienst aufgenommenen GDA, die Registrierungsstellen sowie die mit der Gesundheitsverwaltung betrauten Einrichtungen des öffentlichen Rechts einzuschränken".* Von Zugriffen der Bürger auf ihre eigenen Daten ist in dem bestehenden Gesetz keine Rede, geschweige denn von deren vorheriger Einwilligung zur Erhebung und Speicherung.

7.3 Das GTelG 2011

Sicherlich beeinflusst durch die beschriebene Kritik in der Vergangenheit hat das Bundesministerium für Gesundheit, Familie und Jugend im Februar 2011 den Entwurf für ein ELGA-Gesetz (Bundesgesetz betreffend Datensicherheitsmaßnahmen bei der Verwendung elektronischer Gesundheitsdaten(Gesundheitstelematikgesetz 2011- GTelG-2011)) vorgelegt[267], mit dem das bestehende (kritikbehaftete) Gesundheitstelematikgesetz ersetzt werden soll (§ 25 Abs. 2 des Entwurfs).
Gegenstand des Gesetzes ist die Verwendung elektronischer Gesundheitsdaten im Sinne von § 4 Ziffer 8 DSG 2000, § 1 Abs. 1 GTelG 2011. Dabei wird das Ziel verfolgt, Mindeststandards für die Datensicherheit festzulegen, Informationsgrundlagen für den internationalen Datenaustausch zu schaffen und einheitliche Regelungen für die Kommunikation von Gesundheitsdaten zu treffen, § 1 Abs. 2 GTelG 2011.

Die GDA sind verpflichtet, das ELGA-System zu verwenden, § 13 Abs. 3 GTelG 2011. GDA sind nicht nur Ärzte, sondern alle Einrichtungen, die regelmäßig Gesundheitsdaten zumindest teilweise automationsunterstützt verwenden und für die diese Verwendung Bestandteil ihres Aufgabengebietes, ihrer Erwerbstätigkeit, ihres Betriebszweckes oder ihres Dienstleistungsangebotes ist, § 2 Ziffer 2 GTelG 2011. Sie werden in einen eHealth-Verzeichnis eingetragen, § 9 Abs. 2 GTelG 2011. Die Verwendung von ELGA-Daten setzt eine entsprechende Berechtigung des

---

[266] Ärztekammer für Wien, E-Health: Ärztekammer warnt vor Datenmissbrauch, http://www.initiative-elga.at/initiative/Termin_Infos/E_Health_AeK_Wien_061114.pdf , letzte Abfrage 1^9.01.2012.
[267] http://bmg.gv.at/cms/home/attachments/5/7/4/CH1300/CMS1298381237041/elga-gesetz.pdf, letzte Abfrage 19.01.2012.

Diensteanbieters voraus, § 14 Abs. 3 GTelG 2011. Die generellen Zugriffsberechtigungen auf ELGA-Gesundheitsdaten sind vom Bundesminister für Gesundheit per Verordnung festzulegen, § 20 Abs. 2 GTelG 2011. Über individuelle Zugriffsberechtigungen, die auf einzelne Dienstanbieter und ELGA-Gesundheitsdaten abstellen, entscheiden die Patienten, § 20 Abs.3 GTelG 2011.

Das Gesetz sieht vor, dass grundsätzlich alle medizinischen Daten von Patienten in ELGA erfasst werden, es sei denn diese haben der ELGA-Teilnahme ganz oder teilweise widersprochen, § 15 Abs. 1 Ziffer 1 und Abs. 2 GTelG 2011. Darüber hinaus haben die Patienten das Recht auf Einsicht in ihre Gesundheitsdaten und die Protokolldaten. Außerdem können sie den Zugriff auf Gesundheitsdaten mittels individueller Zugriffsberechtigungen bestimmen, indem sie elektronische Verweise auf ELGA-Daten ausblenden oder bestimmte GDA vom Zugriff ausschließen, § 16 Abs. 1 Ziffer 4 GTelG 2011.

Die Speicherfrist für Verweise auf ELGA-Gesundheitsdaten beträgt grundsätzlich 36 Monate. In Ausnahmefällen, wie z.B. für Laborbefunde, sind kürzere Löschungsfristen vorgesehen, § 19 Abs. 5 und 6 GTelG 2011.

7.4 Rechtliche Begründung des GTelG 2011

Zu den rechtlichen Grundlagen des Entwurfs berufen sich die Verfasser im Wesentlichen auf zwei Argumente, einmal auf Art. 8 Abs.4 DS-RL und zum anderen darauf, dass es sich bei der Verwendung der Gesundheitsdaten in ELGA nicht um Eingriffe einer staatlichen Behörde handele.[268]

Zunächst wird zutreffend dargelegt, dass nach § 1 Abs. 2 DSG 2000 eine Beschränkung des Anspruchs auf Geheimhaltung gemäß § 1 Abs. 1 DSG 2000 nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig ist, soweit die Verwendung nicht im lebenswichtigen Interesse des Betroffenen liegt oder dieser zugestimmt hat. § 9 Ziffer 12 DSG 2000 erlaubt die Verwendung von sensiblen Gesundheitsdaten nur im Rahmen der medizinischen Behandlung und Gesundheitsvorsorge unter der Voraussetzung, dass diese durch ärztliches Personal oder Perso-

---

[268] Erläuterungen zum GTelG 2011, S. 5, http://bmg.gv.at/cms/home/attachments/5/7/4/CH1300/CMS1298381237041/erlaeuterungen.pdf, letzte Abfrage 19.01.2012.

nen mit entsprechender Geheimhaltungspflicht erfolgt. Von diesen Ausnahmen werden die im Rahmen der ELGA geplanten Datenverwendungen nicht alle erfasst, weil nach dem Entwurf z.B. auch Amtsärzte, Schulärzte und Vertrauensärzte der Versicherungen sowie Apotheken Zugriff auf die Daten erhalten sollen, § 2 Ziffer 10 GTelG 2011. Die Verwendung der Daten durch diesen Personenkreis erfolgt in der Regel nicht im Rahmen einer medizinischen Behandlung. § 9 Ziffer 12 DSG 2000 ist daher keine geeignete rechtliche Grundlage für die Verwendung von Gesundheitsdaten durch diesen Gruppe.

Nach Art. 8 Abs. 4 DS-RL können die Mitgliedstaaten vorbehaltlich angemessener Garantien auch aus Gründen eines wichtigen öffentlichen Interesses durch Rechtsvorschrift andere Ausnahmen vorsehen. Die Verfasser des Entwurfs argumentieren daher, dass das DSG 2000 in diesem Punkt nicht der Richtlinie entspreche und meinen, dass Art. 8 Abs. 4 DS-RL im Rahmen einer richtlinienkonformen Auslegung in die Ausnahmetatbestände einzubeziehen sei.[269] Deshalb wird im Entwurf auch das wichtige öffentliche Interesse angesprochen, § 13 Abs. 1 GTelG 2011. Zur Begründung dieses Interesses werden eine Reihe gesundheitspolitischer Ziele aufgelistet. Neben einer Stärkung der Rechte der Patient/inn/en werden die Qualitätssteigerung diagnostischer und therapeutischer Entscheidungen, Steigerung der Prozess- und Ergebnisqualität von Gesundheitsdienstleistungen, Aufrechterhaltung einer hochwertigen Gesundheitsversorgung und Wahrung des finanziellen Gleichgewichts des Systems der sozialen Sicherheit genannt. Nach § 13 Abs. 2 GTelG 2011 sollen ELGA-Gesundheitsdaten für diese Zwecke verwendet werden. Über den Zeitpunkt und die Form der Verwendung soll der Bundesminister für Gesundheit durch Verordnung entscheiden. Daraus wird deutlich, dass die Informationen nicht nur für Behandlung und Betreuung von Patienten, sondern für eine umfassende staatliche Kontrolle und Steuerung des Gesundheitswesens verwendet werden sollen. Obwohl in den Erläuterungen zum Gesetzesentwurf auf den Bericht der Art. 29-Datenschutzgruppe Bezug genommen worden ist[270], wird eine wesentliche Forderung dieses Gremiums, nämlich die Beschränkung der Verwendung von Patientendaten auf Zwecke der Be-

---

[269] Erläuterungen zum GTelG 2011 S. 5.
[270] Erläuterungen zum GTelG 2011, S. 22, http://bmg.gv.at/cms/home/attachments/5/7/4/CH1300/CMS1298381237041/erlaeuterungen.pdf, letzte Abfrage 19.01.2012.

handlung, offensichtlich missachtet. Nach Ansicht der Art. 29-Datenschutzgruppe sollte die Verwendung von personenbezogenen Daten in elektronischen Patientenakten für andere Zwecke als in Art. 8 Abs.3 DS-RL (umgesetzt in § 9 Ziffer 12 DSG 2000) vorgesehen grundsätzlich verboten werden. Die Verwendung von Daten aus elektronischen Patientenakten für andere Zwecke sollte nur in anonymisierter oder zumindest pseudonymisierter Form erfolgen.[271]

In jedem Fall muss für die Verwendung von sensiblen Daten außerhalb der medizinischen Versorgung gemäß Art. 8 Abs. 4 DS-RL und § 9 Ziffer 3 DSG 2000 ein wichtiges öffentliches Interesse bestehen und die damit verbundenen Eingriffe in das Grundrecht auf Datenschutz müssen nach § 1 Abs. 2 Satz 3 DSG 2000 das gelindeste mögliche Mittel zur Erfüllung des jeweiligen Zweckes darstellen. Ob die in § 13 Abs. 1 GTelG 2011 genannten Zwecke wichtige öffentliche Interessen repräsentieren, ist umstritten. Einerseits wird behauptet, dass ELGA das Potential besitze, die Qualität von Gesundheitsdienstleistungen zu erhöhen, die Informationen der Ärzte zu verbessern und dadurch die erfolgreiche Behandlung zu unterstützen, Mehrfachuntersuchungen und Fehlmedikationen zu vermeiden und dadurch auch Kosten zu sparen.[272] Dass Kosteneinsparungen im Gesundheitswesen ein wichtiges öffentliches Interesse bedeuten können, hat der VfGH in zwei Entscheidungen bestätigt.[273] Allerdings wird von der Ärzteschaft bestritten, dass tatsächlich Kosten eingespart werden, weil der Gesetzgeber die zusätzlichen Kosten für Anschaffung und Betrieb der neuen Systeme in seinen Berechnungen nicht berücksichtigt habe.[274] Selbst wenn man davon ausgeht, dass die im Gesetz genannten Ziele wichtige öffentliche Interessen repräsentieren, stellt sich die Frage, ob dafür eine zentrale Zugriffsmöglichkeit auf personenbezogene sensible Daten auch für Einrichtungen außerhalb der behandelnden

---

[271] Art. 29-Datenschutzgrupe, Arbeitspapier WP 131 vom 15. 02 2007, Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), S. 17 u. 18, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_de.pdf, letzte Abfrage 19.01.2012.

[272] Frohner in Bauer/ Reimer , Handbuch Datenschutzrecht, 2009, S. 269 f..

[273] Entscheidung des VfGH vom 10.03.2005, Vfslg. Nr. 17500, Ziffer 2.1.2, (Aufrechterhaltung der Finanzierbarkeit der gesetzlichen Krankenversicherung wichtiges öffentliches Interesse), http://www.ris.bka.gv.at/Dokumente/Vfgh/JFT_09949690_03B01703_00/JFT_09949690_03B01703_00.pdf, letzte Abfrage 19.01.2012; Entscheidung des VfGH vom 19.06.2006, Vfslg. Nr.17869, Ziffer 3.2.2 (kostengünstige Steuerung des Gesundheitswesens wichtiges öffentliches Interesse), http://www.ris.bka.gv.at/Dokumente/Vfgh/JFT_09939381_05G00145_00/JFT_09939381_05G00145_00.pdf , letzte Abfrage 19.01.2012.

[274] ÖZZ 3/2011, S. 1-2.

Ärzte und Krankenanstalten erforderlich ist. Für Steuerungsfunktionen würden anonymisierte Daten ausreichen. Die Verwendung von Daten ohne Personenbezug für die Steuerung des Systems wird auch von der DSK angeregt.[275]

Unabhängig von der Frage, wer als GDA Zugriff auf ELGA-Daten erhält, geht aus dem Gesetz nicht hervor, zu welchen Daten der einzelne GDA aufgrund seiner Rolle Zugang haben wird. Das soll gleichfalls durch den Bundesminister für Gesundheit im Verordnungswege festgelegt werden, § 20 Abs. 2 GTelG 2011. In § 14 Abs.1 Ziffer 1 GTelG 2011 ist vorgesehen, dass die durch ELGA verfügbar gemachten Gesundheitsdaten **direkt** personenbezogen nur für Behandlungszwecke gemäß § 9 Ziffer 12 DSG 2000 verwendet werden dürfen. Dies lässt eine anderweitige Verwendung von indirekt personenbezogenen Daten zumindest als möglich erscheinen. Das stünde nicht in Einklang mit der DS-RL, die personenbezogene Daten uneingeschränkt schützt, unabhängig davon, ob es sich um Daten einer bestimmten oder nur bestimmbaren Person handelt, Art 2 Buchst. a DS-RL. Das geplante Gesetz macht damit nicht hinreichend deutlich, mit welchen Eingriffen Patienten in ihren Anspruch auf Geheimhaltung ihrer Daten zu rechnen haben, lässt also die erforderliche Klarheit und Qualität vermissen, die der EMRK für gesetzliche Eingriffsermächtigungen gefordert hat.[276]

Weiters regelt § 1 Abs. 2 DSG 2000, dass Eingriffe durch Behörden nur auf der Grundlage von Gesetzen erfolgen dürfen, die den Anforderungen von Art. 8 Abs. 2 EMRK genügen. Dazu wird argumentiert, dass es sich bei den GDA nicht um staatliche Behörden handele. Es werde keine Verwendung von Daten vorgesehen, die nicht durch die Betroffenen beeinflusst werden können. Wer Gesundheitsdienstleistungen erbringe, dürfe dies nur mit Einverständnis des Betroffenen tun.[277] Die Verfasser des Entwurfes erwähnen selbst die Amtsärzte als Ausnahme. Außerdem ist nicht auszuschließen, dass im Wege der Verordnung durch den Bundesminister für

---

[275] Stellungnahme der Datenschutzkommission zum ELGA-Gesetz vom 11.03.2011, S. 2, https://www.dsk.gv.at/DocView.axd?CobId=42793, letzte Abfrage 19.01.2012.

[276] Schweizer, Die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zum Persönlichkeits- und Datenschutz, DuD 2009, S. 462 ff. (467); Grabenwarter, Europäische Menschenrechtskonvention, 4. Aufl. 2009, §18 Rz. 11, S. 114.

[277] Erläuterungen zum GTelG 2011, S. 5, http://bmg.gv.at/cms/home/attachments/5/7/4/CH1300/CMS1298381237041/erlaeuterungen.pdf, letzte Abfrage 19.01.2012.

Gesundheit gemäß § 13 Abs. 2 GTelG 2011 Zugriffsmöglichkeiten auf ELGA-Daten für weitere staatliche Behörden geschaffen werden.

Weiter stellt sich die Frage, ob nicht mit Inkrafttreten des Gesetzes in Form des jetzt vorliegenden Entwurfes bereits ein staatlicher Eingriff stattfindet, weil dann automatisch alle anfallenden Patientendaten in ELGA erfasst werden, wenn der Betroffene keinen Widerspruch einlegt, §§ 13 Abs. 3 und 15 Abs. 2 GTelG 2011. Wenn kein Widerspruch erfolgt, sind nach § 13 Abs. 4 GTelG 2011 unabhängig von einer Behandlung oder Betreuung Daten aus anderen Bereichen des Gesundheitsbereiches für ELGA zugänglich zu machen. Auch in dieser Maßnahme dürfte ein Eingriff im Sinne von § 1 Abs. 2 DSG 2000 und Art. 8 Abs. 2 EMRK zu sehen sein. Eingriffe müssen auch nicht zwingend in die Form eines individuellen Rechtsaktes gekleidet sein, und bereits die Geltung eines Gesetzes kann einen Eingriff bedeuten.[278] Auch abstrakte Maßnahmen können einen Eingriff darstellen. Wenn Daten in Unkenntnis der Betroffenen erhoben werden und ihnen der Nachweis nicht möglich oder unzumutbar ist, dass bereits konkrete Eingriffshandlungen vorliegen, so können sie sich gegen die Geltung eines Gesetzes wenden, dass derartige Maßnahmen zulässt.[279]

Unabhängig davon, ob bereits durch das Gesetz selbst staatliche Eingriffe stattfinden oder nur vorbereitet werden, schafft eine systematische Sammlung sensibler Daten mit zentralen Zugriffsmöglichkeiten ein hohes Risiko möglicher Missbräuche. Aus Sicht der Art. 29-Datenschutzgruppe bergen die EPA-Systeme, die die medizinischen Daten einer Person aus verschiedenen Quellen zentral erfassen und diese sensiblen Daten weiteren Kreisen leichter zugänglich machen, ein neues Risikopotenzial, das die Dimensionen des möglichen Missbrauchs medizinischer Daten einzelner Personen völlig verändere.[280]

Im Rahmen seiner Gewährleistungsverpflichtungen aus der EMRK ist ein Staat nicht nur gehalten, selbst ungerechtfertigte Eingriffe in die Freiheitssphäre Einzelner zu

---

[278] Wiederin in Merten/Papier (Hrsg.) Handbuch der Grundrechte, Band VII/1 Grundrechte in Österreich, 2009, S. 180.
[279] Urteil des EGMR vom 02.08.1984, Malone gg. Vereinigtes Königreich, Ziffer 64, EuGRZ 1985, S. 17 ff. (20).
[280] Art. 29-Datenschutzgruppe, Arbeitspapier WP 131 vom 15. 02 2007, Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), S. 5, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_de.pdf, letzte Abfrage 19.01.2012.

unterlassen, sondern durch entsprechende Maßnahmen auch dafür zu sorgen, dass Eingriffe in Grundrechte durch private Personen oder Organisationen auf das erforderliche Mindestmaß beschränkt bleiben[281], beispielsweise durch klare und eindeutige gesetzliche Regelungen. Die Verlagerung der Bestimmungen über Zugriffsrechte zu sensiblen personenbezogenen Daten in noch zu erlassende Verordnungen erfüllt diese Anforderung sicher nicht. Die Zugriffsrechte müssten aus dem Gesetz selbst zu entnehmen sein, weil ansonsten für die Bürger die möglichen Verwendungen ihrer Daten unklar bleiben. In diesem Sinne haben sich auch die DSK[282] und der Datenschutzrat[283] zu dem Gesetzentwurf geäußert.

Nach § 19 Abs. 1 GTelG 2011 sind die ELGA-GDA verpflichtet, die ELGA-Gesundheitsdaten in geeigneten Datenspeichern zu speichern. Darüber hinaus sind sie verpflichtet, elektronische Verweise auf diese Daten in Verweisregistern zu speichern. Gemäß § 19 Abs. 5 sind die elektronischen Verweise auf die Daten automatisch nach 36 Monaten zu löschen. Für Laborbefunde, Patientenverfügungen und Vorsorgevollmachten sind nach Abs. 6 der genannten Bestimmung kürzere Löschungsfristen vorgesehen. Die Daten selbst sollen offensichtlich unbegrenzt gespeichert werden. Eine Ausnahme gilt nach Abs. 7 für Medikationsdaten, die nach sechs Monaten automatisch zu löschen sind. Auch im Falle des Widerspruchs einer Teilnahme an ELGA sind nur die Verweise zu löschen und nicht die Daten selbst, § 15 Abs. 4 GTelG 2011. Eine Erklärung dafür, warum grundsätzlich nur die Verweise und nicht die Gesundheitsdaten selbst gelöscht werden, geht aus dem Entwurf und den Erläuterungen dazu nicht hervor. In den Erläuterungen wird von einer Löschung der Gesundheitsdaten nach 36 Monaten gesprochen und eine Differenzierung wie im Entwurf selbst nach Gesundheitsdaten und Verweisen darauf nicht vorgenommen.[284] Die Begründung für die Frist von 36 Monaten ist die Verjährungsfrist für Schadenersatzansprüche.

---

[281] Grabenwarter, Europäischen Menschenrechtskonvention, 4. Aufl. 2009, §17 Rz. 6,7, S. 103; § 19 Rz. 1, S.125.
[282] Stellungnahme der Datenschutzkommission zum ELGA-Gesetz vom 11.03.2011, S. 2, https://www.dsk.gv.at/DocView.axd?CobId=42793, letzte Abfrage 19.01.2012.
[283] Stellungnahme des Datenschutzrates zum ELGA-Gesetz vom 28 03.2011, S. 23, http://www.bundesregierung.at/DocView.axd?CobId=43036, letzte Abfrage 19.01.2012.
[284] Erläuterungen zum GTelG 2011, S. 23, http://bmg.gv.at/cms/home/attachments/5/7/4/CH1300/CMS1298381237041/erlaeuterungen.pdf, letzte Abfrage 19.01.2012

7.5 Zusammenfassende Stellungnahme zum GTelG 2011

Der Entwurf bringt Verbesserungen der Patientenrechte mit sich. Patienten können der Speicherung ihrer Daten in ELGA ganz oder teilweise widersprechen. Sie haben ein Recht auf Einsicht in die über sie gespeicherten Gesundheitsdaten und auch in die Protokolldaten, § 16 Abs. 1 GTelG 2011. Problematisch erscheint, dass die Patienten der Verwendung ihrer Gesundheitsdaten ausdrücklich widersprechen müssen (Opt-Out-Verfahren) und eine Einwilligung (Opt-In-Verfahren) nicht erforderlich ist. Für ein Opt-In-Verfahren plädiert die Datenschutzkommission. Letztere kritisiert auch, dass die Zahl der Personen, die nach dem vorgesehenen System Zugriff auf die Gesundheitsdaten haben werden, völlig unübersehbar sei.[285] Da ein Teil der möglichen Verwendungen und die Gestaltung der Zugriffsrechte der GDA noch zu erlassenden Verordnungen überlassen bleibt, ist für die Patienten nicht erkennbar, was mit ihren Daten letztendlich geschieht und welche Nachteile ihnen daraus möglicherweise erwachsen. Die denkbaren Eingriffe in das Recht auf Geheimhaltung ihrer Gesundheitsdaten sind für die Patienten nicht vorhersehbar, so dass das geplante Gesetz mangels ausreichender Bestimmtheit im Sinne der Rechtsprechung des EGMR[286] keine ausreichende gesetzliche Grundlage für Eingriffe darstellt.

Da die Rollenzuweisung für die einzelnen GDA und die damit verbundenen Zugriffsrechte künftigen Verordnungen überlassen wird, ist auch nicht klar, zu welchen Gesundheitsdaten die einzelnen Arztgruppen jeweils Zugang haben werden. Nicht jeder Arzt einer bestimmten Fachgruppe benötigt für seine Diagnosen und Behandlungen die Daten aller anderen Fachärzte. Die Art. 29-Datenschutzgruppe hat deshalb für die Zugriffsrechte ein modulares System vorgeschlagen, in dem sichergestellt wird, dass jeder Arzt nur Zugang zu den Daten hat, die er für seine Arbeit benötigt.[287] Die gut gemeinte Möglichkeit für Patienten, durch Widersprüche und Be-

---

[285] Stellungnahme der Datenschutzkommission zum ELGA-Gesetz vom 11.03.2011, S. 2 f., https://www.dsk.gv.at/DocView.axd?CobId=42793, letzte Abfrage 19.01.2012.

[286] Siehe zur Frage der Bestimmtheit von Eingriffsnormen Urteile des EGMR vom 17.06.2008, Meltex Ltd. und Mesrop Movsesyan gg. Armenien, Nr. 32283/04, Ziffer 80, http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Mesrop%20|%20Movsesyan&sessionid=85132653&skin=hudoc-en ; vom 17.01.2010, Gillan and Quinton gg. Vereinigtes Königreich, Nr. 4158/05, Ziffer 76; http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Gillan%20|%20Quinton&sessionid=85132802&skin=hudoc-en , letzte Abfrage 19.01.2012; S. und Marper gg. Vereinigtes Königreich vom 04.12.2008, Ziffer 95/96, EuGRZ 2009, S. 301 ff. (310).

[287] Art. 29-Datenschutzgrupe, Arbeitspapier WP 131 vom 15. 02 2007, Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), S. 20,

schränkung der Zugriffsrechte Informationen auszublenden, führt dazu, dass sich behandelnde Ärzte nicht auf die Vollständigkeit der Informationen in ELGA verlassen können und schon aus Haftungsgründen ggf. ergänzende Untersuchungen veranlassen müssen. Dies ist für die Effizienz und die angestrebten Kosteneinsparungen nicht förderlich.

Die Dokumentation der Diagnosen und Therapien dient nicht nur den Patienten, sondern auch den Ärzten als Beleg für ihre Tätigkeit und ggf. auch als Beweismittel in einem Rechtsstreit. Beide haben einerseits ein Interesse an einem Bestand der Daten nicht nur für die Dauer der Verjährungsfrist, sondern auch darüber hinaus. Beispielsweise für Impfdaten reichen 36 Monate häufig nicht aus. Andererseits legen beide großen Wert auf eine vertrauliche Behandlung der Dokumentation. Diesen berechtigten Interessen wird am besten dadurch Rechnung getragen, dass nur Arzt und Patient Zugang zu elektronisch gespeicherten Patientendaten haben und nur beide im Einvernehmen über eine Weitergabe der Daten an andere ärztliche Dienste entscheiden. Wegen der mit einer zentralen Lösung verbundenen Risiken plädiert auch die DSK für eine dezentrale Speicherung, bei der nur behandelnder Arzt/Krankenhaus und der Patient über die Daten verfügen und diese ggf. an andere weitergeben können. Dem Ziel, Verbesserung der allgemeinen Planung und Steuerung im Gesundheitswesen, könnte auch durch Daten ohne Personenbezug ausreichend Rechnung getragen werden.[288]

Aus den genannten Gründen sollte der Zugang zu personenbezogenen Daten in ELGA auf Ärzte und Patienten beschränkt werden, wie in § 9 Ziffer 12 DSG 2000 und Art. 8 Abs. 3 DS-RL vorgesehen, und nur mit gesteckter eCard möglich sein.[289] Unabhängig davon sollte ELGA modular aufgebaut und auf diese Weise sichergestellt werden, dass die Ärzte und ärztlichen Dienste nur Zugang zu den für ihre jeweilige Disziplin relevanten Informationen erhalten. Sofern Daten für Zwecke der Kontrolle, der Gesundheitsverwaltung und der Steuerung des Gesundheitssystems verwendet

---

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_de.pdf, letzte Abfrage 19.01.2012.

[288] Stellungnahme der Datenschutzkommission zum ELGA-Gesetz vom 11.03.2011, S. 2, https://www.dsk.gv.at/DocView.axd?CobId=42793, letzte Abfrage 19.01.2012.

289 Österreichische Ärztezeitung vom 9-10.05.2011, ELGA: Nur ein IT-Förderungsprojekt? Ziffer 17, http://www.aerztezeitung.at/archiv/oeaez-2011/oeaez-9-10052011/elga-it-foerderungsprojekt-datenschutz-zusatznutzen.html , letzte Abfrage 19.01.2012.

werden, sollte dies nur auf der Grundlage anonymisierter Daten möglich sein. Eine Löschung von Daten sollte nur erfolgen, wenn diese erkennbar nicht mehr benötigt werden und im Einvernehmen von Arzt und Patient erfolgen.

8. Datenverwendung und Datenschutz bei der Sicherheitspolizei

8.1 Einleitung

Die Gewährleistung eines möglichst hohen Grades an Sicherheit für ihre Bürger gehört zu den wesentlichen Aufgaben eines Staates. In der Folge der terroristischen Angriffe in New York (2001), Madrid (2004) und London (2005) sind in vielen Ländern die Möglichkeiten zur Überwachung und damit auch der Beschaffung und Verwendung von personenbezogenen Daten erheblich ausgeweitet worden. Das gilt auch für Österreich. In Bezug auf die Erweiterung polizeilicher Befugnisse sind z.B. die Regelungen der SPG-Novelle 2005 für die Überwachung sog. Kriminalitätsschwerpunkte mittels Bild- und Tonaufzeichnungsgeräten zu nennen, ferner die Bestimmungen der Novelle 2008 über die Errichtung einer zentralen Analysedatei für mit beträchtlicher Strafe bedrohter Gewaltdelikte, ferner die Verpflichtung der Betreiber öffentlicher Telekommunikationsdienste, Auskünfte über Internetprotokolladressen und die internationale Mobilteilnehmerkennung sowie Einsatz technischer Mittel zur Standortbestimmung der internationalen Mobilteilnehmerkennung. Die letzte Änderung erfolgte mit der SPG-Novelle 2011[290], die im Wesentlichen am 01.04.2012 einschließlich der Vorschriften über die Vorratsdatenspeicherung in Kraft getreten ist.

Bei den Änderungen haben schwerpunktmäßig erweiterte Handlungsgrundlagen für die Ermittlungstätigkeit im Vordergrund gestanden. Während früher die Polizei erst tätig geworden ist, wenn Handlungen gegen die öffentliche Sicherheit und Ordnung erkennbar geworden sind, d.h. die Polizei darauf hinweisende Informationen erhalten hatte, ist den Sicherheitsorganen in letzter Zeit verstärkt die Aufgabe übertragen worden, Maßnahmen zur Vorbeugung von gefährlichen Angriffen gegen die öffentliche Sicherheit, § 22 Abs. 2 und 3 SPG, zu ergreifen und entsprechende strategische Analysen einschließlich der dazu erforderlichen Verwendung personenbezogener Daten vorzunehmen, § 53 a Abs. 2 SPG. In diesem Zusammenhang ist auch die erweiterte Gefahrenforschung zur Erkennung krimineller Strukturen und damit ver-

---

[290] Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Polizeikooperationsgesetz und das Bundesgesetz über die Einrichtung und Organisation des Bundesamts zur Korruptionsprävention und Korruptionsbekämpfung geändert werden (SPGNovelle 2011),BGBl. 2012 vom 26.03.2012, S.1-6. http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2012_I_13/BGBLA_2012_I_13.pdf , letzte Abfrage 29.03.2012.

bundener Gefahren zu nennen, § 21 Abs. 3 SPG. Besondere Beachtung haben die am 1. Jänner 2008 in Kraft getretenen Bestimmungen des § 53 Abs. 3a und 3b SPG gefunden, u.a. auch wegen der Art und Weise ihres Zustandekommens.[291] Die genannten Vorschriften enthalten Rechtsgrundlagen für Auskünfte von Betreibern von Telekommunikationseinrichtungen über IP-Adressen, § 53 Abs. 3a SPG, die internationale Mobilteilnehmerkennung (IMSI) und den Einsatz technischer Mittel zu ihrer Lokalisierung, § 53 Abs. 3b SPG (sog. IMSI-Catcher).

Die Tätigkeit der Polizei ist sowohl bei der Gefahrenabwehr als auch bei der Ermittlung von Personen und ggf. deren erkennungsdienstlicher Behandlung mit der Verwendung von Daten im Sinne von § 4 Ziffer 8 DSG 2000 verbunden, so dass zwangsläufig vielfach in die durch § 1 Abs. 1 DSG und Art. 8 Abs. 1 EMRK grundrechtlich geschützte Privatsphäre eingegriffen wird. Durch die neuen gesetzlichen Regelungen sind die Befugnisse der Sicherheitspolizei zur Erhebung von Daten erweitert worden, so dass dadurch der Datenschutz für die von der Sicherheitspolizei verwendeten Daten zusätzliche Bedeutung erlangt.

Eingriffe der Polizeibehörden gleich welcher Art sind an die in § 1 Abs. 2 DSG 2000 und Art. 8 Abs. 2 EMRK aufgeführten Voraussetzungen geknüpft. Für die jeweiligen Eingriffe in das Grundrecht auf Schutz persönlicher Daten müssen gesetzliche Grundlagen bestehen und sie müssen Maßnahmen darstellen, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung strafbarer Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte Anderer notwendig sind. Im Einzelnen sind die Eingriffsvoraussetzungen in Kapitel 2 beschrieben worden.

---

[291] Peissl u. andere, Privatsphäre 2.0, S. 20, http://www.arbeiterkammer.at/bilder/d89/Studie_Datenschutz.pdf , letzte Abfrage 16.01.2012, *„Bereits die Art der Beschlussfassung dieses Gesetzes löste in weiten Teilen der Bevölkerung Unmut aus: Es wurde am Ende einer 15 Stunden dauernden Sitzung des Nationalrates, der letzten im Jahr 2007, am späten Abend beschlossen, ohne, wie es sonst üblich gewesen wäre, vorher den zuständigen Innenausschuss des Parlaments damit zu befassen. Darüber hinaus wurden von den Parlamentsfraktionen der Regierungsparteien kurz vor der Abstimmung noch Änderungsanträge eingebracht, die die Befugnisse der Polizei gegenüber der Gesetzesvorlage stark ausweiteten.“;* zur Kritik siehe auch: http://www.heise.de/newsticker/meldung/Neues-oesterreichisches-Sicherheitspolizeigesetz-in-der-Kritik-171122.html , letzte Abfrage 16.01.2012.

Im Rahmen der Prüfung der gesetzlichen Grundlagen für bestimmte Eingriffe ist erheblich, ob die eingreifende Polizeibehörde sachlich und örtlich zuständig ist. Ist das nicht der Fall, mangelt es bereits an der Legitimation für den Eingriff.[292]

8.2 Sachliche und örtliche Zuständigkeit bei der Sicherheitspolizei

Im Allgemeinen versteht man materiell unter polizeilichen Maßnahmen alle Verwaltungstätigkeiten, die unter Androhung oder Anwendung von Zwang auf die Vorbeugung oder die Abwendung von Gefahren von oder Störungen der öffentlichen Ordnung abzielen (Gefahrenabwehr durch Zwangsmaßnahmen).[293] Organisatorisch umfasst die Institution Polizei alle Behörden, die Aufgaben der Polizei im beschriebenen materiellen Sinne wahrnehmen.[294]
Bei der Polizei im materiellen Sinne ist zwischen Verwaltungspolizei und Sicherheitspolizei zu differenzieren. Verwaltungspolizeiliche Aufgaben beziehen sich auf Maßnahmen zur Abwehr von Gefahren, die im Zusammenhang mit bestimmten verwaltungsrechtlichen Materien, z.B. Baurecht oder Gewerberecht, ergriffen werden (Baustopp, Gewerbeverbot). Es geht dabei um die Beseitigung von Gefahren in einer bestimmten Sachmaterie.

Die Abwehr von Gefahren, die typischerweise nicht im Zusammenhang mit einer bestimmten Verwaltungsmaterie entstehen, die sog. allgemeinen Gefahren, fällt in die Zuständigkeit der Sicherheitspolizei, ebenso die erste allgemeine Hilfeleistungspflicht, § 3 SPG iVm. Art. 10 Abs. 1 Ziffer 7 B-VG. In der genannten Verfassungsbestimmung sind neben der Umschreibung der Aufgaben der Sicherheitspolizei einige Bereiche der Sicherheitsverwaltung aufgeführt, die jedoch nicht Gegenstand des SPG sind und hier nicht näher betrachtet werden.[295]

---

[292] Flendrovsky, Datenverwendung und Datenschutz in der allgemeinen Sicherheitspolizei, in Bauer/Reimer, Handbuch Datenschutzrecht, 2009, S. 353; Hauer/Keplinger, Sicherheitspolizeigesetz, Kommentar, 4. Aufl. 2011, § 5 Anm. 2.2.2.
[293] Flendrovsky, Datenverwendung und Datenschutz in der allgemeinen Sicherheitspolizei, in Bauer/Reimer, Handbuch Datenschutzrecht, 2009, S. 347.
[294] Flendovsky aaO., S. 353.
[295] Art. 10 Abs.1 Ziffer 7 B-VG lautet:
" Bundessache ist die Gesetzgebung und die Vollziehung in folgenden Angelegenheiten: ..... 7. Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit einschließlich der ersten allgemeinen Hilfeleistung, jedoch mit Ausnahme der örtlichen Sicherheitspolizei; Vereins- und Versammlungsrecht; Personenstandsangelegenheiten einschließlich des Matrikelwesens und der Namensän-

Die Organisation und örtliche Zuständigkeit ergeben sich aus den §§ 5, 6 und 7 bis 14 SPG.

Art 78 a B-VG und § 4 Abs. 1 SPG bestimmen den Bundesminister des Inneren als oberste Sicherheitsbehörde. Diesem sind die Sicherheitsdirektionen für die einzelnen Bundesländer unterstellt, Art. 78 b B-VG, den wiederum die Bezirksverwaltungsbehörden und die Bundespolizeidirektionen nachgeordnet sind, § 4 Abs. 2 SPG. Für Wien ist die Bundespolizeidirektion zugleich Sicherheitsdirektion, der Polizeipräsident auch Sicherheitsdirektor, Art. 78 b Abs. 1 B-VG letzter Satz.

Der Aufbau des Wachkörpers Bundespolizei ist in § 10 Abs. 1 SPG geregelt. Für jedes Bundesland ist ein Landespolizeikommando zu bilden, dem die Bezirks- und Stadtpolizeikommanden sowie deren Polizeidirektionen unterstellt sind. Den Exekutivdienst für die genannten Sicherheitsbehörden leisten gemäß § 5 Abs. 1 SPG die Organe des öffentlichen Sicherheitsdienstes. Dies sind die Angehörigen des Wachkörpers Bundespolizei, der Gemeindewachkörper und die des rechtskundigen Dienstes bei den Sicherheitsbehörden, wenn diese Organe zur Ausübung unmittelbarer Befehls- und Zwangsgewalt ermächtigt sind, § 5 Abs. 2 SPG.

Die örtliche Zuständigkeit der Bundespolizeidirektionen ergibt sich aus einer Rechtsverordnung[296] der Bundesregierung auf der Grundlage von Art. 78 c Abs. 2 B-VG. Außerhalb des Wirkungsbereiches der Bundespolizeidirektionen obliegt die Sicherheitsverwaltung den Bezirksverwaltungsbehörden. Diesen sind die Bezirks- und Stadtpolizeikommanden im Rahmen der Sicherheitsverwaltung unterstellt, § 9 Abs. 1 SPG.

Die Sicherheitsbehörden sind grundsätzlich nur innerhalb ihres örtlichen Zuständigkeitsbereichs zu sicherheitsdienstlichen Handlungen ermächtigt. Das ergibt sich aus § 14 Abs. 3 SPG, der ausnahmsweise einen örtlich nicht zuständigen Exekutivdienst

---

derung; Fremdenpolizei und Meldewesen; Waffen-, Munitions- und Sprengmittelwesen, Schießwesen; "

Übersicht über sicherheitspolizeiliche Nebengesetze bei Hauer/Keplinger Sicherheitspolizeigesetz, Kommentar, 4. Aufl. 2011, § 3 Ziffer 4.

[296] Verordnung der Bundesregierung über die Errichtung von Bundespolizeidirektionen und die Festlegung ihres örtlichen Wirkungsbereiches, BGBl. II 1999/56.

ermächtigt, sicherheitsdienstliche Amtshandlungen vorzunehmen, wenn die örtlich zuständige die notwendigen Maßnahmen nicht rechtzeitig treffen kann. Dabei gelten die jeweiligen Maßnahmen als Amtshandlungen der zuständigen Bundespolizeidirektion oder Bundesverwaltungsbehörde, welche von dem einschreitenden Organ unverzüglich zu unterrichten sind.

Soweit sicherheitspolizeiliche Aufgaben anstehen, die nicht in den Zuständigkeitsbereich der örtlichen Sicherheitspolizei fallen, ist die allgemeine (überörtliche) Sicherheitspolizei zuständig. Diesen Aufgabenbereich regelt das SPG. Unter den in § 9 Abs. 3 und 4 SPG genannten Voraussetzungen können Gemeindewachkörpern bestimmte sicherheitspolizeiliche Aufgaben übertragen werden.

Die Sicherheitspolizei ist von der Kriminalpolizei abzugrenzen, die zwar Sicherheitsbehörde, aber nicht Sicherheitspolizei im Sinne von § 2 SPG ist. Die Kriminalpolizei ist Bestandteil des Strafrechtswesens, Art. 10 Abs. 1 Ziffer 6 B-VG.[297] Sobald ein bestimmter Mensch einer strafbaren Handlung verdächtigt wird, gelten die Bestimmungen der StPO, § 22 Abs. 3 Satz 2 SPG. Eine Reihe von Bestimmungen bleiben jedoch davon unberührt: § 53 Abs. 1 SPG (Datenverarbeitung für die erste Hilfeleistungspflicht, Abwehr krimineller Verbindungen, Abwehr gefährlicher Angriffe, Vorbeugung gegen wahrscheinliche Angriffe, für Fahndungszwecke und Aufrechterhaltung der öffentlichen Ordnung), § 53 a Abs. 2-4 und 6 SPG (Datenverarbeitung für operative und strategische Analyse Evidenzhaltung von Wegweisungen und Betretungsverboten, Datenverwendung im Informationsverbundsystem), § 57 SPG (Rahmenbestimmungen für EKIS), § 58 SPG (Sperrung und Löschung von Daten in EKIS) und §§ 58 a-d SPG (Vorschriften für zentrale Dateien wie Sicherheitsmonitor, Vollzugsverwaltung, zentrale Gewaltschutzdatei und zentrale Analysedatei). In der Literatur wird auf die Problematik so genannter doppelfunktionaler Akte hingewiesen.[298] So bleibt die Sicherheitspolizei auch in der Phase des Strafprozesses gemäß § 21 Abs. 2 SPG verpflichtet, gegen gefährliche Angriffe unmittelbar einzuschreiten, so

---

[297] Art 10 Abs. 1 Ziffer 6 B-VG lautet auszugsweise: *Bundessache ist die Gesetzgebung und die Vollziehung in folgenden Angelegenheiten: 6. ..... Strafrechtswesen mit Ausschluss des Verwaltungsstrafrechtes und des Verwaltungsstrafverfahrens in Angelegenheiten, die in den selbständigen Wirkungsbereich der Länder fallen; Justizpflege; Einrichtungen zum Schutz der Gesellschaft gegen verbrecherische oder sonstige gefährliche Personen; .....*

[298] Wessely in Raschauer (Hrsg.)Datenschutzrecht 2010, S. 129/130.

dass eine Handlung der Polizei u.U. sowohl nach strafprozessualen als auch sicherheitspolizeilichen Gesichtspunkten zu beurteilen sei. Unter Berücksichtigung des letzten Satzes in § 21 Abs. 2 SPG „*Hierfür ist dieses Bundesgesetz auch dann maßgeblich, wenn ein bestimmter Mensch einer strafbaren Handlung verdächtig ist*" ist jedoch davon auszugehen, dass nach Einleitung eines Ermittlungsverfahren gegen eine bestimmte Person bei der Abwehr gefährlicher Angriffe, die von dieser Person ausgehen, ungeachtet § 22 Abs. 3 SPG die Bestimmungen des SPG maßgeblich sind.[299]

In Bezug auf die Verarbeitung personenbezogener Daten von Personen, die einer Straftat verdächtigt werden, gibt es also Überschneidungen mit der Kriminalpolizei, die indes im Interesse der Sache notwendig erscheinen.[300]

Über funktionale Zuständigkeiten enthält das SPG keine umfassenden Bestimmungen, d.h. kaum Vorschriften darüber, welcher Ebene bestimmte Aufgaben zugewiesen sind. Nur in Einzelfällen, §§ 14 a (Berufungen gegen Bescheide der Bundespolizeidirektionen und Bundeverwaltungsbehörden) sowie 76 SPG (erkennungsdienstliche Maßnahmen) bestehen spezielle Regelungen. Deshalb muss man davon ausgehen, dass die Sicherheitsbehörden innerhalb ihres örtlichen Zuständigkeitsbereichs zu allen Handlungen berechtigt sind, die in den in Art. 10 Abs. 1 Ziffer 7 B-VG und § 3 SPG beschriebenen allgemeinen Aufgabenbereich der Sicherheitspolizei fallen.

8.3 Ausgewählte Beispiele der Datenverwendung bei der Sicherheitspolizei

Die hier interessierenden Regelungen über die Befugnisse der Sicherheitspolizei zur Verwendung von personenbezogenen Daten sind von der jeweiligen Aufgabenstellung abhängig und an sich im Einzelnen in den §§ 51 ff. SPG geregelt.
Nach § 13 Abs. 2 SPG sind die Sicherheitsbehörden jedoch berechtigt, sich auch für die Dokumentation der Amtshandlungen (Protokollierung) der automationsunterstützten Datenverarbeitung zu bedienen. Soweit erforderlich, dürfen dafür personenbezogene Daten, auch sensible im Sinne von § 4 Ziffer 2 DSG 2000, verarbeitet werden, wobei diese Daten nicht als Suchkriterium verwendet werden dürfen, sondern für die Auswahl darf nur ein auf den protokollierten Sachverhalt bezogenes Datum verwen-

---

[299] Hauer/Kepplinger, Sicherheitspolizeigesetz, Kommentar, 4. Auflage 2011, § 21 Anm. 7.
[300] Thanner/Vogl, Sicherheitspolizeigesetz, 4. Aufl. 2010, § 22, zu Abs. 3.

det werden. Mit dieser Regelung soll klargestellt werden, dass die Dokumentation von Amtshandlungen eine Datenverarbeitung außerhalb des Ermittlungsdienstes darstellt, die (als Angelegenheit des inneren Dienstes[301]) nicht den Regelungen der §§ 51 ff. SPG unterfällt.

Ungeachtet dessen hat der VfGH entschieden, dass bei Aufnahme personenbezogener Daten in ein Protokollbuch Grundrechtspositionen der Bürger betroffen werden, durch die subjektive Rechte entstehen können, u.a. Auskunfts- und Löschungsansprüche. Die Regeln des SPG über die Verwendung personenbezogener Daten im Rahmen der Sicherheitspolizei, die §§ 51 ff. SPG, seien heranzuziehen.[302] Diese Auffassung wird mit dem Hinweis kritisiert, dass der VfGH sich in seinem Urteil nicht mit dem Gesetzeswortlaut auseinandergesetzt habe.[303] In der Sache ist dem VfGH aber zuzustimmen. Wenn Grundrechtspositionen berührt werden, können diese nicht durch einfachgesetzliche Bestimmungen übergangen werden. Aus Sicht der betroffenen Bürger ist die Speicherung seiner personenbezogenen Daten in einer Datei des inneren Dienstes nicht minder eingriffsrelevant wie die Aufnahme in eine Ermittlungsdatei.

(Ab 01.01.2014 wird für die vorstehend beschriebene Dokumentation eine spezielle Rechtsgrundlage in einem § 13 a SPG[304] in Kraft treten, mit der klar gestellt wird, dass die Aufbewahrung und Skartierung auf der Grundlage der gesetzlichen Vorschriften zu erfolgen hat. Die Akten im Dienste der Strafrechtspflege sind gesondert aufzubewahren und entsprechend den getroffenen Entscheidungen zu aktualisieren.)

Die auch für die Datenverwendung maßgeblichen Aufgabenstellungen ergeben sich aus den §§ 16 ff. SPG. Personenbezogene Daten dürfen von der Sicherheitspolizei nur verwendet werden, soweit dies für die jeweilige Aufgabe erforderlich ist, § 52 SPG. Im Folgenden werden die Datenverwendungen zur ersten allgemeinen Hilfeleistung, § 19 SPG, die Gefahrenabwehr, § 21 Abs. 1 SPG, die Gefahrenforschung, §§ 16 Abs. 4, 28 a Abs. 1 SPG, und die erweiterte Gefahrenforschung, § 21 Abs. 3 SPG näher betrachtet. Die Rechtsgrundlagen für die Verwendung personenbezoge-

---

[301] Flendrovsky aaO., S. 351-352.
[302] VfGH vom 30.11.2005, B 1158/03, Vfslg. 17.745/2005.
[303] Flendrovsky aaO. , S. 352.
[304] SPG Novelle 2011, BGBl. I vom 26.03.2012, S. 1-6 (2).

ner Daten im Rahmen der Sicherheitspolizei sind im 4. Teil des SPG in den §§ 51 ff. enthalten, der in drei Hauptstücke unterteilt ist: Allgemeines, § 51 SPG, Ermittlungsdienst, §§ 53 bis 63 SPG, und Erkennungsdienst, §§ 64 bis 80 SPG. In § 51 Abs. 1 SPG wird für die Verarbeitung personenbezogener Daten zunächst auf den Grundsatz der Verhältnismäßigkeit verwiesen - im Hinblick auf Art. 8 EMRK und § 1 DSG 2000 eine Selbstverständlichkeit - und außerdem die Verpflichtung, bei der Verarbeitung sensibler und strafrechtlich relevanter Daten angemessene Vorkehrungen zur Wahrung der Geheimhaltungsinteressen der Betroffenen zu treffen. Die Befugnisse zur Datenverwendung unterscheiden sich abhängig von der Aufgabenstellung.

Im Rahmen der **allgemeinen Hilfeleistung** dürfen die Sicherheitsbehörden selbst ermittelte personenbezogene Daten verwenden, § 53 Abs. 1 Ziffer 1 SPG. Entsprechendes gilt für die Gefahrenabwehr und Gefahrenforschung, Ziffer 2, 3 und 4 der genannten Bestimmung sowie die erweiterte Gefahrenforschung, Ziffer 2 a der genannten Bestimmung. Die Sicherheitspolizei darf bei der Erfüllung der genannten Aufgaben auch auf vorhandene Datenbestände, eigene und solche, die sie in der Vollziehung von anderen Bundes- oder Landesgesetzen ermittelt haben, zugreifen. Ein automationsunterstützter Abgleich im Sinne von § 141 StPO (Rasterfahndung) mit den letztgenannten Datenbeständen ist jedoch in diesem Rahmen nicht zulässig, § 51 Abs. 2 SPG, mit den eigenen Datenbeständen aber schon.[305]

Im Rahmen der **allgemeinen Gefahrenabwehr**, darunter sind die Abwehr gefährlicher Angriffe und die Abwehr krimineller Verbindungen zu verstehen, § 16 Abs. 1 SPG, ist die Sicherheitspolizei gemäß § 53 Abs. 3 berechtigt, von allen anderen Behörden Auskünfte zu verlangen. Nach § 53 Abs. 3 SPG sind die Sicherheitsbehörden berechtigt, von den Dienststellen der Gebietskörperschaften, den anderen Körperschaften des öffentlichen Rechts und den von diesen betriebenen Anstalten Auskünfte zu verlangen, die sie für die Abwehr gefährlicher Angriffe, die erweiterte Gefahrenforschung nach Abs. 1 oder für die Abwehr krimineller Verbindungen benötigen. Eine Verweigerung der Auskunft ist nur zulässig, soweit andere öffentliche Interessen die Abwehrinteressen überwiegen oder eine über die übliche Amtsverschwiegenheit (Art. 20 Abs. 3 B-VG) hinausgehende sonstige gesetzliche Verpflichtung zur Verschwie-

---

[305] Hauer/Kepplinger , Sicherheitspolizeigesetz, Kommentar, 4. Auflage 2011, § 53 Anm. 6.

genheit besteht. Mit dieser Bestimmung erhält die Sicherheitspolizei fast uneingeschränkten Zugang zu personenbezogenen Daten bei allen staatlichen Einrichtungen ohne Rücksicht auf den Zweck, für den diese ursprünglich erhoben und gespeichert worden sind. Eine Verweigerung der Auskunft ist nur zulässig, soweit andere, über die Amtsverschwiegenheit hinausgehende, öffentliche Interessen vorrangig sind.

Nach § 53 Abs. 1 Ziffer 3 dürfen die Sicherheitsbehörden personenbezogene Daten für die Abwehr gefährlicher Angriffe (§§ 16 Abs. 2 und 3 sowie 21 Abs. 2 SPG) ermitteln und weiterverarbeiten einschließlich der im Rahmen der Gefahrenabwehr notwendigen Gefahrenforschung (§ 16 Abs. 4 und § 28a SPG). Im Gegensatz zur erweiterten Gefahrenforschung ist hier Voraussetzung für ein Tätigwerden, dass bestimmte Tatsachen die Annahme einer Gefahrensituation rechtfertigen, § 28 a Abs. 1 SPG. In die Rechte eines Menschen dürfen sie bei der Erfüllung der Aufgabe aber nur dann eingreifen, wenn eine solche Befugnis in diesem Bundesgesetz (SPG) vorgesehen ist und wenn andere Mittel zur Erfüllung dieser Aufgaben nicht ausreichen oder wenn der Einsatz anderer Mittel außer Verhältnis zum sonst gebotenen Eingriff steht, § 28 a Abs. 3 SPG.

§ 53 Abs. 1 Ziffer 4 SPG sieht die Verwendung von personenbezogenen Daten für sogenannte Kriminalitätsanalysen vor. Darunter ist eine Methode zum Erkennen des Ausmaßes, der Erscheinungsformen und des Charakters der Kriminalität mit dem Ziel zu verstehen, Erkenntnisse zu ihrer Bewegung, Entwicklung und ihrer beeinflussenden Rahmenbedingungen herauszuarbeiten, um darauf aufbauend Maßnahmen der Kriminalitätsvorbeugung und Bekämpfung entwickeln zu können.[306] Das Verhältnis von § 53 Abs. 1 Ziffer 4 SPG zu dem später eingefügten § 53 a Abs. 2 SPG, der gleichfalls Kriminalitätsanalysen zum Gegenstand hat, ist unklar. In der letztgenannten Bestimmung sind die Datenarten und die betroffenen Personenkreise genau spezifiziert. Nach Lage der Dinge ist § 53a Abs. 2 SPG als Spezialnorm für Kriminalitätsanalysen anzusehen, so dass die darin enthaltenen Beschränkungen für alle Arten von Kriminalitätsanalysen gelten, auch die vor Inkrafttreten der Norm durchgeführten.

---

[306] Thanner/Vogl, Sicherheitspolizeigesetz, 4. Auflage 2010, § 53 Ziffer 11.

Gemäß § 53 Abs. 4 sind die Sicherheitsbehörden für die in Abs. 1 der Bestimmung genannten Zwecke, also auch für die erweiterte Gefahrenforschung, berechtigt, personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff auf allgemein zugängliche Daten, zu ermitteln und weiterzuverarbeiten. Mit dieser Bestimmung soll die Unbegrenztheit der von den Sicherheitsbehörden einsetzbaren Quellen normiert werden. Die Sicherheitsbehörden sollen ermächtigt sein, im Rahmen der Rechtsordnung alles einzusetzen, was geeignet ist, die gewünschten Erkenntnisse zu beschaffen.[307] Die Beschaffung personenbezogener Daten u.a. auch für die erweiterte Gefahrenforschung darf auch im Rahmen verdeckter Ermittlungen erfolgen, wenn die Gefahrenforschung bei Einsatz anderer Mittel aussichtslos wäre, § 54 Abs. 3 SPG.

Die Sicherheitsbehörden dürfen u.a. auch für die erweiterte Gefahrenforschung personenbezogene Bilddaten verwenden, die andere Rechtsträger des öffentlichen und privaten Bereichs rechtmäßig ermittelt und den Sicherheitsbehörden übermittelt haben, § 53 Abs. 5 SPG.

Die Sicherheitsbehörden sind verpflichtet, den Rechtsschutzbeauftragten (ggf. auch nachträglich) zu unterrichten, wenn personenbezogene Daten im Wege der Observation, § 54 Abs. 2 SPG und verdeckten Ermittlung, § 54 Abs. 3 SPG, sowie mit Bild- und Tonaufzeichnungsgeräten ermittelt werden § 91c Abs. 1 SPG. Liegt eine Ermächtigung für die erweiterte Gefahrenforschung vor, § 21 Abs. 3 und 91c Abs. 3 SPG, ist nach Lage der Dinge auch eine Observation ohne weitere Einschaltung des Rechtsschutzbeauftragten möglich. Lediglich, wenn im Rahmen der erweiterten Gefahrenforschung besondere Ermittlungsverfahren nach § 54 Abs. 3 (verdeckte Ermittlung) und Abs. 4 SPG (Einsatz von Bild- und Tonaufzeichnungsgeräten) verwendet werden oder eine Weiterverarbeitung von bei Großveranstaltungen mittels Bild- und Tonaufzeichnung erfassten personenbezogenen Daten für die erweiterte Gefahrenforschung in Betracht kommt, ist eine besondere Ermächtigung des Rechtsschutzbeauftragten erforderlich.

---

[307] Thanner/Vogl, aaO. § 53 Ziffer 7

Verdeckte Ermittlungen sind aber nur zur Abwehr einer kriminellen Verbindung zulässig, wenn die Strafe für die fragliche Tat mit mehr als einem Jahr Freiheitsstrafe bedroht ist, §§ 17 und 54 Abs. 4a SPG.

Der Sicherheitspolizei ist gemäß § 53 Abs. 3 a SPG auch der Zugriff auf Kommunikationsdaten nach folgenden Kriterien gestattet:

1. Für alle Aufgaben dürfen Name, Anschrift und Teilnehmernummer eines bestimmten Anschlusses von den Diensteanbietern verlangt werden.

2. Für die Erfüllung der Hilfeleistungspflicht bei Vorliegen einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen sowie die die Abwehr allgemeiner Gefahren (gefährliche Angriffe und kriminelle Verbindungen gemäß § 16 SPG) können auch die IP-Adressen zu einer bestimmten Nachricht und der Zeitpunkt der Übermittlung verlangt werden.

3. Ebenso kann unter den unter 2. genannten Voraussetzungen der Name des Nutzers zu einer IP-Adresse, dem diese zu einem bestimmten Zeitpunkt zugewiesen war, angefordert werden, letzeres auch, wenn hierfür die Verwendung von Vorratsdaten im Sinne §§ 99 Abs. 5 Ziffer 4 iVm. § 102 a TKG 2003 erforderlich ist.

4. Ferner können im Rahmen der allgemeinen Hilfeleistungspflicht und zur Abwehr allgemeiner Gefahren Name, Anschrift und Teilnehmernummer eines bestimmten Anschlusses durch Bezugnahme auf ein bestimmtes Gespräch durch Bezeichnung eines möglichst genauen Zeitpunktraumes und der passiven Teilnehmernummer angefordert werden.

Nach § 53 Abs. 3 b SPG sind die Sicherheitsbehörden *bei Vorliegen einer gegenwärtigen Gefahr* für das Leben, die Gesundheit oder die Freiheit eines Menschen zur Abwehr dieser Gefahr berechtigt, von den Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die Internationale Mobilteilnehmerkennung der mitgeführten Endeinrichtung zu verlangen.

Zur Gefahrenabwehr gehört auch die Gefahrenforschung, §§ 16 Abs. 4, 19 Abs. 2 und 28 a Abs. 1 SPG. Gefahrenforschung im Sinne von § 28 a Abs. 1 SPG ist so zu verstehen, dass davon sowohl die Feststellung der Ursache einer bekannten Gefahr

erfasst wird als auch die Gefahrenklärung, d.h. die Aufklärung, ob bei Vorliegen von Indizien für eine Gefahr überhaupt eine wirkliche Gefahr besteht.[308]

Von der schlichten Gefahrenforschung ist die erweiterte Gefahrenforschung im Sinne von § 21 Abs. 3 SPG zu unterscheiden. Da die schlichte Gefahrenforschung gemäß §§ 16 Abs.4 und 28 a SPG bereits bei Indizien für eine Gefahr eingreift, ist davon auszugehen, dass die erweiterte Gefahrenforschung bereits früher einsetzt.[309] Nach dem Tatbestand des § 21 Abs. 3 SPG geht es um die Beobachtung von Gruppierungen, bei denen aufgrund bestehender Strukturen und im Hinblick auf zu gewärtigende Entwicklungen in deren Umfeld mit kriminellen Handlungen zu rechnen ist. Dabei muss es sich um mit schwerer Gefahr für die öffentliche Sicherheit verbundene Kriminalität handeln, ohne dass das Gesetz den Kreis in Betracht kommender Straftaten näher eingrenzt. Nach Lage der Dinge brauchen für die erweiterte Gefahrenforschung keine konkreten Tatsachen für die Annahme einer Gefahr vorliegen, es reichen Verdachtsmomente, dass es zu schweren kriminellen Handlungen kommen kann, d.h. eine entsprechende Prognose, die auf die Strukturen der Gruppierung und Entwicklungen in deren Umfeld gestützt wird, [310]schlichte Vermutungen reichen also nicht aus. Es muss die ernsthafte Möglichkeit bestehen, dass sich derartige Handlungen in Zukunft ereignen können.[311]

8.4 Voraussetzungen für Eingriffe der Sicherheitspolizei in das Recht auf Datenschutz

Nach der Grundrechtsbestimmung des § 1 Abs. 2 DSG 2000 dürfen staatliche Behörden, soweit der Betroffene nicht zustimmt oder seine lebenswichtigen Interessen berührt sind, nur auf der Grundlage von Gesetzen in dieses Recht eingreifen, die aus den in Art. 8 Abs.2 EMRK genannten Gründen notwendig sind. Die EMRK ist im Übrigen nicht nur für die Anwendung der genannten Bestimmung maßgeblich, sondern in ihrem gesamten Umfang. Sie hat in Österreich Verfassungsrang.[312] Es ist daher geboten, bei Eingriffen der Sicherheitspolizei in das Recht auf Datenschutz nicht nur

---

[308] Wiederin, Privatsphäre und Überwachungsstaat, 2003, S. 74/75;Thanner/Vogl, Sicherheitspolizeigesetz, 4. Aufl. 2010, § 53 Anm. zu Abs. 1 Ziffer 3, S. 150 f.
[309] Wiederin, aaO. S. 83
[310] Hauer/Kepplinger , Sicherheitspolizeigesetz, Kommentar, 4. Auflage 2011, § 21 Anm. 12.
[311] Wiederin, Privatsphäre und Überwachungsstaat, 2003, S. 88.
[312] BGBl. 210/1958 und BGBl. Nr. 59/1964 zuletzt geändert durch BGBl. I Nr. 2/2008, Art. 2 Ziffer 7

originäre österreichische Gesetze zu prüfen, sondern auch die einschlägigen Bestimmungen der EMRK und die dazu ergangene Rechtsprechung des EGMR. Darüber hinaus sind die europarechtlichen Bestimmungen zum Datenschutz relevant, soweit nicht ausschließlich nationalstaatliche Maßnahmen betroffen sind, die die EU-Verträge nicht berühren, d.h. soweit nicht Maßnahmen der EU oder nationalstaatliche Handlungen bei der Umsetzung oder Anwendung von EU-Recht in Rede stehen, Art. 51 Abs. 1 EUV. Auch insoweit kommt der EMRK eine herausragende Bedeutung zu, weil der EuGH u. a. in der Beurteilung von Fragen des Datenschutzes schon vor Inkrafttreten der GRCh die Bestimmungen der EMRK und die Rechtsprechung des EGMR dazu als allgemein gültige europäische Verfassungsüberlieferung bei der Anwendung der Datenschutzrichtlinie berücksichtigt hat.[313] Mit Inkrafttreten des Lissabon- Vertrages am 01.12. 2009 ist nunmehr eindeutig klargestellt, dass die Grundrechte der EMRK als allgemeine Grundsätze und Teil des Unionsrechts zu betrachten sind, Art. 6 Abs. 3 EUV. Im Zusammenhang mit Rechtsprechung des EGMR, der eine Verletzung des Rechtes auf Datenschutz als Verletzung der Privatsphäre im Sinne von Art. 8 Abs. 1 EMRK ansieht[314], der zitierten Rechtsprechung des EuGH und dem Inkrafttreten des Lissabon-Vertrages wird in der Literatur auch zunehmend von einer Europäisierung des Datenschutzes gesprochen.[315] Wenn die derzeit als Entwurf einer so genannten Grundverordnung vorliegende Kodifikation, durch die DS-RL ersetzt werden soll, und eine neue Richtlinie für den Datenschutz im Rahmen der polizeilichen und justiziellen Zusammenarbeit Wirklichkeit werden sollten, dürfte die Europäisierung des Datenschutzes weitgehend abgeschlossen sein, da den Mitgliedstaaten nur ein enger Regelungsbereich verbleibt.

8.5 Prüfung der Datenschutzregelungen des SPG nach den vom EGMR entwickelten Kriterien

Grundsätzlich gelten die Bestimmungen des DSG 2000 auch für die Sicherheitspolizei. Allerdings enthält § 51 Abs. 2 SPG die Einschränkung „ *soweit nicht ausdrück-*

---

[313] EuGH vom 20.05.2003 in verb. Rechtssachen C-465/00, C-138/01 u. C-139/01(österr. Rundfunk), Slg. I, S. 5018 ff., Rd.-Nr. 68 bis 72, http://curia.europa.eu/juris/document/document.jsf?docid=48330&doclang=DE&mode=&part=1, letzte Abfrage 21.04.2012.

[314] Urteil des EGMR vom 04.12.2008, Marper gg. Vereinigtes Königreich, Ziffer 66, EuGRZ 2009, S. 299 ff. (307).

[315] Siehe dazu insbes. Britz, Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, S. 1 ff.

lich etwas Anderes angeordnet wird". Daraus ist aber nicht auf einen Vorrang des SPG gegenüber dem DSG 2000 zu schließen. Die Vorschrift ist so zu verstehen, dass das SPG für die Arbeit der Sicherheitspolizei spezifische Regelungen für die Verwendung von Daten, Sicherungen und Löschungsfristen enthält.[316] Soweit das SPG lediglich speziell auf die Arbeit der Sicherheitspolizei ausgerichtete Ermächtigungen oder Konkretisierungen aufweist, so steht dies im Einklang mit § 8 Abs. 1 Ziffer 1 DSG 2000, der derartige Regelungen voraussetzt: „*Gemäß § 1 Abs. 1 bestehende schutzwürdige Geheimhaltungsinteressen sind bei der Verwendung dann nicht verletzt, wenn 1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung dieser Daten besteht", f*erner dann nicht, wenn die Verwendung der Daten gemäß § 8 Abs. 3 Ziffer 1 und Abs. 4 Ziffer 2 DSG 2000 „*für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist".* Entsprechende Regelungen enthält § 9 DSG 2000 für die Verwendung sensibler Daten durch öffentliche Auftraggeber. Allerdings müssen derartige Spezialbestimmungen auch die Anforderungen von § 1 Abs. 2 DSG erfüllen und einer Prüfung nach Art. 8 Abs. 2 EMRK standhalten.

Die Behörden der Sicherheitspolizei sind im Übrigen nach § 17 Abs. 3 Ziffer 5 DSG 2000 im Rahmen der Vorbeugung, der Verhinderung und der Verfolgung von Straftaten von der Meldepflicht an die DSK ausgenommen, soweit dies zur Verwirklichung des Zweckes der Datenanwendung erforderlich ist . In derartigen Fällen besteht auch keine Pflicht des Auftraggebers zur Information des Betroffenen, § 24 Abs. 4 DSG 2000. Auch das Recht auf Auskunft ist eingeschränkt, § 26 Abs. 2 Ziffer 5 DSG 2000. Die Verweigerung einer Auskunft unterliegt aber nach § 26 Abs. 2 letzter Satz DSG 2000 der Kontrolle durch die DSK nach § 30 Abs. 3 DSG 2000.

In § 53 Abs. 1 SPG sind die Zwecke aufgelistet, für welche personenbezogene Daten ermittelt und verarbeitet werden dürfen. Soweit es sich dabei um Zwecke handelt, die im Rahmen der herkömmlichen Polizeiarbeit liegen, also der Verhinderung und Beseitigung von konkreten Gefahren für die öffentliche Sicherheit und Ordnung und die Verfolgung von Straftaten, begegnet die Verwendung von personenbezogenen Da-

---

[316] Flendrovsky in Bauer, Reimer (Hrsg.), Handbuch Datenschutzrecht, 2009, S. 354; Hauer/Kepplinger, Sicherheitspolizeigesetz, Kommentar 4. Aufl. 2011, § 51, Ziffer 8 u. 9.

ten keinen grundsätzlichen Bedenken. Der EGMR hat den nationalen Gesetzgebern insoweit einen Ermessensspielraum eingeräumt, der allerdings durch die Gerichte überprüft werden kann.[317] In den Fällen jedoch, in denen personenbezogene Daten anlasslos und ohne Kenntnis der Betroffenen, gewissermaßen auf Vorrat, verwendet werden, sind zusätzliche Anforderungen zu erfüllen.[318] Zunächst sollen jedoch die Vorschriften und die Voraussetzungen für ihre Anwendung dargestellt werden, die der Sicherheitspolizei die Speicherung und Verarbeitung von personenbezogenen Daten ohne Vorliegen einer konkreten Gefährdungssituation erlauben.

8.5.1 Regelungen des SPG, die eine Speicherung von personenbezogenen Daten ohne Vorliegen einer sonst üblichen Gefahrensituation im Sinne von § 16 Abs. 1 SPG ermöglichen

An erster Stelle ist hier die Bestimmung des § 53 Abs. 1 Ziffer 2a SPG zu nennen. Danach dürfen die Sicherheitsbehörden unter den Voraussetzungen des § 91 c Abs. 3 SPG personenbezogene Daten für die erweiterte Gefahrenforschung (§ 21 Abs. 3 SPG) ermitteln und verarbeiten. Erweiterte Gefahrenforschung im Sinne von § 21 Abs. 3 SPG bedeutet die *Beobachtung von Gruppierungen, wenn im Hinblick auf bestehende Strukturen und auf zu gewärtigende Entwicklungen in deren Umfeld damit zu rechnen ist, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität, insbesondere zu weltanschaulich oder religiös motivierter Gewalt kommt*. Seit der SPG-Novelle 2011[319], die am 01.04.2012 in Kraft getreten ist, ist die erweiterte Gefahrenforschung auf die Beobachtung von Einzelpersonen ausgedehnt worden, *die*

---

[317] EGMR-Urteil vom 16.12.1997, Camendizid gegen Schweiz, , Ziffer 44, ÖJZ 1998,S. 797 f., „ *Nach der stRsp des GH impliziert der Begriff der „Notwendigkeit", daß der Eingriff einem dringenden sozialen Bedürfnis entspricht und insb daß er gegenüber dem verfolgten Ziel verhältnismäßig ist; bei der Entscheidung, ob ein Eingriff „in einer demokratischen Gesellschaft notwendig" ist, wird der GH darauf Bedacht nehmen, daß den Vertragsstaaten ein Ermessensspielraum belassen ist.*".

[318] EGMR Urteil vom 04.05.2000 Rotaru gg. Rumänien, ÖJZ 2001, 74 ff., Ziffer 52: *„ The Court reiterates its settled case-law, according to which the expression "in accordance with the law" not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects."*
http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Rotaru&sessionid=98053067&skin=hudoc-en, letze Abfrage 01.06,2012.

[319] SPG-Novelle 2011, BGBl. I vom 26.03.2012, S. 1-6.

a.) sich öffentlich oder in schriftlicher oder elektronischer Kommunikation für Gewalt gegen Menschen, Sachen oder die verfassungsmäßigen Einrichtungen ausspricht oder
b.) sich Mittel und Kenntnisse verschafft, die sie in die Lage versetzt, Sachschäden in großem Ausmaß oder die Gefährdung von Menschen herbeizuführen, wenn damit zu rechnen ist, dass sie eine mit schwerer Gefahr für die öffentliche Sicherheit verbundene weltanschaulich oder religiös motivierte Gewalt herbeiführt.

Mit den entsprechenden Maßnahmen darf jedoch erst nach Vorliegen einer Ermächtigung des Rechtschutzbeauftragten begonnen werden, § 91c Abs. 3 SPG.

8.5.2 Exkurs zur Strafprozessordnung

In diesem Zusammenhang sei auf die vergleichbaren Vorschriften der Strafprozessordnung hingewiesen, die für Strafverfahren gelten, d.h. den Fall, dass Kriminalpolizei oder Staatsanwaltschaft bereits damit begonnen haben, zur Aufklärung des Verdachts einer Straftat gegen eine bekannte oder unbekannte Person ermitteln, § 1 Abs. 2 StPO. Wenn die Ermittlungen durch Observation, also das heimliche Beobachten erfolgen, und diese Maßnahme durch technische Mittel unterstützt wird oder über 48 Stunden ausgedehnt werden soll, so ist sie nur dann zulässig, wenn der Verdacht einer vorsätzlich begangenen Straftat besteht, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, § 130 Abs. 3 StPO. Außerdem ist in diesen Fällen eine Anordnung der Staatsanwaltschaft für die Durchführung der Observation erforderlich. Eine Observation darf über den in § 130 Abs. 3 Ziffer 2 StPO vorgesehenen Zeitraum von 48 Stunden bis längstens vierzehn Tage fortgesetzt werden, sofern die Kriminalpolizei der Staatsanwaltschaft unverzüglich nach der Fristüberschreitung berichtet §§ 100 Abs. 2 Ziffer 2, 133 StPO. Derartige Beschränkungen bestehen für die Observation im Rahmen der erweiterten Gefahrenforschung der Sicherheitspolizei nicht, obwohl nicht einmal ein konkreter Verdacht gegen eine oder mehrere Personen besteht.

Im Rahmen des strafrechtlichen Ermittlungsverfahrens können systematische verdeckte Ermittlungen über einen längeren Zeitraum nur auf Anordnung der Staatsanwaltschaft durchgeführt werden, §§ 131 Abs. 2 und 133 StPO. Auch die Staatsanwaltschaft benötigt für bestimmte Maßnahmen eine richterliche Bewilligung, so z.B. für körperliche Untersuchungen, § 123 Abs. 3 StPO, Auskunft über Daten einer Nachrichtenübermittlung, §§ 134 Ziffer 2 und 137 Abs. 1 Satz 2 StPO, Überwachung von Nachrichten, §§ 134 Ziffer 3 und 137 Abs. 1 Satz 2 StPO, ferner Observation, §§ 134

Ziffer 4, 137 Abs. 1 Satz 2 StPO. Für die Aufgaben der Sicherheitspolizei bestehen vergleichbare Beschränkungen nicht. Darüber hinaus besteht auch im strafprozessualen Ermittlungsverfahren die Einrichtung des Rechtsschutzbeauftragten. Für bestimmte Ermittlungsmaßnahmen benötigt die Staatsanwaltschaft neben der richterlichen Einwilligung auch die des Rechtsschutzbeauftragten, z.B. für verdeckte Ermittlungen, Observation und automationsunterstützten Datenabgleich, § 147 Abs. 1 StPO.

8.5.3 Entsprechen die Voraussetzungen für die anlasslose und geheime Verwendung personenbezogener Daten im Rahmen der erweiterten Gefahrenforschung (§ 21 Abs. 3 SPG) den Anforderungen des Art. 8 Abs. 2 EMRK?

Wie oben beschrieben, ist die Sicherheitspolizei im Rahmen der erweiterten Gefahrenforschung, d.h. wenn sie damit rechnet, dass von bestimmten Gruppierungen und Strukturen eine die öffentliche Sicherheit bedrohende Kriminalität ausgeht, berechtigt, personenbezogene Daten zu beschaffen und verarbeiten. Dabei sind alle öffentlichen Einrichtungen verpflichtet, auf Anforderung entsprechende Auskünfte zu erteilen. Eine Verweigerung ist, wie bereits erwähnt, grundsätzlich nicht zulässig, § 53 Abs. 3 SPG. Die Sicherheitsbehörden sind im Rahmen der erweiterten Gefahrenforschung auch berechtigt, Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel zu beschaffen und zu verarbeiten, § 53 Abs. 4. Außerdem dürfen sie für diese Aufgabenstellung auch auf personenbezogene Bilddaten zugreifen, die Rechtsträger des privaten und öffentlichen Bereiches mittels Bild- und Tonaufzeichnungsgeräten rechtmäßig ermittelt haben, § 53 Abs. 5 SPG. Auch Datenerhebungen im Rahmen der Observation und der verdeckten Ermittlung, § 54 Abs. 2 Ziffer 1 und Abs. 3 SPG, sind für die erweiterte Gefahrenforschung zulässig.

Allerdings ist die Sicherpolizei gehalten, vor Aufnahme von Aktivitäten der erweiterten Gefahrenforschung eine Ermächtigung des Rechtsschutzbeauftragten einzuholen, § 91 c Abs. 3 SPG.

Unter Berücksichtigung der bisherigen Rechtsprechung des EGMR stellen sich zu den beschriebenen Regelungen drei Fragen. Ist der Anwendungsbereich der Bestimmungen über die erweiterte Gefahrenforschung hinreichend gesetzlich bestimmt, sind ausreichende Sicherungen gegen Missbrauch vorgesehen und den Anforderungen des EGMR entsprechende Löschungsregeln vorhanden?

Bei der Beurteilung dieser Fragen muss man davon ausgehen , dass die Recherchen der Sicherheitspolizei im Rahmen der erweiterten Gefahrenforschung geheim erfolgen und die Betroffenen davon regelmäßig vor Aufnahme der strafprozessualen Ermittlungen keine Kenntnis erhalten und sich gegen die damit verbundenen Eingriffe in ihre Privatsphäre auch nicht mit Rechtsmitteln wehren können.

Die Anwendung von Art. 8 Abs. 1 EMRK setzt zunächst voraus, dass ein Eingriff in ein geschütztes Rechtsgut stattgefunden hat. Bereits die bloße Speicherung von Daten und deren weitere Verwendung stellen einen Eingriff dar, der der Rechtfertigung bedarf.[320]

Für die Rechtfertigung eines Eingriffs nach Art. 8 Abs. 2 EMRK ist eine gesetzliche Grundlage für den Eingriff erforderlich, die man hier in den zitierten Bestimmungen als gegeben ansehen kann.

a.) Erfüllt § 21 Abs. 3 SPG die Qualitätsanforderungen des EGMR?

Die betreffenden Vorschriften müssen so klar und präzise sein, dass Betroffene - ggf. mit entsprechender Beratung - in der Lage sind, ihr Verhalten danach auszurichten.[321] Die Anforderungen an die hinreichende Bestimmtheit und die Vorhersehbarkeit des innerstaatlichen Rechts sind dort besonders hoch, wo es sich um geheime Maßnahmen handelt.[322] Klar ist, dass die Sicherheitspolizei im Rahmen der erweiter-

---

[320] EGMR Urteil vom 26.03.1987, Leander gg. Schweden, EGMR-E 3, S. 430, Ziffer 48: *„Sowohl das Speichern von Daten als auch ihre Weitergabe, verbunden mit der Verweigerung einer Möglichkeit zum Widerspruch gegen die Weitergabe durch Herrn Leander, führen zu einem Eingriff in das Recht auf Achtung des Privatlebens, wie es Art. 8 Abs. 1 gewährt“* ; Grabenwarter, Europäische Menschenrechtskonvention, 4. Aufl. 2009, § 22 Rd.-Nr.: 26.

[321] EGMR Urteil vom 20.05.1999, Rekvényi gg. Ungarn**,** ÖJZ 2000, S. 235 ff, Ziffer 34: *“According to the Court’s well-established case-law, one of the requirements flowing from the expression “prescribed by law” is foreseeability. Thus, a norm cannot be regarded as a “law” unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.”*, http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Rekv%E9nyi&sessionid=98053603&skin=hudoc-en, letzte Abfrage 01.06.2012.

[322] Grabenwarter aaO. § 22 Rd.-Nr.: 34; EGMR Urteil vom 02.08.1984, Malone gg. Vereinigtes Königreich, EGMR-E 2, S. 452 ff, Ziffer 68: „Der Gerichtshof hat ….. entschieden, dass *„ein Gesetz, das Ermessen (pouvoir d’appréciation / discretion) einräumt, die Reichweite des Ermessens angeben muss“, wenn auch die Einzelheiten der Bedingungen und der zu beachtenden Verfahren nicht in demselben Gesetz enthalten sein müssen……. Folglich muss das Gesetz Reichweite und Ausübungsmodalitäten einer solchen Ermächtigung hinreichend klar festlegen, um dem Einzelnen unter Berücksichtigung des verfolgten rechtmäßigen Zieles einen angemessenen Schutz vor Willkür zu gewähren. Ausübungsmodalitäten einer solchen Ermächtigung hinreichend klar festlegen, um dem Einzelnen*

ten Gefahrenforschung nicht erst dann tätig werden kann, wenn sich schon eine konkrete Gefahr für die öffentliche Sicherheit abzeichnet, sondern bereits im Vorfeld, wenn sie bei bestimmten Gruppen und deren Strukturen sowie deren erwarteter Entwicklungen mit einer schweren Gefahr für die öffentliche Sicherheit durch kriminelle Handlungen rechnet.[323] Bei der Formulierung § 21 Abs. 3 SPG *„wenn im Hinblick auf zu gewärtigende Entwicklungen mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität zu rechnen ist“* handelt es sich um unbestimmte Begriffe. Was bedeutet „zu gewärtigende Entwicklungen“? Im Hinblick auf die Tatsache, dass die Aufgabe der Sicherheitspolizei mit Grundrechtseingriffen verbunden ist, dürfen Eingriffe nicht willkürlich vorgenommen werden. Es müssen nach der oben unter Kapitel 8.3 vorgenommen Abgrenzung zwar noch keine Tatsachen vorliegen, die kriminelle Handlungen als wahrscheinlich erscheinen lassen, aber es reichen Verdachtsmomente, dass es zu schweren kriminellen Handlungen kommen kann, d.h. eine entsprechende Prognose, die auf die Strukturen der Gruppierung und Entwicklungen in deren Umfeld gestützt wird,[324] schlichte Vermutungen reichen also nicht aus. Es muss die ernsthafte Möglichkeit bestehen, dass sich derartige Handlungen in Zukunft ereignen können.[325] Dabei ergibt sich die Frage, ob Grundrechtseingriffe der Sicherheitspolizei nach Art. 8 Abs. 2 EGMR zulässig sind, selbst wenn weder ein konkreter Verdacht gegen bestimmte Personen noch tatsächliche Anzeichen für eine Gefahrenlage bestehen.

Welche Kriminalität bedeutet eine schwere Gefahr für die öffentliche Sicherheit? Hier wäre die Bezeichnung der Tatbestände sinnvoll, mit denen aus Sicht des Gesetzgebers eine schwere Gefahr verbunden ist. Nur solche Taten dürften ggf. verfolgt und bestraft werden (nulla poena sine lege). In Betracht kommen hier die Straftatbestände betreffend kriminelle und terroristische Vereinigungen in den §§ 278 bis 278 d StGB. In diesem Zusammenhang ist auf den Rahmenbeschluss des Rates vom 13.06.2002 zur Terrorismusbekämpfung hinzuweisen, in dem eine umfangreiche Definition zu terroristischen Straftaten und Vereinigungen gegeben wird.[326] Art. 2 Abs. 1

---

unter Berücksichtigung des verfolgten rechtmäßigen Zieles einen angemessenen Schutz vor Willkür zu gewähren.“

[323] Thanner/Vogl, Sicherheitspolizeigesetz, 4. Aufl. 2010, § 21 Anm. 2.

[324] Hauer/Kepplinger , Sicherheitspolizeigesetz, Kommentar, 4. Auflage 2011, § 21 Anm. 12.

[325] Wiederin, Privatsphäre und Überwachungsstaat, 2003, S. 88.

[326] ABl. Vom 22.6.2002*.* L 164*/*3*,* Rahmenbeschluss des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung.

des Rahmenbeschlusses definiert als „terroristische Vereinigungen“ „*einen auf längere Dauer angelegten organisierten Zusammenschluss von mehr als zwei Personen, die zusammenwirken, um terroristische Straftaten zu begehen. Der Begriff „organisierter Zusammenschluss“ bezeichnet einen Zusammenschluss, der nicht nur zufällig zur unmittelbaren Begehung einer strafbaren Handlung gebildet wird und der nicht notwendigerweise förmlich festgelegte Rollen für seine Mitglieder, eine kontinuierliche Zusammensetzung oder eine ausgeprägte Struktur hat.“* Diese Definition ist wesentlich genauer als die in § 21 Abs. 3 SPG. Eine vergleichbar bestimmte Regelung wie im Rahmenbeschluss in § 21 Abs. 3 SPG würde das Verständnis der Bestimmung und ihrer Tragweite verbessern.

Auf der Grundlage des im Polizeirecht geltenden Legalitätsprinzips wird deshalb vertreten, dass auch hohe Anforderungen an die Normdichte zu stellen sind. Nur sachliche Gründe, wie die Unmöglichkeit einer bestimmten Regelung oder ein zwingendes Bedürfnis, den rechtsanwendenden Behörden Handlungs- und Entscheidungsspielräume einzuräumen, vermögen die Anforderungen an die Bestimmtheit einer Norm herabzusetzen. Sei aber eine bestimmte Regelung möglich und sinnvoll, dann dürfe der Gesetzgeber auf eine bestimmte Regelung nicht verzichten, habe sich also mit der Einräumung von Ermessen und der Verwendung unbestimmter Rechtsbegriffe zurückzuhalten.[327]

Es ist jedoch anzuerkennen, dass mit der Abwehr terroristischer Angriffe und Maßnahmen gegen kriminelle Verbindungen nicht gewartet werden kann bis eine Gefahr unmittelbar bevorsteht. Eine Terror- und Verbrechensvorbeugung würde dann wohl häufig ins Leere laufen. Es liegt in der Natur der Sache, dass die Wahrscheinlichkeit von Schutzgutverletzungen ungewiss ist, aber die Notwendigkeit besteht, Vorsorge dagegen zu treffen. Es geht deshalb darum, Kriterien zu entwickeln, unter denen auch ohne das Bestehen einer unmittelbar bevorstehenden Gefahr im Interesse der in Art. 8 Abs. 2 EMRK genannten Rechtsgüter „*Leben und Gesundheit anderer* und *Erhaltung der öffentlichen Sicherheit und Ordnung“* in die durch Art. 8 Abs. 1 EMRK geschützte Privatsphäre eingegriffen werden kann. Bloße Vermutungen dürften nicht

---

[327] Schweizer/Müller, Zwecke, Möglichkeiten und Grenzen der Gesetzgebung im Polizeibereich, Leges 2008, S. 379 – 399 (384).
http://www.bk.admin.ch/themen/lang/00938/02124/04296/index.html?lang=de, Abfrage 19.11.2010

ausreichen. Für eine latente Bedrohung müssen tatsächliche Anhaltspunkte bestehen. Die Anforderungen sind umso niedriger anzusetzen, je höherwertig das geschützte Rechtsgut ist und je stärker es gefährdet wird.[328] Auch wenn die Ziele Schutz der nationalen Sicherheit und Verfolgung schwerer Straftaten legitim erscheinen, sind nach Auffassung des EGMR an die sogenannte strategische Überwachung bestimmte Anforderungen zu stellen, wenn die Maßnahmen verhältnismäßig sein sollen. Eine Beschränkung auf besonders schwere Straftaten sowie Vorkehrungen gegen Missbrauch erscheint geboten.[329] Es müssen ausreichende gesetzlich vorgesehene Schutzmaßnahmen gegen willkürliche Akte der Sicherheitsbehörden[330] bestehen, um zu vermeiden, dass mit dem Argument der Verteidigung der nationalen Sicherheit die Demokratie und die Freiheit der Bürger gefährdet werden.[331] Auf jeden Fall sind genügende Rechtsschutzmöglichkeiten, mindestens im Sinne von Art.13 EMRK besonders im grundrechtssensiblen Polizeibereich unerlässlich.[332] Die Schutzmechanismen müssen umso stärker ausgeprägt sein, je größer der Handlungsspielraum und das Ermessen der staatlichen Organe ausgelegt ist.[333] Dieser Gesichtspunkt erhält durch die seit 01.04.2012 vorgenommen Erstreckung der erweiterten Gefahrenforschung auf Einzelpersonen besonderes Gewicht. Kritiker der Regelung bemängeln deshalb insbesondere, dass die Rechtsschutzmaßnahmen mit der laufenden Ausdehnung der Befugnisse der Polizei insbesondere bei präventiven Ermittlungen nicht Schritt halten.[334]

Im Ergebnis bestehen Zweifel an der Bestimmtheit, d.h. ob die gesetzliche Grundlage in § 21 Abs. 3 SPG hinreichend klar ist, um den Betroffenen genügend Angaben da-

---

[328] Frenz, Europäischer Datenschutz und Terrorabwehr, EuZW 2009, S 6 ff. (7)
[329] EGMR Urteil vom 29.06.2006, Weber und Saravia gg. Deutschland, Ziffer 115, NJW 2007, S. 1433.
[330] EGMR Urteil vom 20.06,2002, Al-Nashif gg. Bulgarien, Ziffer 119, ÖJZ 2003, S.344; EGMR Urteil vom 16.02.2000, Amann gg. Schweiz, ÖJZ 2001, S. 71, , Ziffern 55 und 56.
[331] EGMR Urteil vom 04.05. 2000, Rotaru gg. Rumänien, ÖJZ 2001, S. 74 ff. (76), *„Der Gerichtshof muss außerdem überzeugt worden sein, dass es angemessene und wirksame Sicherungen gegen Missbrauch gibt, weil ein System der geheimen Überwachung, welches bestimmt ist, die nationale Sicherheit zu schützen, die Gefahr mit sich bringt, die Demokratie mit der Begründung ihrer Verteidigung zu untergraben oder gar zu zerstören"*.
[332] Schweizer/Müller, Zwecke, Möglichkeiten und Grenzen der Gesetzgebung im Polizeibereich, Leges 2008, S. 393; EGMR Urteil vom 04,05.2000, Rotaru gg. Rumänien, Ziffer 68 und 69 ÖJZ 2001, S. 74.
[333] Schweizer/Müller, Zwecke, Möglichkeiten und Grenzen der Gesetzgebung im Polizeibereich, Leges 2008, S.393.
[334] Ludwig Boltzmann Institut für Menschenrechte, Tag der Menschenrechte - Protest gegen das Sicherheitspolizeigesetz, http://bim.lbg.ac.at/de/print/2197, letzte Abfrage 21.04.2012.

rüber zu machen, in welchen Fällen und unter welchen Voraussetzungen die öffentliche Gewalt berechtigt ist, einen geheimen und potentiell gefährlichen Eingriff in das Privatleben vorzunehmen, wie dies vom EGMR gefordert wird.[335] Auch das Ermessen zur Ausübung einzelner Befugnisse erscheint anders als in der StPO nicht ausreichend eingegrenzt. Es erschließt sich einem Normalbürger nicht ohne weiteres, was unter „*Gewalt mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität*" zu verstehen ist. Der Gesetzgeber hat zwar in der Regierungsvorlage[336] zu § 21 Abs. 3 SPG auf die Regelung in § 149 d StPO (jetzt § 136 Abs.1 Ziffer 3 StPO) hingewiesen, in der von der „*Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder des Verbrechens der kriminellen Organisation oder der terroristischen Vereinigung (§§ 278 a und 278 b StGB)"* die Rede ist. Eine klare Beschränkung im Gesetzestext selbst wäre geeigneter und würde den Anforderungen des EGMR in Bezug auf die Bestimmtheit, Klarheit und Zugänglichkeit der Regelung besser entsprechen.

b.) Ist die Kontrolle der Sicherheitsbehörden bei der erweiterten Gefahrenforschung ausreichend?

Für die Kontrolle der Sicherheitsbehörden in den sensiblen Bereichen Observation, verdeckte Ermittlungen und erweiterte Gefahrenforschung ist im SPG die Bestellung eines Rechtsschutzbeauftragten mit zwei Stellvertretern vorgesehen, die ihre Aufgaben weisungsfrei und unabhängig wahrnehmen, § 91 a Abs. 1 SPG. Sie müssen über eine juristische Ausbildung § 91 b Abs.1 SPG verfügen und werden vom Bundespräsidenten auf Vorschlag der Bundesregierung nach Anhörung der Präsidenten des Nationalrates, des Verwaltungsgerichtshofes und des Verfassungsgerichtshofes für die Dauer von fünf Jahren bestellt, § 91 a Abs. 2 SPG. Im Interesse der Wahrung der Unabhängigkeit des Rechtsschutzbeauftragten ist eine Verfassungsbestimmung in das Gesetz aufgenommen worden. Eine Einschränkung der Befugnisse des Rechtsschutzbeauftragten und seiner Stellvertreter nach §§ 91 c und 91 d SPG und ihrer Rechte und Pflichten kann vom Nationalrat nur bei Anwesenheit von mindestens der Hälfte der Mitglieder mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen beschlossen werden, § 91a Abs. 3 SPG. Organisatorisch sind der Rechts-

---

[335] EGMR Urteil vom 26.03.1987, Leander gg. Schweden, Ziffer 51, EGMR-E 3, S. 430.
[336] Siehe bei Thanner /Vogl, Sicherheitspolizeigesetz, 4. Aufl. 2010, § 21 Anm. 2.

schutzbeauftragte und seine Stellvertreter in das Bundesinnenministerium eingebettet. Der Bundesinnenminister stellt ihnen die erforderlich sachlichen und personellen Mittel bereit und sorgt auch für eine angemessene Vergütung, § 91 b Abs. 3 SPG.
Für die Kontrollmöglichkeiten des Rechtsschutzbeauftragten sind abhängig von der Eingriffsintensität der Ermittlungstätigkeiten unterschiedliche Befugnisse vorgesehen. Bei Einsatz besonderer Ermittlungstechniken wie verdeckte Ermittlung (§ 54 Abs. 3 SPG), verdeckter Einsatz von Bild- und Tonaufzeichnungsgeräten (§ 54 Abs. 4 SPG) oder Verarbeitung von Daten, die andere mittels Einsatz von Bild- und Tonaufzeichnungsgeräten übermittelt haben, ist eine nachträgliche Unterrichtung vorgesehen, § 91 c Abs. 1 SPG. Vor Beginn einer Videoüberwachung im öffentlichen Raum ist eine Stellungnahme des Rechtsschutzbeauftragten einzuholen, § 91 c Abs. 2 SPG. Für Maßnahmen der erweiterten Gefahrenforschung ist vor Beginn von Ermittlungshandlungen die ausdrückliche Ermächtigung des Rechtsschutzbeauftragten erforderlich, die Voraussetzung für die Zulässigkeit ist, § 91 c Abs. 3 SPG.

Ungeachtet der verfassungsmäßig garantierten Unabhängigkeit des Rechtsschutzbeauftragten erscheint die organisatorische Einbindung in das Bundesinnenministerium nicht als Ideallösung. Ein Grad an Unabhängigkeit[337], wie sie der EuGH vergleichsweise auch für Datenschutzbehörden gefordert hat, ist nicht gegeben.

Der EGMR hält eine richterliche Kontrolle für wünschenswert, auch wenn Art. 13 EMRK dies nicht ausdrücklich verlangt.[338] In jedem Fall verlangt aber Art. 13 EMRK auf nationaler Ebene Maßnahmen, mit denen der Erhalt der Substanz der Konventionsrechte gewährleistet wird. Regelmäßig müssten Betroffene zumindest nachträg-

---

[337] EuGH Urteil vom 09.03.2010, Kommision gg. Deutschland, C 518/07, Ziffer 36. „*Hinzu kommt, dass bereits die bloße Gefahr einer politischen Einflussnahme der Aufsichtsbehörden auf die Entscheidungen der Kontrollstellen ausreicht, um deren unabhängige Wahrnehmung ihrer Aufgaben zu beeinträchtigen. Zum einen könnte es, wie die Kommission ausführt, einen „vorauseilenden Gehorsam“ der Kontrollstellen im Hinblick auf die Entscheidungspraxis der Aufsichtsstellen geben. Zum anderen erfordert die Rolle der Kontrollstellen als Hüter des Rechts auf Privatsphäre, dass ihre Entscheidungen, also sie selbst, über jeglichen Verdacht der Parteilichkeit erhaben sind*.“ http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62007CJ0518:DE:HTML, Abfrage 04.04.2012

[338] EGMR Urteil vom 04,05.2000, Rotaru gg. Rumänien, aaO. ÖJZ 2001, S. 74 ff. (77) “*Der Grundsatz der Vorherrschaft des Rechts impliziert ua, dass Eingriffe in die Rechte des einzelnen einer wirksamen Überwachung unterworfen werden sollen, welche normalerweise von der Gerichtsbarkeit ausgeführt werden sollte, zuminde4st als letzte Möglichkeit(at least in the last resort), da eine richterliche Kontrolle die besten Garantien für die Unabhängigkeit, die Unparteilichkeit und ein ordentliches Verfahren bietet”*; EGMR Urteil vom 06.09.1978 Klass gg. Deutschland, Ziffer 56, EuGRZ 1979, S. 278; NJW 1979, S. 1755.

lich über Eingriffe in ihre Privatsphäre unterrichtet werden, ausgenommen der Zweck der Maßnahmen würde damit unterlaufen werden.[339] Im letzteren Fällen sind die Auswirkungen von Überwachungsmaßnahmen auf ein unvermeidliches Minimum zu beschränken und sicherzustellen, dass sie in völliger Übereinstimmung mit dem Gesetz erfolgen. Nach Auffassung des EGMR enthält das System der Konvention einen gewissen Kompromiss zwischen den Erfordernissen, eine demokratische Gesellschaft zu verteidigen und individuelle Rechte zu schützen. Im Zusammenhang mit Art. 8 EMRK bedeutet dies, dass ein Ausgleich zwischen der Ausübung des durch Abs. 1 garantierten Rechts des Einzelnen und der Notwendigkeit von Maßnahmen- gemäß Abs. 2 angestrebt werden muss, um geheime Überwachungsmaßnahmen zum Schutze einer demokratischen Gesellschaft in ihrer Gesamtheit einzusetzen.[340] Unter Berücksichtigung dieser Erwägungen erscheint die Einrichtung des Rechtsschutzbeauftragten im SPG als vertretbare Lösung. Soweit erkennbar, ist aber eine nachträgliche Unterrichtung von Betroffenen, deren personenbezogene Daten im Rahmen der erweiterten Gefahrenforschung verwendet worden sind, auch in den Fällen nicht vorgesehen, in denen eine Information den Zweck der Maßnahmen nicht gefährden würde. Außerdem ist die Einschaltung des Rechtsschutzbeauftragten bei der erweiterten Gefahrenforschung lediglich bei Beginn der Maßnahmen vorgesehen, § 91 c Abs. 3 SPG, wenn nicht besondere Ermittlungsmaßnahmen wie Observation und verdeckte Ermittlungen eingesetzt werden sollen, § 91 c Abs. 1 SPG. Zwar ist der Rechtsschutzbeauftragte berechtigt, von sich aus weitergehende Kontrollen vorzunehmen, § 91 d SPG. Aber diese Maßnahmen sind nicht zwingend vorgeschrieben. Wenn, wie bei geheimen Ermittlungen üblich, Betroffene ihre Rechte nicht selbst wahrnehmen können, müssen Kontrollmechanismen eingerichtet werden, die in etwa den gleichen Schutz gegen Missbrauch bieten. Auch Vorschriften über die Dauer einzelner Überwachungsmaßnahmen fehlen. Insofern besteht also Nachbesserungsbedarf. Allerdings ist mit der SPG Novelle 2011[341] insofern eine Verbesserung eingetreten, als der Rechtsschutzbeauftragte anders als bisher nicht

---

[339] EGMR Urteil vom 06.09.1978, Klass gg. Deutschland, aaO. Ziffer 58.
[340] EGMR Urteil vom 06.09.1978, Klass gg. Deutschland, Ziffer 59, aaO.
[341] Beschluss des Nationalrates vom 28.04.2011, Änderung der Strafprozessordnung und des Sicherheitspolizeigesetzes.
http://www.parlament.gv.at/PAKT/VHG/XXIV/BNR/BNR_00361/fname_216278.pdf, letzte Abfrage 12.04.2012.

nur befugt, sondern auch verpflichtet ist, Beschwerde bei der DSK einzulegen, wenn Rechte der Betroffenen verletzt worden sind.

Der Rechtsschutzbeauftragte selbst hält die Einrichtung dieser Institution für europaweit einmalig. Sie habe sich als Garant des Rechtsschutzes bewährt. Das zur Verfügung stehende Instrumentarium sei ausreichend und bei verhältnisgemäßem Einsatz grundsätzlich EMRK-konform. Andere europäische, auch demokratische Rechtsstaaten, wie z.B. Deutschland und Frankreich, würden für die erweiterte Gefahrenforschung ohne richterliche Genehmigung nicht nur verdeckte Ermittlungen, sondern auch Telefonüberwachung vorsehen.[342]

c.) Entsprechen die Regelungen zur Löschung von personenbezogenen Daten den Anforderungen des EGMR?

Da die Verwendung von personenbezogenen Daten bei der Gefahrenforschung in der Regel ohne Kenntnis der Betroffenen erfolgt, diese also Rechtsmittel dagegen nicht ergreifen können, muss dafür Sorge getragen werden, dass die Sicherheitsbehörden von sich aus unverzüglich unrichtige Daten korrigieren und diese löschen, wenn sich herausstellt, dass von den betroffenen Personen keine Gefahr ausgeht. Dies ist umso wichtiger, weil die Daten in aller Regel nicht nur lokal bei den zuständigen Behörden gespeichert werden, sondern abhängig von unterschiedlichen Voraussetzungen in zentralen Evidenzen wie Sicherheitsmonitor, § 58 a SPG, zentrale Gewaltschutzdatei, § 58c SPG, zentrale Analysedatei über mit beträchtlicher Strafe bedrohte Gewaltdelikte, § 58 d SPG, sowie die Verwaltungs-strafevidenz für Übertretungen des SPG, § 60 SPG.

Für den Ermittlungs- und den Erkennungsdienst bestehen für die Berichtigung und Löschung von personenbezogenen Daten unterschiedliche Vorschriften. Für den Ermittlungsdienst regelt § 63 SPG (wie auch in § 6 Abs. Ziffer 4 und § 27 Abs.1 DSG 2000 vorgesehen), dass ermittlungsdienstliche Daten richtigzustellen oder zu löschen sind, wenn festgestellt wird, dass sie entgegen den Bestimmungen des SPG verarbeitet werden. Nach § 57 Abs. Ziffer 6 SPG reicht für eine Eintragung von personenbezogenen Daten in zentrale Informationssammlungen aus, dass gegen den Betrof-

---

[342] Matscher, Öffentliche Sicherheit 2008, S. 108 ff. (113)

fenen Ermittlungen im Dienste der Strafrechtspflege eingeleitet worden sind, eine Löschung nach § 58 Abs. 1 Ziffer 6 SPG aber nur dann erfolgen muss, wenn gegen den Betroffenen kein Tatverdacht mehr besteht, also nicht schon dann, wenn das Verfahren eingestellt und nicht mit einer Anklageerhebung und Verurteilung geendet hat. Der VfGH hat in diesem Zusammenhang entschieden, dass im Rahmen der erforderlichen Prüfung der Verhältnismäßigkeit, Art. 8 Abs. 2 EMRK, §§ 1 Abs. 2 DSG 2000 und 29 SPG eine Interessenabwägung vorzunehmen ist. Die Sicherheitsbehörde hat das Interesse des von der Speicherung und Übermittlung der Daten gemäß § 57 Abs. 1 Ziffer 6 SPG Betroffenen an einer Löschung der Daten mit dem öffentlichen Interesse an der Notwendigkeit der Speicherung und Übermittlung dieser Daten auch während des Zeitraumes gemäß § 58 Abs.1 Ziffer 6 lit. b SPG iVm. dem zweiten Satz dieses Absatzes aufgrund der Umstände des Einzelfalles abzuwägen.[343] Dies gilt ungeachtet der gesetzlich vorgesehenen Sperr- und Löschfristen in § 58 SPG. Diese Fristen sind nur als Obergrenzen für die Speicherung anzusehen.[344] Der EGMR ist in dieser Frage weiter gegangen, wenn er feststellt, dass Personen, die keiner Straftat für schuldig gesprochen worden sind und für die das Recht der Unschuldsvermutung gilt, in gewissem Umfange genauso behandelt werden wie verurteilte Personen, wenn ihre Daten weiterhin aufbewahrt werden. Nach Art. 6 Abs. 2 EMRK gilt jede Person bis zum Beweis ihrer Schuld als unschuldig. Es sei zu berücksichtigen, dass das in der Konvention verankerte Recht auf Beachtung der Unschuldsvermutung die allgemeine Regel beinhaltet, dass kein Zweifel hinsichtlich der Unschuld eines Angeklagten mehr geäußert werden darf, wenn dieser freigesprochen wurde.[345] Aus diesem Grunde hat er die Aufbewahrung von Fingerabdrücken Zellproben und DNA-Profilen verdächtiger, aber keiner Straftat schuldig gesprochener Personen als unverhältnismäßig im Sinne von Art. 8 Abs. 2 EMRK angesehen, weil für die Betroffenen darin ein Risiko der Stigmatisierung liege.[346]

---

343 VfGH vom 16. März 2001, Geschäftszahl G94/00, VfSlg. 16150/2001, http://www.ris.bka.gv.at/Dokumente/Vfgh/JFR_09989684_00G00094_01/JFR_09989684_00G00094_01.pdf , letzte Abfrage 16.01.2012

344 Flendrovsky in Bauer/Reimer (Hrsg.), Datenverwendung und Datenschutz in der allgemeinen Sicherheitspolizei, S. 363.

345 EGMR Urteil vom 21.03.2000, Asan Rushite gg. Österreich, Ziffer 31, ÖJZ 2001, S.155.

346 EMRK Urteil vom 04.12.2008, S. und Marper gg. Vereinigtes Königreich, EuGRZ 2009, S. 299 ff. (313).

Daraus kann man den Grundsatz ableiten, das personenbezogene Daten bei den Polizeibehörden ungeachtet der kasuistischen Bestimmungen im SPG zu löschen sind, wenn es nach Abschluss von Ermittlungen oder eines strafrechtlichen Verfahrens zu keiner Schuldfeststellung kommt. Das gilt nicht nur hinsichtlich der Vorschriften über die Löschung von Daten im polizeilichen Ermittlungsverfahren, sondern auch für die Regelungen zur Löschung im Erkennungsdienst, § 73 SPG.

8.6 Entsprechen die mit der Novelle 2007 eingeführten Bestimmungen der § 53 Abs. 3 a und 3 b SPG datenschutzrechtlichen Anforderungen?

§ 53 Abs.3 a

Nach dieser Vorschrift sind Telekommunikationsdienstleister und Internetprovider verpflichtet, den Sicherheitsbehörden Auskunft über Inhaber von Teilnehmeranschlüssen, IP-Adressen zu einer bestimmten Nachricht und Identität des Nutzers einer IP-Adresse zu einem bestimmten Zeitpunkt zu nennen. Voraussetzung ist das Vorliegen von Tatsachen, die die Annahme einer konkreten Gefahrensituation rechtfertigen und diese Daten von den Sicherheitsbehörden zur Erfüllung der Ihnen nach dem SPG übertragenen Aufgaben benötigt werden. Die Auskünfte sind unverzüglich und kostenlos zu erteilen. Daraus ist zu entnehmen, dass die angefragten Stellen nicht berechtigt sind, die Voraussetzungen für ein Auskunftsverlangen zu hinterfragen und zu prüfen.[347]

Mit dieser Vorschrift wird den Sicherheitsbehörden ein weiter Ermessensspielraum eingeräumt, nicht nur Daten über einer Straftat verdächtigte Personen abzufragen, sondern ebenso von unbeteiligten Kontaktpersonen, auch solchen, die der beruflichen Verschwiegenheitspflicht unterliegen. Auch das mögliche Gewicht der Rechtsgutverletzung oder die Schwere einer Straftat sind nicht relevant. Die Wahrscheinlichkeit einer konkreten Gefahrensituation sowie das Erfordernis für die Erfüllung einer polizeilichen Aufgabe sind ausreichend.[348]

Das ist insofern bemerkenswert, weil im strafprozessualen Ermittlungsverfahren derartige Auskünfte nur in Bezug auf Entführer oder Personen zulässig sind, die einer vorsätzlich begangenen Straftat verdächtigt werden, die mit mehr als sechs Monaten Freiheitsstrafe bedroht ist und der Anschlussinhaber zustimmt oder die vorsätzlich

[347] Hauer/Keplinger, Sicherheitspolizeigesetz, Komm, 4. Aufl. 2011, § 53 Abs. 3a Anm. 10.1 (S. 565).
[348] Hauer/Keplinger aaO. § 53, Anm. 10.5 (S. 568).

begangene Straftat mit mehr als einem Jahr Freiheitsstrafe bedroht ist, § 135 Abs. 2 StPO. Darüber hinaus sind ein entsprechender Antrag der Staatsanwaltschaft und eine richterliche Einwilligung erforderlich, § 137 Abs. 1 StPO.

Die Sicherheitsbehörden sind nach § 91 c Abs. 1 SPG lediglich verpflichtet, den Rechtsschutzbeauftragten in den Fällen des § 53 Abs. 3 a Ziffer 2 und 3 sowie der nachträglichen Rufdatenerfassung, § 53 Abs. 3 a zweiter Satz SPG, zu informieren, was auch nachträglich geschehen kann.

§ 53 Abs. 3 b SPG

Diese Bestimmung verpflichtet die Betreiber öffentlicher Kommunikationsdienste, den Sicherheitsbehörden bei Vorliegen einer Gefahr für das Leben oder die Gesundheit eines Menschen Auskunft über die Standortdaten und internationale Teilnehmerkennung der von dem gefährdeten Menschen mitgeführten Endeinrichtung zu geben sowie technische Mittel für die Lokalisierung zum Einsatz zu bringen. Dabei brauchen die Behörden sich nicht gegenüber den Betreibern zu rechtfertigen. Die Bestimmung regelt ausdrücklich, dass die Verantwortung für die Zulässigkeit des Auskunftsbegehrens bei den Sicherheitsbehörden liegt. Auch bei Anfragen nach § 53 Abs. 3 b SPG ist der Rechtsschutzbeauftragte zu informieren, § 91 c Abs. 1 SPG.

Es gehört zu den wesentlichen Aufgaben der Sicherheitspolizei, Gefährdungen für Leben oder Gesundheit von Menschen zu verhindern, § 19 Abs. 1 SPG. Die Polizei muss auch in die Lage versetzt werden, moderne technische Hilfsmittel für die Befreiung von Menschen aus einer Gefahrensituation einzusetzen. Nachdenklich stimmen jedoch die Begleitumstände des Zustandekommens der Vorschrift, die nicht auf dem üblichen Weg über parlamentarische Ausschussberatungen und Stellungnahmen anderer fachlich relevanter Institutionen entstanden ist, sondern durch einen Änderungsantrag der Regierungsfraktion im Nationalrat kurz vor der Abstimmung.[349]

---

[349] Peissl u. Andere, Privatsphäre 2.0, http://www.arbeiterkammer.at/bilder/d89/Studie_Datenschutz.pdf , letzte Abfrage 16.01.2012, S. 20 „*Bereits die Art der Beschlussfassung dieses Gesetzes löste in weiten Teilen der Bevölkerung Unmut aus: Es wurde am Ende einer 15 Stunden dauernden Sitzung des Nationalrates, der letzten im Jahr 2007, am späten Abend beschlossen, ohne, wie es sonst üblich gewesen wäre, vorher den zuständigen Innenausschuss des Parlaments damit zu befassen. Darüber hinaus wurden von den Parlamentsfraktionen der Regierungsparteien kurz vor der Abstimmung noch Änderungsanträge eingebracht, die die Befugnisse der Polizei gegenüber der Gesetzesvorlage stark ausweiteten.*“; zur Kritik siehe auch: http://www.heise.de/newsticker/meldung/Neues-oesterreichisches-Sicherheitspolizeigesetz-in-der-Kritik-171122.html, letzte Abfrage 16.01.2012

Ferner stimmt bedenklich, dass das Innenministerium offenbar schon vor Inkrafttreten der Regelung sog. IMSI-Catcher verwendet hat und wohl auch relativ teure (600 T€) Geräte einsetzt, mit denen nicht nur die Standorte von Endgeräten ermittelt, sondern auch Mobilfunkgespräche im Wege der Simulation einer Funkzelle abgehört werden können.[350] Da die Geräte im Übrigen alle in Wien stationiert sind, erscheint die behauptete Notwendigkeit des Einsatzes für die Rettung von Lawinenopfern und verirrten Bergwanderern als vorgeschobenes Argument.[351] Das Lokalisieren von mobilen Endgeräten, und nur dazu ist die Sicherheitspolizei berechtigt, ist einfacher, z. B. mit einer sog. „stillen SMS", möglich.

In der Literatur wird insbesondere der durch die Unbestimmtheit der Anfragevoraussetzungen bedingte weite Ermessensspielraum kritisiert: *„ Wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen"*. Wegen dieses weiten Ermessensspielraums wird auch eine richterliche Kontrolle der Anfragen gefordert.[352]

Nach der oben in Kap. 8.4 dargestellten Rechtsprechung des EGMR müssen gesetzliche Regelungen, mit denen in Grundrechte eingegriffen wird, hinreichend bestimmt und für die Betroffenen vorhersehbar sein, so dass sie ihr Verhalten danach ausrichten können. Die im Gesetz gewählte Formulierung legt nahe, dass bloße Vermutungen einer Gefährdungssituation ausreichen, so dass bereits Zweifel an der ausreichenden Bestimmtheit der Vorschrift bestehen. Selbst wenn man Voraussetzungen für die Verhältnismäßigkeit des Eingriffs wie legitimes Ziel und dringendes soziales Bedürfnis bejaht, bleibt die Frage, ob ausreichende Kontrollmechanismen bestehen, um Missbrauch seitens der Behörden zu verhindern.

Zwar ist der Rechtsschutzbeauftragte zu informieren. Das geschieht aber im Regelfall nachträglich, d.h. erst dann, wenn u.U. ein unzulässiger Grundrechtseingriff bereits stattgefunden hat. Wünschenswert wäre wie bei strafprozessualen Ermittlungen eine richterliche Bewilligung. Sinnvoller wäre aber in jedem Fall eine vorherige Ein-

---

[350] IMSI-Catcher: Das Phantom der Polizei, Der Standard vom 30. Jänner 2008, http://derstandard.at/3204440/IMSI-Catcher-Das-Phantom-der-Polizei, Abruf am 16.11.2011

[351] http://www.ueberwachungsstaat.at/index.php?id=56276, Abruf 16.11.2011.

[352] Stellungnahme der OCG zur Novellierung des Sicherheitspolizeigesetzes, OCG Journal 2/ 2008, S7/8 http://www.ots.at/presseaussendung/OTS_20080227_OTS0062/stellungnahme-der-ocg-zur-novellierung-des-sicherheitspolizeigesetzes, Abruf 16.11.2011.

schaltung des Rechtsschutzbeauftragten wie bei Maßnahmen der erweiterten Gefahrenforschung. In den ersten vier Monaten des Jahres 2008 sind von den Sicherheitsbehörden täglich durchschnittlich 32 Anfragen gestellt worden.[353] Dabei stellt sich die Frage, ob dem Rechtsschutzbeauftragten und seinem Vertreter angesichts dieser Zahlen neben ihren sonstigen Aufgaben eine angemessenen Prüfung möglich ist.

8.7 Zusammenfassung

8.7.1 Schlussfolgerungen

Insgesamt betrachtet erweisen sich die Regelungen über die anlasslose Verwendung personenbezogener Daten im Rahmen der erweiterten Gefahrenforschung, § 21 Abs. 3 SPG, d.h. ohne dass eine konkrete Gefährdungslage gegeben ist, unter Berücksichtigung der vom EMRK entwickelten Kriterien wegen der Verwendung von Begriffen mit unklarem Inhalt als zu unbestimmt und für Betroffene daher in ihren Konsequenzen nicht vorhersehbar. Die Bestimmungen über die Zulässigkeit der Speicherung von personenbezogenen Daten im Rahmen der Kriminalitätsanalyse werfen diese Probleme nicht auf, weil hier an bereits erfolgte gefährliche Angriffe angeknüpft wird mit dem Ziel, Erkenntnisse für die Vorbeugung zukünftiger zu gewinnen. Im Gegensatz zur erweiterten Gefahrenforschung nach § 21 Abs. 3 SPG sind bei der schlichten Gefahrenforschung im Rahmen der Vorbeugung von Angriffen, § 16 Abs. 4 und § 28a SPG, bereits Tatsachen gegeben, die Angriffe wahrscheinlich erscheinen lassen.

Die Kontrollinstanz, der Rechtschutzbeauftragte, ist nicht gesetzlich verpflichtet, die Maßnahmen in Abständen zu überwachen. Er darf zwar Auskünfte verlangen, muss es aber nicht, so dass die Kontrolle letztendlich nicht der vom EGMR gestellten Anforderung einer fortlaufenden und zeitnahen Überwachung entspricht.

In diesem Zusammenhang sei darauf hingewiesen, dass auch im strafprozessualen Ermittlungsverfahren die Institution des Rechtsschutzbeauftragten besteht. Für das strafprozessuale Ermittlungsverfahren erscheint die Funktion des Rechtsschutzbeauftragten weniger dringlich als im Aufgabenbereich der Sicherheitspolizei. Einmal überwacht der Staatsanwalt als Leiter des Vorverfahrens, § 101 Abs. 1 StPO, die Kriminalpolizei. Gegen ihren Willen können keine Maßnahmen durchgeführt werden.

---

[353] Der Standard vom 3.Juli 2008, http://derstandard.at/3391080/Handy--und-Internetueberwachung-Durchschnittlich-32-Anfragen-pro-Tag, letzte Abfrage 04.04.2012

Außerdem verfügt der Beschuldigte über Rechtsmittel und kann gegen die Verletzung seiner Rechte Einspruch beim Gericht einlegen, § 106 Abs. 1 Ziffer 1 StPO. Gegen die Entscheidung des Gerichts ist Beschwerde an das Oberlandesgericht möglich, § 106 Abs. 3 StPO.

Darüber hinaus könnte man in der Einrichtung des Rechtsschutzbeauftragten im strafprozessualen Ermittlungsverfahren eine Verletzung des Grundsatzes der Gewaltenteilung sehen, Art. 94 B-VG[354]. Der Rechtsschutzbeauftragte gemäß § 47 a StPO ist eine Einrichtung beim Bundesminister der Justiz. Er berichtet einmal im Jahr dem Bundesminister für Justiz über seine Tätigkeit und seine Wahrnehmungen im Rahmen seiner Aufgabenerfüllung (§§ 23 Abs. 1 a, 147, 195 Abs. 2 a StPO) im vorangegangenen Jahr. Allerdings ergibt eine nähere Prüfung der dem Rechtsschutzbeauftragten beim BMJ eingeräumten Befugnisse, dass seine Tätigkeit in erster Linie darauf ausgerichtet ist, die Staatsanwaltschaft und die Kriminalpolizei in Bezug auf die Wahrung der Rechte des Beschuldigten im Ermittlungsverfahren zu überwachen. Nach § 147 Abs. 1 StPO obliegt dem Rechtsschutzbeauftragten u.a. die Prüfung und Kontrolle der Anordnung, Genehmigung, Bewilligung und Durchführung von verdeckten Ermittlungen, der Observation von Personen, des automationsunterstützten Datenabgleichs und von Auskünften über Nachrichtenübermittlungen. Die Maßnahmen zielen mehr auf eine Stärkung der Position des Beschuldigten als auf eine Kontrolle der Justiz, so dass verfassungsrechtliche Bedenken insoweit nicht bestehen.

Die Löschung von Daten ist im SPG sehr detailliert geregelt, §§ 53 Abs. 6, 58, 73, 74 SPG, obwohl unter Berücksichtigung des höherrangigen Rechts der EMRK klar ist, dass in jedem Fall personenbezogene Daten unverzüglich zu löschen sind, wenn die Aufgabe, die ihre Verwendung erlaubt hat, erledigt worden ist und keine gesetzlich gerechtfertigten Gründe für ihre weitere Speicherung vorliegen, u.a. auch, wenn ein Strafverfahren ohne Schuldfeststellung geendet hat. Die in § 58 Abs. 1 SPG in einzelnen Fällen vorgesehene Sperrung für die Sicherheitsbehörden ersetzt eine an sich gebotene Löschung nicht, weil jederzeit eine Reaktivierung der Daten möglich ist.

---

[354] Artikel 94 B-VG: „*Die Justiz ist von der Verwaltung in allen Instanzen getrennt*.“.

8.7.2 Rechtswirkungen der Urteile des EGMR

Die Urteile wirken, wenn sie gemäß Art. 44 EMRK unanfechtbar und damit formell und materiell rechtskräftig geworden sind, in erster Linie zwischen den Parteien, entfalten jedoch generell eine Orientierungswirkung für die Mitgliedstaaten des Europarates.[355] In diesem Zusammenhang ist die Aussage des EGMR von Bedeutung, dass Art. 8 EMRK die Mitgliedsstaaten nicht nur verpflichtet, nicht zu rechtfertigende Eingriffe in die Privatsphäre zu unterlassen, sondern darüber hinaus auch zu positivem Handel zum Schutz des Grundrechts.[356] Das bedeutet, dass die nationalen Gesetzgeber in ihren Entscheidungen nicht völlig frei sind. Die Grundrechte in ihrer Interpretation durch den EGMR sind als Prinzipien zu verstehen, die dem Gesetzgeber inhaltliche Leitlinien vorgeben und ihn verpflichten, durch positives Tun für die ungehinderte Ausübung der Grundrechte zu sorgen.[357] Bezogen auf die hier untersuchten Bestimmungen des SPG bedeutet das für den österreichischen Gesetzgeber eine Verpflichtung zur Anpassung an den europäischen Grundrechtsstandard der EMRK.

8.8 Terrorismusbekämpfung in der EU

Der Datenaustausch im Rahmen der internationalen polizeilichen Zusammenarbeit ist Gegenstand des folgenden Kapitels. Im Hinblick darauf, dass die vorstehend betrachteten polizeilichen Maßnahmen schwerpunktmäßig der Abwehr des Terrorismus in Österreich dienen, sei jedoch darauf hingewiesen, dass die EU weitere Aktionen zur Bekämpfung des Terrorismus plant und dabei offensichtlich dem Schutz personenbezogener Daten einen höheren Stellenwert einräumen will als dies bei den bisherigen Regelungen (z.B. Richtlinie zur Vorratsdatenspeicherung) erkennbar war. Danach hat es sich die Kommission zur Aufgabe gemacht, bei allen Instrumenten, die zur Terrorismusbekämpfung eingesetzt werden, darauf zu achten, dass die Grundrechte gewahrt bleiben.[358] Der Europäische Datenschutzbeauftragte bemängelt in diesem Zusammenhang, dass in der Vergangenheit viele Maßnahmen im Inte-

---

[355] Grabenwerter, Europäische Menschenrechtskonvention, 4. Auflage 2009, S. 93,98.
[356] Europäischer Gerichtshof für Menschenrechte, Große Kammer, Beschwerdesache Guerra u.a. gegen Italien, Urteil vom 19.02.1998, Bsw. 14967/89, ÖJZ 1999, S.33, EuGRZ 1999, S. 188.
[357] Hinteregger, Der Schutz der Privatsphäre durch das österreichische Schadensersatzrecht de lege ferenda und de lege lata in Liber amoricum Pierre Widmer,Tort and Insurance Law, Band 10, 2003. S. 143 ff (146).
[358] Mitteilung der Kommission an das Parlament und den Rat, Politik der EU zur Terrorismusbekämpfung: wichtigste Errungenschaften und künftige Herausforderungen, S.12, http://ec.europa.eu/home-affairs/news/intro/docs/com_2010_386_de.pdf, letzte Abfrage: 16.01.2012

resse einer schnellen Reaktion auf terroristische Vorfälle ohne Prüfung der möglichen Überschneidungen mit bestehenden Instrumenten getroffen worden seien. Er begrüßt es daher, wenn dem Schutz der Grundrechte und dem Datenschutz mehr Aufmerksamkeit geschenkt wird und systematischem Vorgehen der Vorzug gegenüber Einzelmaßnahmen gegeben wird.[359]

[359] EDSB fordert systematischen und konsistenten Ansatz, um unnötige Beschränkungen der Privatsphäre zu vermeiden: http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/10/16&format=HTML&aged=0&language=DE&guiLanguage=en, letzte Abfrage am 16.01.2012.

9. Internationale polizeiliche Zusammenarbeit und Datenschutz

Mit der zunehmenden internationalen wirtschaftlichen Verflechtung ist auch eine entsprechende Entwicklung bei der internationalen Kriminalität einhergegangen. Drogen und Menschenhandel sowie internationaler Terrorismus sind die Stichworte. Kennzeichnend für die Gefahren des Terrorismus sind die Anschläge auf das New Yorker Trade Center im September 2001, die Londoner Underground sowie Züge in Spanien. Deshalb kann kein Zweifel an der Notwendigkeit einer verstärkten internationalen polizeilichen Zusammenarbeit bestehen, wenn man die internationale schwere Kriminalität wirksam bekämpfen will. In den folgenden Abschnitten wird die Entwicklung der internationalen polizeilichen Zusammenarbeit dargestellt und der Frage nachgegangen, ob mit dieser Entwicklung auch eine entsprechende Ausgestaltung der Rechte der Bürger verbunden worden ist und damit ein angemessenes Verhältnis zwischen den Sicherheitsbedürfnissen und den privaten Rechten der Bürger gewahrt bleibt.

Während Europol bis 2007 eine jährliche Steigerung terroristischer Angriffe beobachtete[360], ist die Zahl der Anschläge im Jahr 2008 um ein Viertel zurückgegangen[361]. Im Jahr 2009 wurde ein abermaliger Rückgang um rd. Ein Drittel gegenüber. 2008 und die Hälfte gegenüber 2007 berichtet[362]. Offensichtlich hat die verstärkte internationale Polizeiarbeit Früchte getragen.

9.1 Interpol

Interpol ist die größte internationale Polizeiorganisation. 190 Staaten sind Mitglieder.[363] Ihre Aufgabe ist die Verbesserung der grenzüberschreiten Kooperation der nationalen Polizeibehörden sowie die Unterstützung aller Organisationen, Behörden und Dienste bei der Vermeidung und Bekämpfung von internationalen Verbrechen.

---

[360] EU-Terrorism Situation and Trend Report 2008, Kap. 10 Trends, https://www.europol.europa.eu/sites/default/files/publications/tesat2008.pdf ,letzte Abfrage 16.01.2012.

[361] EU-Terrorism Situation and Trend Report 2009, Kap. 2 Executive Summary, https://www.europol.europa.eu/sites/default/files/publications/tesat2009_0.pdf , letzte Abfrage 16.01.2012.

[362] EU -Terrorism Situation and Trend Report 2010, Kap. 2 Executive Summary, https://www.europol.europa.eu/sites/default/files/publications/tesat2010_0.pdf , letzte Abfrage 16.01.2012.

[363] http://www.interpol.int/About-INTERPOL/Overview, letze Abfrage 21.04.2012.

Die Anfänge datieren bis in das 19. Jahrhundert. Infolge von Kriegsereignissen und des Ost/Westkonfliktes kam es mehrfach zu Änderungen der Struktur und auch zu Neugründungen. Die derzeitige Organisation und Aufgabenstellung basiert auf Abkommen aus dem Jahre 1956. 1971 wurde Interpol als zwischenstaatliche Organisation von der UN anerkannt. 1982 wurde im Rahmen einer Änderung der Statuten mit dem Aufbau interner Kontrolleinrichtungen für den Datenschutz begonnen.[364]
Die Aufgaben im Einzelnen ergeben sich aus dem Art. 3 der „Rules on the processing of information for the purposes of international police co-operation".[365] Im Wesentlichen sind es folgende:

- Personensuche zum Zwecke der Festnahme,
- Erhalt von Informationen über eine Person, die ein Verbrechen begangen hat oder im Begriff ist, eines zu begehen oder sich daran zu beteiligen,
- Polizeibehörden vor den kriminellen Aktivitäten einer Person zu warnen,
- eine vermisste Person ausfindig zu machen,
- einen Zeugen oder ein Opfer ausfindig zu machen,
- eine Person oder eine Leiche zu identifizieren,
- Objekte ausfindig zu machen oder zu identifizieren.

Zur Erfüllung dieser Aufgaben betreibt Interpol ein umfangreiches Informationssystem mit verschiedene Datenbanken[366], u. a. zu

- verdächtigen Terroristen,
- Daten über Kriminelle (Namen, Fotos),
- Fingerabdrücke,
- DNA-Profilen,
- verlorenen oder gestohlene Reisedokumenten,
- Kindesmissbrauch,
- gestohlenen Kunstgegenständen,
- gestohlenen Kraftfahrzeugen.

Zugang zu den Daten haben nationale Behörden. Auf der Grundlage der erwähnten „Rules on processing of information" können sie Informationen oder auch direkten

---

[364] http://www.interpol.int/About-INTERPOL/History, letzte Abfrage 21.04.2012.
[365] http://www.interpol.int/About-INTERPOL/Legal-materials , letzte Abfrage 17.01.2012.
[366] http://www.interpol.int/Public/ICPO/corefunctions/databases.asp, letzte Abfrage 17.01.2012.

Zugang zu den Datenbanken von Interpol erhalten. Zum Datenschutz findet sich die Aussage, dass die Basis für die rechtlichen Garantien die Verfassung der Organisation darstelle. Diese stelle sicher, dass die Tätigkeit der Organisation sich im Rahmen der Gesetze in den verschiedenen Mitgliedsländern und im Geist der Allgemeinen Erklärung der Menschenrechte bewegt. Interpol habe internationale Datenschutz-Prinzipien adaptiert, die aus dem Grundrecht des gesetzlichen Schutzes gegen willkürliche Eingriffe in die Privatsphäre abgeleitet seien.[367]

Die Einhaltung der Regeln soll durch eine unabhängige Kommission gewährleistet werden, die aus fünf Mitgliedern besteht, die direkt von der Generalversammlung für eine Amtszeit von drei Jahren gewählt werden.[368] Die Kommission bearbeitet auch Auskunftsersuchen betroffener Bürger[369] und erstellt jährlich einen Rechenschaftsbericht[370].

Der völkerrechtliche Status der Interpol macht es erforderlich, die in der Verfassung von Interpol für die Nationalstaaten enthaltenen Verpflichtungen in nationales Recht umzusetzen. Rechtsgrundlage für die Zusammenarbeit nationaler Behörden mit Interpol ist daher das jeweilige nationale Recht.[371] In Österreich kommt dafür das Polizeikooperationsgesetz[372] infrage. Dieses Gesetz regelt die Leistung und Inanspruchnahme von Amtshilfe im Verhältnis zu anderen Staaten und internationalen Sicherheitsorganisationen, u.a. auch Interpol. Zum Zwecke der Leistung von Amtshilfe darf in Menschenrechte nur eingegriffen werden, soweit dies auch österreichischen Sicherheitsbehörden in einem vergleichbaren Fall gestattet wäre, § 5 Abs. 2 PolKG. Im Wege der Amtshilfe dürfen personenbezogene Daten nicht übermittelt werden, wenn der ersuchende Staat oder die internationale Sicherheitsorganisation keinen ausreichenden Schutz im Sinne von Art 8 EMRK und § 1 DSG 2000 gewährleisten können, § 8 Abs. 2 Ziffer 3 PolKG. In Bezug auf Interpol findet das EU-Polizeikooperationsgesetz, EU-PolKG, keine Anwendung.[373] Nach dessen § 1 Abs. 1

---

[367] http://www.interpol.int/About-INTERPOL/Legal-materials , letzte Abfrage 21.04.2012.
[368] Art. 2 Buchst. b und 3 Buchst. a der RULES ON THE CONTROL OF INFORMATION AND ACCESS TO INTERPOL'S FILES, http://www.interpol.int/public/icpo/legalmaterials/constitution/control/rulescontrolinformation.pdf , letzte Abfrage 06.02.2011.
[369] Art.4 der genannten Regeln
[370] Art. 6 Buchst. d der genannten Regeln
[371] Férérvàry, „Europäisierung der Polizeiarbeit“ in Férérvàry/Stangl, Polizei zwischen Europa und den Regionen: Analyse disparater Entwicklungen, 2001, S. 42 f..
[372] Polizeikooperationsgesetz, BGBl. I Nr.104/1997.
[373] EU-Polizeikooperationsgesetz, EU-PolKG, BGBl. I Nr. 132/2009.

beschränkt sich der Anwendungsbereich dieses Gesetzes auf die Zusammenarbeit zwischen den nationalen Sicherheitsbehörden und Sicherheitsbehörden der anderen Mitgliedstaaten der Europäischen Union sowie dem Europäischen Polizeiamt (Europol).

Bei Interpol existiert kein spezifisches Regelwerk für den Datenschutz. Zwar gibt es eine Kontrollkommission. Diese prüft jedoch schwerpunktmäßig die Einhaltung der internen Regeln und nicht nach spezifischen Standards für den Schutz personenbezogener Daten wie z.b. in der EU auf der Grundlage der Datenschutzrichtlinie 95/46/EG. Bei Fehlverhalten anderer Mitgliedstaaten von Interpol bestehen nur eingeschränkte Sanktionsmöglichkeiten. Diese Staaten können vorübergehend oder endgültig von der Kooperation ausgeschlossen werden. Ein darüber hinausgehender Rechtsschutz gegen falsche Angaben oder Missbräuche einzelner Mitgliedstaaten oder auch gegen Maßnahmen der Generaldirektion besteht nicht.[374] Außerdem wird die Meinung vertreten, dass Interpol nicht den Status einer internationalen Organisation erlangt habe. Ihre Einrichtungsakte seien nicht offiziell kundgemacht. Wegen der fehlenden außenwirksamen Rechtsgrundlage sei der Datenaustausch unter Berücksichtigung von § 1 Abs. 2 DSG 2000 und Art. 48 f B-VG kritisch zu betrachten. Die Weitergabe von Daten aus Österreich und der gesamte Datenaustausch mit Interpol erscheine deshalb unter Berücksichtigung von § 1 Abs. 2 DSG 2000 und Art 48 f B-VG bedenklich.[375]

9.2 Instrumente des Datenaustausches in der Europäischen Union

In der Europäischen Union existieren eine Vielzahl von Informationsplattformen und mehrere Einrichtungen, die für die Speicherung und den Austausch von Informationen auf dem Gebiet der innereuropäischen polizeilichen Zusammenarbeit zuständig sind. Das Entstehen dieser Plattformen und Einrichtungen ist auf immer neue Anforderungen im Zuge der Bekämpfung des Terrorismus und der internationalen Kriminalität und den Wegfall der Grenzkontrollen zwischen vielen europäischen Staaten zurückzuführen. Im Einzelnen handelt es sich um das Schengener Informationssystem

---

[374] Férérvàry, „Europäisierung der Polizeiarbeit“ in Férérvàry/Stangl, Polizei zwischen Europa und den Regionen: Analyse disparater Entwicklungen, 2001, S. 42 f. Fußnote 7.

[375] Flendrovsky, „Datenverwendung und Datenschutz bei der Sicherheitspolizei“ in Bauer/Reimer (Hrsg.) Handbuch Datenschutzrecht 2009, S. 345 ff. (372).

(SIS)[376], EURODAC, geschaffen durch die EURODAC-Verordnung[377] im Interesse der Unterstützung bei der Bearbeitung von Asylanträgen, das Visa-Informationssystem (VIS)[378], das Advance Passenger Informationssystem (API)[379], das Zollinformationssystem (ZIS)[380], das Aktennachweissystem für Zollzwecke (FIDE)[381], der Beschluss von Prüm[382] aus dem Jahre 2008, mit dem eine 2005 zwischen mehreren EU-Ländern getroffene Vereinbarung in ein EU-Instrument überführt wurde und das dem grenzüberschreitenden Austausch von DNA-Profilen, Fingerabdrücken, Daten aus Fahrzeugregistern und Daten über Personen unter Terrorverdacht dient. Ferner sind die Richtlinie über Vorratsdatenspeicherung[383]zu nennen, das Europäische Strafregisterinformationssystem (ECRIS)[384] und die von Europol verwaltete Europäische Cyberplattform (ECCP)[385]. Sechs der Systeme weisen eine Speicherung der Daten auf EU-Ebene auf (SIS, VIS, EURODAC, ZIS, Europol, und Eurojust). Alle anderen Instrumente regeln den grenzüberschreiten Austausch von personenbezogenen Daten innerhalb der EU oder an Drittländer. Neben den zentral oder dezentral eingerichteten Online-Anwendungen bestehen verschiedene Regelungen über organisierten Informationsaustausch. Dazu zählt einmal die so genannte schwedische Initiative zum Austausch von Informationen zur Durchführung strafrechtlicher Ermittlungen oder Gewinnung polizeilicher Erkenntnisse[386], ferner ein Instrument zum Austausch von Informationen zwischen zentralen Meldestellen zur

---

[376] SCHENGEN-BESITZSTAND gemäß Artikel 1 Absatz 2 des Beschlusses 1999/435/EG des Rates vom 20. Mai 1999 , ABl. L 239 vom 22.09.2000

[377] Verordnung(EG) Nr. 2725/2000 DES RATES vom 11. Dezember 2000, ABl. 316 vom 15.12.2000.

[378] Entscheidung 2004/512/EG des Rates, L 213 vom 15.06.2004; Verordnung EG/76/08, ABl. L218 vom 13.08.2008.

[379] Richtlinie 2004/82/EG des Rates, ABl. L 261 vom 06.08.2004, S. 24.

[380] Übereinkommen aufgrund von Artikel K.3 des Vertrags über die Europäische Union über den Einsatz der Informationstechnologie im Zollbereich, ABl. C 316 vom 27.11.1995, S. 34, geändert durch den Beschluss 2009/917/JI des Rates, ABl. L 323 vom 10.12.2009, S. 20.

[381] Verordnung EG/766/2008, ABl. C 139 vom 13.06. 2003.

[382] Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, ABl. L 210 vom 06.08.2008.

[383] Richtlinie 2006/24/EG, ABl. L 105 vom 13.04.2006.

[384] Legislative Entschließung des Europäischen Parlaments vom 9. Oktober 2008 zu dem Vorschlag für einen Beschluss des Rates zur Einrichtung des Europäischen Strafregisterinformationssystems (ECRIS) gemäß Artikel 11 des Rahmenbeschlusses 2008/XX/JI (KOM(2008)0332 — C6-0216/2008 — 2008/0101(CNS)), ABl. C 9 E/ 70 vom 15.01.2010.

[385] Art. 5 Abs. 2 des Beschlusses des Rates vom 09.04.2009 zur Errichtung des Europäischen Polizeiamtes (Europol), Beschluss 2009/371/JI, ABl. L 121 vom 15.05.2009.

[386] Rahmenbeschluss 2006/960/JI des Rates, ABl. L 386 vom 29.12.2008, S. 89

Entgegennahme von Finanzinformationen, Financial Intelligence Units (FIU)[387], und ein Instrument zur Zusammenarbeit zwischen Vermögensabschöpfungsstellen (Asset Recovery Offices (ARO)).

9.2.1 Das Europäische Polizeiamt (Europol)

9.2.1.1 Entwicklung von Europol

Offene Grenzen der Schengen-Staaten, Ausbreitung der organisierten Kriminalität sowie Gefährdungen durch Terrorismus haben Anfang der 1990er Jahre zu einer verstärkten polizeilichen Zusammenarbeit in der EU geführt, die u.a. in die Errichtung eines Europäischen Polizeiamtes mündete. Ausgangspunkt dafür war der Gipfel von Maastricht 1991, auf dem man sich über entsprechende Verhandlungen verständigte, die aber erst 1995 zum Abschluss eines Vertrages, dem Europolübereinkommen, führten.[388] Europol war ursprünglich keine EU-Agentur, sondern eine internationale Organisation auf der Grundlage eines völkerrechtlichen Vertrages zwischen den beteiligten Mitgliedstaaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit, (dritte Säule). Die Ratifizierung des Vertrages durch alle beteiligten Mitgliedstaaten dauerte einige Jahre, so dass das Amt erst 1999 seine Tätigkeit aufnehmen konnte. Die Umwandlung in eine EU-Agentur erfolgte mit dem 01. Jänner 2010 auf der Grundlage eines entsprechenden Ratsbeschlusses vom 06.04.2009 (Europolstatut)[389] gemäß Art. 64 Abs. 2 dieses Beschlusses.

9.2.1.2 Aufgaben von Europol

Ziel von Europol ist es, die Tätigkeit der zuständigen Behörden der Mitgliedstaaten sowie deren Zusammenarbeit bei der Prävention und Bekämpfung von organisierter Kriminalität, Terrorismus und anderen Formen schwerer Kriminalität zu unterstützen und zu verstärken, wenn zwei oder mehr Mitgliedstaaten betroffen sind, Art. 3 Abs. 1 Europolstatut. Europol war nach Art. 2 Abs. 2 Europol-Übk. 1995 zunächst nur für Drogenhandel, Nuklearschmuggel, Schleuserkriminalität, Menschenhandel und Kfz-Kriminalität zuständig, jedoch konnte aufgrund des letzten Satzes der genannten Be-

---

[387] Beschluss 2000/642/JI des Rates, ABl. L 271 vom 24.10.2000, S. 4

[388] Übereinkommen aufgrund von Artikel K.3 des Vertrags über die Europäische Union über die Errichtung eines Europäischen Polizeiamts (Europol-Übereinkommen), ABl. C 316 vom 27.11.1995 S. 02 - 32

[389] Beschluss des Rates vom 6. April 2009 zur Errichtung eines Europäischen Polizeiamts (Europol), ABl. L 121 vom 15.05.2009 S. 37 ff.

stimmung der Aufgabenbereich auf weitere im Anhang zum Übereinkommen aufgeführte Bereiche erweitert werden. Die Kriminalitätsbereiche, für die Europol aktuell gemäß Art. 4 Abs. 1 des Europolstatuts zuständig ist, sind im Anhang zu dem genannten Beschluss wiedergegeben.

Europol wird nicht selbst unmittelbar operativ bei der Verbrechensbekämpfung tätig, sondern leistet seine Unterstützung dadurch, dass es Informationen und Erkenntnisse sammelt, speichert, verarbeitet, analysiert und austauscht, Art. 5 Abs. 1 Buchst. a Europolstatut. Europolpersonal kann jedoch nach Maßgabe des Art. 6 Europolstatut in gemeinsamen Ermittlungsgruppen tätig werden, darf jedoch nicht bei der Durchführung von Zwangsmaßnahmen mitwirken. Jedes Mitgliedsland benennt oder errichtet eine nationale Verbindungsstelle, Art. 8 Abs. 1 Europolstatut, über die die Kontakte zu Europol laufen. Außerdem entsenden die Mitgliedstaaten Verbindungsbeamte, Art. 9 Abs. 1 Europolstatut. Im Rahmen seiner Unterstützungsfunktion betreibt Europol ein Informationssystem (EIS), Art. 11 Abs. 1 Europolstatut. In diesem Informationssystem können nach Art. 12 Abs. 1 Europolstatut Daten über Personen gespeichert werden, die nach innerstaatlichem Recht unter Verdacht stehen, Straftaten, für die Europol zuständig ist, begangen zu haben oder die wegen solcher Straftaten verurteilt worden sind bzw. bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie derartige Straftaten begehen könnten. Es können also auch Daten von Personen gespeichert werden, bei denen Tatsachen auf die Möglichkeit der Begehung einer Straftat hindeuten, ohne dass bereits ein konkreter Verdacht oder gar eine unmittelbare Gefahr für die öffentliche Sicherheit und Ordnung oder die Gesundheit oder das Leben anderer vorliegen. Es bestehen insoweit Zweifel an der erforderlichen Bestimmtheit der Regelung.[390] Im Einzelnen können nach Art. 12 Abs. 2 Europolstatut folgende Daten zu dem beschriebenen Personenkreis gespeichert werden:

a) Name, Geburtsname, Vornamen, gegebenenfalls Aliasnamen;

b) Geburtsdatum und Geburtsort;

c) Staatsangehörigkeit;

d) Geschlecht;

e) Wohnort, Beruf und Aufenthaltsort der betreffenden Person;

---

[390] Martino, Datenschutz im europäischen Recht, 1. Aufl. 2005, S. 83.

f) Sozialversicherungsnummern, Fahrerlaubnisse, Ausweispapiere und Passdaten und

g) soweit erforderlich, andere zur Identitätsfeststellung geeignete Merkmale, insbesondere objektive und unveränderliche körperliche Merkmale wie daktyloskopische Daten und (dem nicht codierenden Teil der DNA entnommene) DNA-Profile.

Zusätzlich dürfen nach Art. 12 Abs. 3 Europolstatut weitere Daten verarbeitet werden:

a) Straftaten, Tatvorwürfe sowie (mutmaßliche) Tatzeiten, Tatorte und Vorgehensweisen;

b) Tatmittel, die verwendet wurden oder verwendet werden könnten, einschließlich Informationen zu juristischen Personen;

c) die aktenführenden Dienststellen und deren Aktenzeichen;

d) Verdacht der Zugehörigkeit zu einer kriminellen Organisation;

e) Verurteilungen, soweit sie Straftaten betreffen, für die Europol zuständig ist;

f) Eingabestelle.

Neben dem EIS werden weitere so genannte Arbeitsdateien zu Analysezwecken geführt, in denen Daten über folgende Personengruppen gespeichert werden können, Art. 14 Abs. 1 Europolstatut:

a) Personen gemäß Artikel 12 Absatz 1,;b) Personen, die bei Ermittlungen in Verbindung mit den betreffenden Straftaten oder bei anschließenden Strafverfahren als Zeugen in Betracht kommen;

c) Personen, die Opfer einer der betreffenden Straftaten waren oder bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie Opfer einer solchen Straftat sein könnten;

d) Kontakt- und Begleitpersonen und

e) Personen, die Informationen über die betreffende Straftat liefern können.

Zu den jeweiligen Analyseprojekten werden Analyseteams gebildet, bestehend aus Mitarbeitern von Europol und Verbindungsleuten oder Experten der Mitgliedstaaten, von denen die Daten stammen oder die von den Untersuchungen betroffen sind. Nur dieser Kreis hat Zugang zu den Daten der jeweiligen Analysedatei, Art. 14 Abs. 2 Europolstatut. Es ist jedoch ein Indexsystem eingerichtet worden, mit dem die Eintragungen verschlagwortet werden. Damit ist Mitarbeitern von Europol, den zuständigen nationalen Stellen und den Verbindungsbeamten die Feststellung möglich, ob zu

einem bestimmten Thema Daten in den Analysesystemen verfügbar sind, ohne dass aber ein unmittelbarer Zugang zu den Dateninhalten eröffnet wird, Art. 15 Abs. 3 Europolstatut.

9.2.1.3 Verantwortung für den Datenschutz

Im Rahmen des Datenschutzes ist der jeweilige Mitgliedstaat für die Rechtmäßigkeit der Erhebung, der Übermittlung an Europol und der Eingabe sowie die Richtigkeit und Aktualität und die Beachtung der Speicherfristen im Rahmen der nationalen Vorschriften verantwortlich, Art. 29 Abs. 1 Buchst. a, Art 8 Abs. 4 Buchst. g Europolstatut. Im Falle von Österreich ist die nationale Verbindungsstelle ausschließlich für den Kontakt mit Europol zuständig und zum Zugriff auf die Europol Informationssysteme berechtigt, § 6 Abs. 1 EU-PolKG. Nationale Kontaktstelle im Sinne von Art. 8 Europolstatut ist der Bundesminister des Inneren (BMI), § 4 Abs. 1 PolKG. Innerhalb des Ministeriums ist das Bundeskriminalamt (BKA) für diese Aufgabe zuständig, für die ein eigenes Referat, Büro II/BK/2.2 (Nationale Stelle Europol/Verbindungsbeamtenbüro) besteht.[391]

Jedermann hat das Recht, sich an die die nationale Verbindungsstelle zu wenden und Auskunft darüber zu verlangen, ob bei Europol ihn betreffende Daten verarbeitet werden, § 16 Abs. 1 EU-PolKG. Die Auskunft kann nach § 16 Abs. 2 EU-PolKG verweigert werden, wenn höherrangige Interessen Österreichs berührt oder die Erfüllung der Aufgaben von Europol und die Ermittlungen in einer Strafsache oder schutzwürdige Interessen Dritter gefährdet werden würden.

Hinsichtlich der Daten, die von Privatpersonen, kooperierenden Organisationen oder Drittstaaten übermittelt werden und die Ergebnis der Analysetätigkeit sind, ist Europol für den Datenschutz verantwortlich, Art. 29 Abs. 1 Buchst. b Europolstatut. Dabei sind einmal die Bestimmungen des Europolstatutes selbst sowie als Datenschutzstandard die Bestimmungen des Übereinkommens des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbe-

---

[391] Öffentliche Sicherheit 2010, Seite 8, http://www.bmi.gv.at/cms/BMI_OeffentlicheSicherheit/2010/01_02/files/Europol.pdf, letzte Abfrage 16.01.2012;
Innerhalb seines Zuständigkeitsbereiches ist das Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung nationale Kontaktstelle gegenüber Interpol, Europol, OLAF sowie anderen vergleichbaren internationalen Einrichtungen, § 4 Abs. 2 Bundesgesetz über die Einrichtung und Organisation des Bundesamts zur Korruptionsprävention und Korruptionsbekämpfung, BGBl. I Nr. 72/2009.

zogener Daten und die Empfehlung R (87) 15 des Ministerkomitees des Europarates vom 17. September 1987[392] zu beachten, Art. 27 Europolstatut.

Zur Überwachung der nationalen Verbindungsstellen in Bezug auf die Einhaltung nationaler Rechtsvorschriften, insbesondere in Bezug auf den Datenschutz, sowie der Bedingungen des Europolstatutes werden nationale Kontrollinstanzen benannt, Art. 33 Abs. 1 Europolstatut. In Österreich ist das die Datenschutzkommission, § 14 EU-PolKG.

Gemäß Art. 28 Abs. 1 Europolstatut wird auf Vorschlag des Direktors von Europol vom Verwaltungsrat ein in der Erfüllung seiner Pflichten unabhängiger Datenschutzbeauftragter bestellt. Seine Aufgabe ist es im Wesentlichen, dafür zu sorgen, dass personenbezogene Daten rechtmäßig und unter Einhaltung des Europolstatutes verarbeitet werden.

Darüber hinaus ist eine gemeinsame Kontrollinstanz eingesetzt worden, deren Aufgabe darin besteht, die Aktivitäten von Europol daraufhin zu überprüfen, ob durch die Speicherung, Verarbeitung und Verwendung der bei Europol vorhandenen Daten die Rechte des Einzelnen verletzt werden. Sie setzt sich aus Mitgliedern der nationalen Kontrollinstanzen zusammen (höchstens zwei je Land), Art. 34 Abs. 1 Europolstatut.

9.2.1.4 Datenschutz und Rechtsschutz

Es stellt sich die Frage, ob die genannten Regelungen ausreichen, um einen angemessenen Schutz österreichischer Bürger gegen mögliche Verletzungen des Datenschutzes eigener Behörden und durch Organe von Europol zu gewährleisten.

9.2.1.4.1 Datenschutz in Österreich in der Zusammenarbeit mit Europol

Hinsichtlich der Daten, die von österreichischen Behörden eingegeben oder übermittelt worden sind, obliegt Österreich die Verantwortung für die Rechtmäßigkeit der

---

[392] Übereinkommen zum Schutz des der Menschen bei der Verarbeitung personenbezogener Daten, Übereinkommen 108 des Europates vom 28.01.1981, http://conventions.coe.int/treaty/ger/treaties/html/108.htm, letzte Abfrage16.01.2012; Council of Europe Committee of Ministers Recommendation No. R (87) 15 vom 17.09.1987, http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1987_15.pdf, letzte Abfrage 16.01.2012.

Erhebung, der Übermittlung, der Eingabe sowie für die Aktualität der Daten und die Prüfung der Speicherfristen, Art. 29 Abs. 1 Buchst. a Europolstatut.

Die für die Zusammenarbeit Österreichs mit Europol maßgeblichen nationalen Vorschriften finden sich im Polizeikooperationsgesetz (PolKG) und EU-Polizeikooperationsgesetz (EU-PolKG). Dem BMI/BKA obliegt der alleinige Zugriff auf die Europol Informationssysteme und der Kontakt zu Europol, § 6 Abs. 1 EU-PolKG, und diese Behörde hat die Rechtmäßigkeit des Datenaustausches mit Europol zu gewährleisten, § 6 Abs. 2 Ziffer 7 EU-PolKG. Nach § 9 Abs. 1 und 2 EU-PolKG darf die Nationale Europolstelle die in Art. 12 Europolstatut aufgeführten personenbezogenen Daten und andere Daten an Europol melden oder eingeben, soweit es sich um Daten zu Personen handelt, die wegen einer Straftat, welche in den Zuständigkeitsbereich von Europol fällt, verurteilt worden sind oder verdächtigt werden bzw. aufgrund von bestimmten Tatsachen anzunehmen ist, dass sie derartige Straftaten begehen werden. Das BMI/BKA darf Europol auch Daten zur Erstellung sogenannter Analysedateien (Art. 14 Europolstatut) übermitteln, soweit die Sicherheitsbehörden nach § 53 a SPG derartige Informationen selbst zur Erstellung von Analysen verarbeiten dürfen, § 10 Abs. 1 EU-PolKG. § 53 a Abs. 2 SPG erlaubt u.a. zur Vorbeugung gegen gefährliche Angriffe die Verwendung personenbezogener Daten von Verdächtigen, aber auch Opfern, Zeugen, Kontaktpersonen und Informanten sowie auch fallbezogene besonders schutzwürdige Daten im Sinne von § 4 Abs. 2 DSG 2000 für operative und strategische Analysen zu verarbeiten. Nach § 91 c Abs. 2 SPG ist der BMI an sich gehalten, unverzüglich den Rechtschutzbeauftragten zu verständigen, wenn die Sicherheitspolizei u.a. eine Datenanwendung nach § 53 a Abs. 2 SPG plant. In § 8 Abs. 1 EU-PolKG wird lediglich auf § 53 a Abs. 2 SPG Bezug genommen, nicht auf § 91 c Abs. 2 SPG, so dass nicht ganz klar erscheint, ob auch in diesen Fällen eine Einschaltung des Rechtsschutzbeauftragten stattfindet. Von der Sache her macht es keinen Unterschied, ob derartige Analysen im Informationsverbund innerhalb Österreichs oder durch Europol erstellt werden.

Für die Kontrolle der Datenverwendungen und -übermittlungen der nationalen Europolstelle ist die Datenschutzkommission (DSK) als nationale Kontrollinstanz zuständig, Art. 33 Europolstatut und § 14 EU-PolKG. Der DSK obliegt die Kontrolle der Zulässigkeit der Eingabe in die Europoldatenbanken und des Abrufs aus diesen Systemen sowie die Kontrolle jedweder Übermittlung personenbezogener Daten an Euro-

pol durch österreichische Behörden und deren Organe, § 14 EU-PolKG. Die DSK hat die in §§ 30, 31 DSG 2000 festgelegten Befugnisse. Ähnlich wie bei der Gemeinsamen Kontrollinstanz (siehe dazu unten 7.2.1.4.2) ist davon auszugehen, dass dies keine fortlaufenden begleitenden Kontrollen sind, sondern anlassbezogene Prüfungen oder Stichprobenkontrollen. Festzuhalten ist an dieser Stelle, dass auf dem Wege über §§ 10 Abs. 1 EU-PolKG und 53 a Abs. 2 SPG auch Daten von nicht verdächtigen Personen wie Opfern, Zeugen, Kontaktpersonen und Informanten in Analysedateien bei Europol gespeichert werden können und dass die Rechtmäßigkeit dieser Datenverwendungen im Wesentlichen vom ordnungsgemäßen Verhalten der Beteiligten abhängt.

Zu ergänzen ist noch, dass den Bürgern hinsichtlich der sie betreffenden bei Europol verarbeiteten personenbezogenen Daten Auskunfts- (stark eingeschränkt) Löschungs- und Beschwerderechte zustehen, § 16 bis 19 EU-PolKG. Diese Rechte laufen im Regelfall ins Leere, weil die Betroffenen keine Kenntnis von den genannten Datenverwendungen erhalten. Die Zahl der Auskunftsersuchen hat zwar im Laufe der Jahre zugenommen, belief sich jedoch im Jahre 2008 laut dem Bericht der GKI von 2009 lediglich auf 135 Anfragen[393]. Eine nachträgliche Information, sobald der Verarbeitungszweck erfüllt und nicht mehr gefährdet werden kann, ist nicht vorgesehen.

Die datenschutzrechtliche Würdigung des beschriebenen Zustandes erfolgt im Anschluss an die folgende Darstellung des Datenschutzes bei Europol selbst.

9.2.1.4.2 Datenschutz bei Europol

Wie bereits oben erwähnt wurde, ist Europol gehalten, einen Datenschutzstandard zu gewährleisten, der den Grundsätzen des Übereinkommens des Europarates vom 28. Januar 1981 zum Schutze der Menschen bei der automatischen Verarbeitung personenbezogener Daten (EuDSK) und der Empfehlung R (87) 15 des Ministerkomitees des Europarates vom 17. September 1987 entspricht, Art. 27 Europolstatut. Der Verwaltungsrat, Art. 37 Europolstatut, ernennt auf Vorschlag des Direktors, Art. 38 Europolstatut, einen Datenschutzbeauftragten, Art. 28 Abs.1 Europolstatut, zu

---

[393] Vierter Tätigkeitsbericht der gemeinsamen Kontrollinstanz, https://www.dsk.gv.at/DocView.axd?CobId=35701, Seite 34, **2003** 5, **2004** 9, **2005** 6, **2006** 19, **2007** 122, **2008** 135, letzte Abfrage 16.01.2012.

dessen Aufgaben u.a. gehört, dafür zu sorgen, dass die Übermittlung und der Empfang personenbezogener Daten protokolliert werden und dass Betroffene auf Anfrage über die ihnen nach dem Statut zustehenden Rechte informiert werden. Außerdem ist er gehalten, mit der gemeinsamen Kontrollinstanz (GKI) zusammenzuarbeiten, Art. 28 Abs. 2 c Europolstatut. Die gemeinsame Kontrollinstanz hat die Aufgabe, die Aktivitäten von Europol dahingehend zu prüfen, ob durch die Datenverwendung bei Europol Rechte Einzelner verletzt werden und ob Übermittlungen rechtmäßig erfolgen, Art. 34 Abs. 1 Europolstatut. Außerdem hat die GKI Beratungsfunktionen, indem sie Anwendungs- und Auslegungsfragen in Bezug auf die Tätigkeit von Europol bearbeitet oder Vorschläge für Lösungen zu anstehenden Problemen erarbeitet, Art. 34 Abs. 3 Europolstatut. Österreich ist durch Vertreter der DSK in der gemeinsamen Kontrollinstanz vertreten, Art. 34 Abs. 1 Europolstatut, § 15 Abs. 1 EU-PolKG.
Die Zahl der bei Europol Beschäftigten ist mittlerweile auf über 600[394] gewachsen. Die GKI prüft im Regelfall einmal im Jahr die Abläufe und einzelne Vorgänge bei Europol[395], so dass man nicht von einer begleitenden Aufsicht sprechen kann. Auch in Bezug auf die Unparteilichkeit der GKI bestehen Bedenken, weil sie neben ihrer Aufgabe als Beschwerde- und Kontrollinstanz auch Beratungsfunktionen (Art. 34 Abs. 3 Europolstatut) ausübt und in die Situation geraten kann, über ihre eigenen Vorschläge oder Auslegungen zu entscheiden. Neben der GKI ist auch der Datenschutzbeauftragte für die Gewährleistung einer ordnungsgemäßen Bearbeitung personenbezogener Daten zuständig, Art. 28 Abs. 2 Europolstatut. Dieser ist zwar von Gesetzes wegen in der Erfüllung seiner Pflichten unabhängig, Art 28 Abs.1 Europolstatut, gehört aber zum Stab von Europol und wird vom Verwaltungsrat auf Vorschlag des Direktors gewählt. Er erfüllt damit ebenso wie die GKI nicht die Anforderungen an eine unabhängige Instanz.
In dem oben erwähnten Übereinkommen des Europarates aus dem Jahre 1981 wird zwar keine Überwachungsinstanz gefordert, wohl aber in den Empfehlungen des Ministerkomitees aus dem Jahre 1987. Dort wird unter Prinzip 1.1 gefordert, dass jeder

---

[394] Übereinkommen zum Schutz des der Menschen bei der Verarbeitung personenbezogener Daten, Übereinkommen 108 des Europates vom 28.01.1981,
http://conventions.coe.int/treaty/ger/treaties/html/108.htm, letzte Abfrage16.01.2012;
Council of Europe Committee of Ministers Recommendation No. R (87) 15 vom 17.09.1987,
http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1987_15.pdf, letzte Abfrage 16.01.2012
[395] Vierter Tätigkeitsbericht der gemeinsamen Kontrollinstanz, S. 24,
https://www.dsk.gv.at/DocView.axd?CobId=35701, letzte Abfrage 16.01.2012

Mitgliedstaat eine unabhängige Überwachungsbehörde außerhalb des Polizeisektors haben sollte, die die Einhaltung der gegebenen Empfehlungen überwacht. Übertragen auf Europol müsste eine Institution außerhalb dieser Organisation für die Überwachung zuständig sein. Insoweit ist die Empfehlung des Ministerkomitees also nicht umgesetzt worden. Unabhängig von dem Europolstatut, dem Europaratsübereinkommen und der Empfehlung des Ministerkomitees sind aber möglicherweise weitere datenschutzrechtliche Reglungen auf die Aktivitäten der Mitgliedstaaten und Europol in ihrer Zusammenarbeit anwendbar.

Die Datenschutzrichtlinie 96/46/EG sieht zwar in Art. 28 Abs. 1 unabhängige Kontrollstellen für den Datenschutz vor; sie enthält jedoch in Art. 3 Abs. 2 eine Ausnahmeregelung für den Bereich der polizeilichen und justiziellen Zusammenarbeit.

Der Rat der Europäischen Union hat am 27. November 2008 einen Rahmenbeschluss über den Schutz personenbezogener Daten[396] erlassen, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Dieser Rahmbeschluss sieht in Art. 25 Abs. 1 auch Kontrollstellen vor, die völliger Unabhängigkeit arbeiten sollen. Allerdings wird in den Gründen zum Rahmenbeschluss unter Ziffer 39 ausgeführt, dass die einschlägigen Datenschutzvorschriften bestimmter Rechtsakte, insbesondere solche, die die Arbeitsweise von Europol, Eurojust, des Schengener Informationssystems (SIS) und des Zollinformationssystems (ZIS) regeln, sowie diejenigen, die den direkten Zugriff der Mitgliedstaaten auf bestimmte Datensysteme anderer Mitgliedstaaten einführen, von dem Rahmenbeschluss unberührt bleiben. Begründet wird dies damit, dass die einschlägigen Vorschriften für die genannten Institutionen ein vollständiges in sich geschlossenes Regelwerk enthalten, das alle relevanten Datenschutzaspekte abdecke.

Seit 01.12.2009 ist der Vertrag von Lissabon in Kraft und mit ihm die Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000 (GRCh), die den gleichen Rang wie der der Vertrag selbst einnimmt, Art. 6 Abs. 1 EUV. Der Schutz personenbezogener Daten ist durch Art. 16 Abs. 1 AEUV und Art. 8 Abs.1 GRCh gewährleistet. Zwar gilt die Charta nicht uneingeschränkt. Sie ist aber maßgeblich für die Organe der Union und die Mitgliedstaaten bei der Ausführung von Unionsrecht,

---

[396] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. V L 350/60 vom 30.12.2008.

Art. 51 Abs. 1 GRCh. Art. 8 Abs. 3 der Charta legt fest, dass die Einhaltung der Datenschutzvorschriften in Art. 8 Abs. 2 GRCh durch eine unabhängige Stelle zu überwachen ist. Zu den detaillierten Anforderungen in Bezug auf die Unabhängigkeit im Sinne von Art. 28 Abs. 1 DSRL hat der Europäische Gerichtshof in seiner Entscheidung Kommission gegen Deutschland vom 09.03.2010 näher Stellung genommen.[397] In Deutschland sind die Datenschutzbehörden in die Verwaltung der Bundesländer integriert und unterliegen der allgemeinen Verwaltungsaufsicht. Nach Auffassung des Gerichtshofes ist Art. 28 Abs. 1 Unterabs. 2 der DS-RL so auszulegen, dass die für die Überwachung der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich zuständigen Kontrollstellen mit einer Unabhängigkeit ausgestattet sein müssen, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Diese Unabhängigkeit schließt nicht nur jegliche Einflussnahme seitens der kontrollierten Stellen aus, sondern auch jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins Gleichgewicht zu bringen, erfüllen. Da der Datenschutzbeauftragte bei Europol auf Vorschlag des Direktors vom Verwaltungsrat bestellt wird und damit zumindest in gewissem Umfange von diesen Organen abhängig ist, kann man nicht von einer unabhängigen Stelle im Sinne der Rechtsprechung des EuGH sprechen. Bei der GKI ist das zwar nicht der Fall, die Mitglieder rekrutieren sich aus den Kontrollstellen der Mitgliedsländer, aber im Hinblick auf die Beratungsfunktionen sind Zweifel an der Unabhängigkeit angebracht.

Die Europäische Kommission hat im November 2010 ein Gesamtkonzept für den Datenschutz in der Europäischen Union vorgestellt und Stellungnahmen dazu von den verschiedenen beteiligten Institutionen eingefordert.[398] Das Gesamtkonzept sieht u.a. eine Überarbeitung der DS-RL vor. Einbezogen werden soll auch eine Änderung des

---

[397] EuGH, Urteil vom 09.03.2010, Az. C-518/ 07, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=de&num=79899690C19070518&doc=T&ouvert=T&seance=ARRET , letzte Abfrage 16.01.2012.

[398] Die Konsultationsfrist war zum Zeitpunkt der Fertigstellung dieser Arbeit abgelaufen, aber ein neuer Rechtsakt der Union noch nicht erlassen worden. Im Januar 2012 hat die Kommission Entwürfe für eine Datenschutz-Grundverordnung und eine Richtlinie über den Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit vorgelegt Beide Regelwerke werden jedoch für EU-Organe wie Europol nicht gelten.

derzeitigen Kontrollsystems im Bereich der polizeilichen und justiziellen Zusammenarbeit.[399]

Die mangelnde Unabhängigkeit der Kontrollinstanzen ist aber nur eines von den datenschutzrechtlichen Problemen bei Europol. Nach Art. 30 Abs. 1 Europolstatut hat jede Person unter den in diesem Artikel genannten Voraussetzungen das Recht, in angemessenen Zeitabständen zu erfahren, ob sie betreffende Daten von Europol verarbeitet werden. Auskünfte werden von Europol jedoch nicht erteilt, wenn die zuständige nationale Kontaktstelle ihr Einverständnis unter Angabe entsprechender Gründe verweigert, Art. 30 Abs. 4 Europolstatut. Davon unabhängig kann Europol die geforderten Informationen verweigern, wenn dies aus seiner Sicht für die ordnungsgemäße Erfüllung der Aufgaben von Europol, zum Schutz der öffentlichen Sicherheit und Ordnung in den Mitgliedstaaten oder zur Bekämpfung von Straftaten, zur Vermeidung von Störungen bei den Ermittlungen und zum Schutze der Rechte und Freiheiten Dritter erforderlich ist, Art. 30 Abs. 5 Europolstatut. Ausnahmen sind allerdings laut der letztgenannten Bestimmung unter Berücksichtigung der Interessen betroffener Personen möglich. Betroffene Personen sind berechtigt, Europol zu ersuchen, sie betreffende Daten zu berichtigen oder zu löschen, wenn diese unrichtig oder Speicherfristen abgelaufen sind, Art. 31 Abs. 1 Europolstatut. Diese Regelungen entsprechen den Anforderungen der EuDSK, die in Art. 8 ein Auskunftsrecht und Löschungs- sowie Berichtigungsansprüche fordert, aber in Art. 9 Ausnahmen vor allem zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit sowie der Währungssicherheit oder zur Bekämpfung von Straftaten zulässt. Entsprechende Regeln stellt das Prinzip Nr. 6 der Empfehlung des Ministerkomitees des Europarates aus dem Jahre 1987 auf. Die Regelungen über Auskunfts- Berichtigungs- und Löschungsansprüche entsprechen nur dann den zu fordernden Datenschutzstandards, wenn sie den Anforderungen der Rechtsprechung des EGMR zu Art. 8 EMRK in diesen Punkten entsprechen. (siehe dazu Ausführungen unten zu „Art. 8 EMRK“)

Einer kritischen Betrachtung bedürfen die Analysedateien. Bei Kriminalitätsanalysen wird zwischen strategischen und operativen Analysen unterschieden. Die strategi-

---

[399] Gesamtkonzept für den Datenschutz in der Europäischen Union, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 04.11.2010, KOM(2010) 609 endgültig, S. 17, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf , letzte Abfrage 16.01.2012.

sche Analyse ist auf die Erstellung von Lagebildern, Beschreibung der Ursachen und Entwicklungstendenzen in bestimmten Kriminalitätsbereichen ausgerichtet, während bei der operativen Analyse personenbezogene Daten mit Informationen zum Tathergang verarbeitet werden, um verschiedene Tathergänge zu vergleichen und auf diese Weise Serientaten zu entdecken und neue Ermittlungsansätze zu finden oder Strukturen krimineller Verbindungen sichtbar zu machen.[400] Der Mehrwert liegt aus Sicht der Polizei darin, dass aus dem Zusammenführen bruchstückhafter Informationen neue Erkenntnisse gewonnen werden können, die es erlauben, rechtzeitig Gefahren zu erkennen und einzuschreiten und nicht erst zu reagieren, wenn eine Gefahr bereits konkret eingetreten ist.[401]

Das Problem liegt aus dem Gesichtspunkt des Datenschutzes insbesondere darin, dass nicht nur Daten von verurteilten Straftätern und Verdächtigten in eine Analyse einbezogen werden, sondern auch personenbezogene Daten von Zeugen, Opfern, Kontaktpersonen und Informanten, Art. 14 Abs. 1 Europolstatut. Die Daten erhält Europol von den nationalen Kontaktstellen der Mitgliedsländer, ggf. auf Anforderung, Art. 14 Abs. 3 Europolstatut. Diese Daten werden dann u.U. auch unter Einbeziehung von Daten aus anderen Quellen verarbeitet, wie z.B. mit Daten von Organisationen oder Drittstaaten, mit denen Kooperationsvereinbarungen getroffen worden sind, Art. 22 Abs. 1 und Art. 23 Abs. 1 Europolstatut. Darüber hinaus kann Europol auch Daten aus anderen Informationssystemen beziehen, wenn dafür entsprechende rechtliche Grundlagen bestehen, Art. 21 Europolstatut. Außerdem können – unter gewissen Einschränkungen - auch Daten von privaten Organisationen, Art. 25 Abs. 1 Europolstatut, und öffentlich zugänglichen Quellen, Art. 25 Abs. 4, verarbeitet werden. Dazu gehört sicherlich nicht zuletzt das Internet. Durch die analytische Aufbereitung der Gesamtheit der Daten entstehen neue Daten mit einer eigenen neuen Qualität. Nach Auffassung des derzeitigen Direktors von Europol, Rob Wainwright, liegen die besonderen Stärken seiner Organisation in der Analysekompetenz. Europol habe dadurch einzigartige Fähigkeiten und Möglichkeiten der Verbrechensbekämpfung

---

[400] Thanner/Vogl, Sicherheitspolizeigesetz, 4 Aufl. 2010, § 53 a, Anm. zu Abs. 2; Hauer/Kepplinger, Sicherheitspolizeigesetz, 11. Aufl. 2010, § 53 a Anm. 2.
[401] Thanner/Vogl aaO.

und beschäftige die besten Analytiker Europas. Europol habe eine Schlüsselstellung bei der Bekämpfung der organisierten Kriminalität und des Terrorismus erlangt.[402] Zweifelsohne hat Europol sehr gute Ergebnisse in ihrem Aufgabengebiet erzielt. Ob aber der Zweck unter datenschutzrechtlichen Gesichtspunkten die Mittel heiligt, ist eine noch zu beantwortende Frage. In den Analysedateien dürften vielfach personenbezogene Daten fern von ihrer ursprünglichen Zweckbestimmung verarbeitet werden, so dass eine Vereinbarkeit mit dem Zweck der ursprünglichen Verarbeitung nicht mehr besteht. Um diese Aktivitäten von Europol zu beurteilen und unter datenschutzrechtlichen Gesichtspunkten zu bewerten, soll noch einmal auf den Unterschied zur klassischen Strafverfolgung hingewiesen werden. Letztere setzt erst nach einer Straftat, der Gefahr einer Straftat oder einer Gefahr für die öffentliche Sicherheit und Ordnung ein. Für die Annahme einer Gefahr müssen konkrete Anhaltspunkte vorliegen. Soweit sich dabei Taten oder Verdachtsmomente Personen zuordnen lassen, bestehen gegen eine Ermittlungstätigkeit und die Speicherung personenbezogener Daten von Tätern und Verdächtigen unter Beachtung datenschutzrechtlicher Bestimmungen grundsätzlich keine Bedenken. Bei der Analyse durch Europol auf der Grundlage der so genannten Arbeitsdateien sind diese Voraussetzungen im Regelfall nicht gegeben. Es geht darum, ohne Vorliegen eines konkreten Verdachtes gegen eine oder mehrere Personen oder Organisationen, potentielle Gefahren zu erkennen. In diesem Stadium bestehen weitestgehend nur Vermutungen in Bezug auf mögliche Straftaten. Aufgrund von strategischen Analysen werden Lagebilder mit möglichen Bedrohungs- und Gefährdungspotentialen generiert. Die auf diese Weise erzielten Ergebnisse werden in „täterorientierte Verdachtsgewinnungsregister“ einbezogen, um dann an Hand weiterer Quellen wie Vernehmungen, Tätigkeitsberichten, Berichten verdeckter Ermittler usw. eine Vermutung oder einen Verdacht zu erzeugen.[403] Dabei können auch sensible Daten verarbeitet werden, wenn dies für den Zweck der Aufgabenstellung unbedingt erforderlich ist, Art. 14 Abs. 1 Europolstatut. Darüber entscheiden aber nach Lage der Dinge die Bearbeiter in der Analysegruppe selber. Es handelt sich um eine Verdachtsgewinnungsstrategie. Offensichtlich wird zu diesem Zweck eine offensive Informationsbeschaffung im Wege des Data-Mining

---

[402] „Einzigartige Möglichkeiten“, Europoldirektor Rob Wainwright über die Struktur, Dienste und Zukunft des europäischen Polizeiamtes Europol in Den Haag. In Öffentliche Sicherheit 2010, S. 14-16.
[403] Schubert, Europol und der virtuelle Verdacht – Die Suspendierung des Rechts auf informationelle Selbstbestimmung, 2008, S. 106.

betrieben, wobei auf der Grundlage automatisierter Suchmuster verschiedene Informationssysteme durchsucht werden. Die Relevanz von Personen und ihren Daten zu der angenommenen Gefahr kann zum Zeitpunkt des durch die Speicherung und Verarbeitung ausgelösten Eingriffs in der Regel noch nicht bestimmt, sondern nur vermutet werden. Dadurch entsteht die Gefahr, dass unbescholtene Bürger grundlos für die Zwecke von Europol vereinnahmt werden.[404]

Art. 5 EuDSK schreibt u.a. vor, dass personenbezogene Daten, die automatisch verarbeitet werden, nach Treu und Glauben und auf rechtmäßige Weise beschafft und verarbeitet werden müssen und nur für ***festgelegte*** und rechtmäßige Zwecke gespeichert und nur so verwendet werden dürfen, dass es mit diesen Zwecken nicht unvereinbar ist. Die Mehrzahl der Daten wird aus Quellen der Mitgliedstaaten im Wege der Amtshilfe oder anderen Organisationen und Einrichtungen beschafft, wobei die Verwendung dieser Daten bei Europol dem ursprünglichen Verarbeitungszweck nicht entsprechen oder mit diesem auch nur vereinbar sein dürfte. Die Art und Weise der Verarbeitung von personenbezogenen Daten entspricht unter diesen Umständen nicht den in Art. 5 EuDSK aufgestellten Qualitätskriterien. Allerdings erlaubt Art. 9 EuDSK Ausnahmen von Art. 5 EuDSK, wenn sie durch das Recht der Vertragspartei vorgesehen und in einer demokratischen Gesellschaft zum Schutz Sicherheit des Staates notwendige Maßnahmen sind. Als gesetzliche Maßnahme käme hier das Europolstatut in Betracht.

Die Europäische Datenschutzkonvention begründet keine Rechte Einzelner und verpflichtet lediglich die Mitgliedstaaten, die Konvention in innerstaatliches Recht umzusetzen, Art. 4 Ziffer 1 EuDSK. Weiter enthält Art. 12 Ziffer 2 EuDSK das grundsätzliche Verbot, die Übermittlung von Informationen allein aus Gründen des Datenschutzes zu verweigern. Aus diesen Gründen gewährt die Europaratskonvention nur ein geringes Schutzniveau. Dies wiegt umso schwerer, weil eine ausreichende Kontrolle durch eine von Europol unabhängige Instanz, wie z.B. durch einen Parlamentsausschuss, nicht gewährleistet ist.

Bei der Empfehlung des Ministerrates Nr. R (87) 15 vom 17.09.1987, auf die in Art. 27 Europolstatut gleichfalls als Datenschutzstandard Bezug genommen wird, handelt es sich um eine unverbindliche Handlungsanweisung, aus der Bürger keine un-

---

[404] Schubert, aao: S. 107.

mittelbaren Rechte herleiten können. Sie ist im Übrigen auch so gefasst, dass Ausnahmen von den vorgegebenen Grundsätzen durch geeignete Regelungen möglich sind. Ein Beispiel dafür ist Prinzip Nr. 2.1 der Empfehlung. Dort heißt es, dass personenbezogene Daten für polizeiliche Zwecke nur gespeichert werden sollen, wenn es für die Abwehr einer wirklichen Gefahr oder die Abwehr eines bestimmten kriminellen Angriffs erforderlich ist. Diese Voraussetzungen dürften bei den Arbeitsdateien von Europol nicht gegeben seien, weil diese darauf ausgerichtet sind, erst Verdachtsmomente zu generieren. Die Empfehlung lässt jedoch Ausnahmen von diesem Grundsatz durch nationale gesetzliche Regelungen zu. Insgesamt ist deshalb festzustellen, dass der Datenschutz im Europolstatut schwach ausgeprägt ist. Europol wird deshalb auch vorgeworfen, dass die polizeiliche Opportunität und nicht unbedingt rechtliche Gesichtspunkte dafür maßgeblich sind, was in den Arbeitsdateien landet.[405] Das Problem wird dadurch etwas gemildert, dass der Zugriff auf die Arbeitsdateien grundsätzlich auf den Personenkreis der jeweiligen Analysegruppe beschränkt ist, Art. 14 Abs. 2 Europolstatut, und für die Errichtung und den Betrieb strenge Durchführungsbestimmungen erlassen worden sind.[406]

In ihrem Gesamtkonzept zur Reform des Datenschutzes in der EU[407] plant die Kommission auch neue Bestimmungen für die polizeiliche und justizielle Zusammenarbeit in der EU. Der Rahmenbeschluss des Rates vom 27. November 2008[408] enthalte zu viele Ausnahmen vom Zweckbindungsgrundsatz und gelte im Übrigen nicht für die sektorspezifischen Vorschriften über die polizeiliche und justizielle Zusammenarbeit, insbesondere nicht die Rechtsakte über Europol, Eurojust und das Schengener Informationssystem SIS und das Zollinformationssystem ZIS. Die Empfehlung des Ministerkomitees R (87) des Europarates[409] sei nicht rechtsverbindlich und dies könne

---

[405] Aden in Rogan (Hrsg.) Handbuch zum Recht der inneren Sicherheit, 2. Aufl. 2006, S. 559.
[406] Beschluss 2009/936/JI des Rates vom 30.November 2009 zur Annahme der Durchführungsbestimmungen für die von Europol geführten Arbeitsdateien zu Analysezwecken, ABl. vom 11. 12 2009 L 325 /14.
[407] 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 vom 4.11.2010, KOM(2010) 609 endgültig, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf, letzte Abfrage 16.01.2012.
[408] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. V L 350/60 vom 30.12.2008
[409] Empfehlung R (87) 15 des Ministerkomitees des Europarates zur Regelung der Benutzung personenbezogener Daten durch die Polizei, Europarat, 17. September 1987,

sich direkt auf die Möglichkeiten von Bürgern auswirken, ihre Datenschutzrechte in diesem Bereich auszuüben. Deshalb müsse auch eine Änderung der geltenden Datenschutzregeln im Bereich der polizeilichen und justiziellen Zusammenarbeit in Erwägung gezogen werden.[410]

Art. 8 GRCh

Da das Europolstatut selbst keinen angemessenen Datenschutzstandard gewährleistet, stellt sich bei der Bewertung der Arbeitsdateien zu Analysezwecken die Frage, ob die dabei geübte Praxis bei Europol mit der Charta der Grundrechte der EU vereinbar ist. Die Charta der Grundrechte hat den gleichen Rang wie Primärrecht der EU, Art. 6 Abs. 1 EUV. Art. 8 Abs. 1 GRCh, ebenso Art. 16 Abs. 1 AEUV, gewährt ausdrücklich ein Recht auf den Schutz personenbezogener Daten. Nach Art. 8 Abs. 2 GRCh dürfen Daten nur nach Treu und Glauben für festgelegte Zwecke und nur mit Einwilligung der betroffenen Person oder auf der Grundlage einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jeder hat das Recht, Auskunft über die ihn betreffenden Daten zu erhalten und ggf. eine Berichtigung zu verlangen. Nach Art. 8 Abs. 3 GRCh soll die Einhaltung dieser Vorschriften durch eine unabhängige Stelle überwacht werden. Mit der Formulierung *„oder auf einer sonstigen gesetzlichen legitimen Grundlage*“ in Art. 8 Abs. 2 GRCh enthält die Bestimmung eine Schrankenregelung, die die Einschränkung des Grundrechtes auf Schutz personenbezogener Daten durch geeignete gesetzliche Regelungen ermöglicht. Dabei stellt sich die Frage des Verhältnisses zu der allgemeinen Schrankenregelung in Art. 52 Abs. 1 GRCh. Aus den Erläuterungen des Präsidiums zur GRCh ist zu entnehmen, dass Art. 8 GRCh „*gemäß den Bedingungen nach Art. 52 der Charta eingeschränkt werden kann“.*[411] In der Literatur wurde darüber diskutiert, ob dabei von einer Doppelbeschränkung ausgegangen werden muss und damit die einheitliche Schranke des Art. 52 Abs.1 GRCh durchlöchert wird.[412] Bei näherem Hinsehen zeigt sich, dass sich die Regelungen ergänzen. Art. 52 Abs. 1 GRCh stellt den Grundsatz

---

http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1987_15.pdf, letzte Abfrage 16.01.2012.

[410] Gesamtkonzept für den Datenschutz in der Europäischen Union vom 4.11.2010 aaO. S. 15 f..

[411] Erläuterungen zur Grundrechtecharta der EU, EuGRZ 2000, S. 559 ff. (561);

[412] Eisner, Die Schrankenregelung der Grundrechtscharta der Europäischen Union, Diss. 2004, S. 132

der Verhältnismäßigkeit in den Vordergrund, während Art. 8 Abs. 2 GRCh das Prinzip von Treu und Glauben sowie Zweckbindung betont.[413]

Die Grundrechte wie sie in der der EMRK gewährleistet sind und wie sie sich aus den allgemeinen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, sind als allgemeine Grundsätze Teil des Unionsrechts. Bereits vor Inkrafttreten der Charta hat der EuGH im Rahmen der Auslegung von datenschutzrechtlichen Regelungen auf die Charta der Grundrechte der EU und die der EMRK sowie die zu letzterer ergangene Rechtsprechung zurückgegriffen.[414] In der zitierten Entscheidung hat er die Auffassung vertreten, dass die Richtlinien der EU in Einklang mit den Grundrechten der Charta und unter Berücksichtigung allgemeiner Grundsätze des Gemeinschaftsrechts wie dem Grundsatz der Verhältnismäßigkeit auszulegen sind. Die Grundrechte seien integraler Bestandteil der allgemeinen Rechtsgrundsätze, deren Wahrung der Gerichtshof zu sichern habe. Der Gerichtshof lasse sich dabei von den gemeinsamen Verfassungstraditionen der Mitgliedstaaten sowie von den Hinweisen leiten, die die völkerrechtlichen Verträge über den Schutz der Menschenrechte geben, an deren Abschluss die Mitgliedstaaten beteiligt waren oder denen sie beigetreten sind. Hierbei komme der EMRK besondere Bedeutung zu.[415] Nach Inkrafttreten des Vertrages und der Charta der Grundrechte der EU hat der EuGH die Bestimmungen der Charta als EU-Grundrechte mit Hinweis auf Art. 6 Abs.1 EUV unmittelbar angewendet[416] und bereits verschiedene Entscheidungen zu den Grundrechten der GRCh getroffen.[417]

Detaillierte Datenschutzbestimmungen auf der Grundlage von Art 16 Abs. 2 AEUV wie z. B. eine Neuauflage der Datenschutzrichtlinie 95/46 EG sind noch nicht erlas-

---

[413] Britz,, Das Grundrecht auf Datenschutz in Art. 8 der Grundrechtscharta, Kap. II,3., http://www.datenschutz.hessen.de/download.php?download_ID=188, letzte Abfrage 16.01.2012.

[414] Urteil des EuGH vom 18.07.2007, Productores de Música de España (Promusicae) gegen Telefónica de España SAU, C 275/06, LNR 2007, 35876, Rn. 61 bis 70, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006J0275:DE:HTML, letzte Abfrage 16.01.2012, siehe auch Tinnefeld, Reformvertrag von Lissabon, Charta der Grundrechte und Rechtspraxis im Datenschutz, DuD 2009, S. 504.

[415] Urteil des EuGH (Große Kammer) vom 27. Juni 2006 , C-540/03, Europäisches Parlament gegen Rat der Europäischen Union, Rn. 35, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62003J0540:DE:HTML, letzte Abfrage 16.01.2012.

[416] Urteil des EuGH vom 19. Januar, 2010 Seda Kücükdeveci gegen Swedex GmbH & Co. KG, C-555/07, Rn. 22, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62007J0555:DE:HTML , letzte Abfrage 16.01.2012 .

[417] Siehe Kokott,Sobotta, Die Charta der Grundrechte der Europäischen Union nach dem Inkrafttreten des Vertrages von Lissabon, EuGRZ 2010, S. 265 ff..

sen worden, sondern befinden sich erst im Stadium der Vorbereitung.[418] Zur Zeit liegt Entwürfe der Kommission für eine Datenschutz-Grundverordnung und eine Richtlinie für den Datenaustausch zwischen den Mitgliedstaaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit vor (siehe dazu Kapitel 2.6). Die entsprechenden Vorschriften würden jedoch für Europol als EU-Agentur nicht gelten.

Unabhängig davon soll geprüft werden, ob die beschriebenen Datenverwendungen von Europol mit bereits bestehenden Regelungen in Einklang stehen.
Nach Art. 8 Abs.1 GRCh hat jede Person das Recht auf den Schutz der sie betreffenden personenbezogenen Daten. Nach den Schrankenregelungen der Art. 8 Abs. 2 und 52 Abs. 1 GRCh sind Einschränkungen dieses Rechts zulässig, wenn sie gesetzlich vorgesehen sind, den Wesensgehalt dieses Rechts achten und unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutz der Rechte und Freiheiten anderer tatsächlich entsprechen.[419] Ein Eingriff in das Recht auf Datenschutz ist gegeben, wenn Europol die betreffenden Daten verwendet. Die gesetzliche Grundlage ergibt sich aus dem Europolstatut. Mit der Bekämpfung des Terrorismus und der schweren Kriminalität dient die Verwendung auch Zielen des Gemeinwohls. Es bleibt zu prüfen, ob die Einschränkung des Rechts aus Art. 8 Abs. 1 GRCh in einem angemessenen Verhältnis zu dem verfolgten berechtigten Zweck steht. Soweit bekannt, hat der EuGH sich bisher noch nicht mit der Verhältnismäßigkeit im Bereich der öffentlichen Sicherheit befasst. Der Datenschutz in der EU beruht aber nicht allein auf Primär- und Sekundärrecht der EU. Durch die Charta werden bereits anerkannte Grundrechte nicht verändert. Nach Art. 52 Abs. 3 GRCh haben Bestimmungen der Charta, die Rechte enthalten, welche denen der EMRK entsprechen, die gleiche Bedeutung und Tragweite wie sie ihnen in der genannten Konvention verliehen werden. Die Grundrechte der Charta sind darü-

---

[418] Siehe Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts-und Sozialausschuss und den Ausschuss der Regionen vom 4.11.2010, KOM(2010) 609 endgültig, Gesamtkonzept für den Datenschutz in der Europäischen Union, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf , letzte Abfrage 16.01.2012.
[419] Urteil des EuGH vom 09.11. 2010, Schecke u. Eifert gg. Land Hessen, Ziffer 65, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62009J0092:DE:HTML, letzte Abfrage 16.01.2012.

ber hinaus im Einklang mit den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten auszulegen, Art. 52 Abs. 4 GRCh. Die Grundrechte der Verfassungsüberlieferungen und auch die der EMRK sind zwar nicht unmittelbares Unionsrecht, aber finden über die Einordnung als Bestandteil der allgemeinen Rechtsgrundsätze Anwendung, Art. 6 Abs. 2 EUV.[420] Die bisherige Rechtsprechung des EuGH zu Grundrechten hat also weiterhin Bestand, und auch die Rechtsprechung des EGMR zur EMRK ist im Rahmen der gemeinsamen Verfassungsüberlieferungen heranzuziehen.[421] Das bedeutet in der Praxis, dass im Rahmen des Grundrechtes auf den Schutz personenbezogener Daten gemäß Art. 8 Abs.1 GRCh in jedem Fall als Mindeststandard das gilt, was der EGMR im Rahmen seiner Rechtsprechung zu Art. 8 EMRK an Grundsätzen zum Datenschutz entwickelt hat. Dadurch kann sich in Zukunft möglichweise eine Art Rechtsprechungskonkurrenz zwischen EuGH und EGMR entwickeln, die beide Gerichte allerdings durch eine geeignete Abstimmung zu vermeiden trachten.[422]

.

Es liegt also nahe, auf die vom EGMR entwickelten Grundsätze zur Verhältnismäßigkeit von Maßnahmen der öffentlichen Sicherheit für die Frage der Verhältnismäßigkeit im Rahmen der Prüfung des Art. 8 Abs.2 EMRK iVm. Art. 52 Abs.1 GRCh zurückzugreifen, wie sie nachfolgend beschrieben werden.

Art. 8 EMRK

Die Verwendung und Weitergabe personenbezogener Daten bedeuten Eingriffe in das von Art. 8 Abs. 1 EMRK geschützte Privatleben des betreffenden Bürgers.[423] Etwaige Eingriffe in das von Art. 8 Abs. 1 EMRK geschützte Privatleben sind nur unter den Voraussetzungen des Art. 8 Abs. 2 EMRK zulässig. Als Ausnahmebestimmung von der Regel des Art. 8 Abs. 1 EMRK ist Art. 8 Abs. 2 EMRK eng auszulegen.[424]

---

[420] Grabenwerter, Europäische Menschenrechtskonvention, 4. Aufl. 2009, § 4 Anm. 2
[421] Kokott,Sobotta, Die Charta der Grundrechte der Europäischen Union nach dem Inkrafttreten des Vertrages von Lissabon, EuGRZ 2010, S. 265 ff, (267).
[422] Gemeinsame Erklärung der Präsidenten von EGMR (Straßburg)und EuGH (Luxemburg) vom 24. Januar 2011, „Parallele Auslegung“ von GRCh und EMRK sowie Beitritt der EU zur EMRK, EuGRZ 2011, S. 95 f..
[423] EGMR-Urteil vom 28.01.2003, Peck gg. Vereinigtes Königreich, ÖJZ 2004, S. 651 ff.(652).
[424] EGMR-Urteil vom 04.05.2000 Rotaru gg. Rumänien , OJZ 2001, S. 74 ff.(76).

Als erste Voraussetzung muss eine gesetzliche Grundlage für den Eingriff bestehen. Das Europolstatut und das EuPolKG kommen als gesetzliche Grundlage in Betracht. Die Gesetze müssen für die Betroffenen zugänglich und in ihren Konsequenzen für ihn vorhersehbar sein.[425] Bei der Verwendung unbestimmter Rechtsbegriffe in der Beschreibung des Anwendungsbereiches ist die Vorhersehbarkeit nur gegeben, wenn diese Begriffe durch eine gefestigte Rechtsprechung hinreichend konkretisiert sind und diese für den Betroffenen zugänglich ist.[426] Der Gerichtshof hat darüber hinaus deutlich gemacht, dass *„gesetzlich vorgesehen“* nicht nur einen schlichten Verweis auf innerstaatliches Recht bedeutet, sondern sich auch auf die Gesetzesqualität bezieht und Anforderungen an die Rechtsstaatlichkeit der jeweiligen Normen bedeutet. Der Begriff bedeute, dass das innerstaatliche Recht einen gewissen Schutz gegenüber willkürlichen Eingriffen der öffentlichen Gewalt gewähren müsse. Es müsse genügend klar abgefasst sein, um dem Einzelnen deutlich zu machen, unter welchen Umständen und unter welchen Bedingungen es die öffentliche Gewalt ermächtigt, einen geheimen und potentiell gefährlichen Eingriff in die Privatsphäre vorzunehmen.[427] Soweit den Behörden ein Ermessen eingeräumt wird, muss das betreffende Gesetz die Reichweite des Ermessens angeben, wenn auch die Einzelheiten der Bedingungen und der zu beachtenden Verfahren nicht in demselben Gesetz enthalten sein müssen.[428]

Im Rahmen der Rechtfertigungsprüfung eines Eingriffs ist zunächst festzustellen, ob einer der in Art. 8 Abs. 2 EMRK auf geführten legitimen Zwecke in Betracht kommt. Der Schutz der nationalen Sicherheit oder der öffentlichen Ordnung können es erforderlich machen, personenbezogene Daten zu speichern, insbesondere wenn es um die Verhinderung von Straftaten geht.[429]

---

[425] EGMR-Urteil vom 24.04.1990, Kruslin gg. Frankreich, 11801/85, ÖJZ 1990, 564 ff.(565), Ziffer 27. „*Der Ausdruck gesetzmäßig iSd Art 8 Abs. 2 verlangt zu8nächst, daß die bekämpfte Maßnahme eine Grundlage im innerstaatlichen Recht hat; er bezieht sich aber auch auf die Qualität des in Betracht kommenden Gesetzes (quality oft he law), indem er verlangt, daß dieses für den Betroffenen zugänglich (accessible) ist. Dieser muß außerdem die Auswirkungen des Gesetzes vorhersehen können und es muß mit dem Grundsatz der Rechtsstaatlichkeit vereinbar sein (compatible with the rule of law).*“.

[426] EGMR-Urteil vom 24.04.1990, Kruslin gg. Frankreich, aaO. S. 565 „*Eine gefestigte Rechtsprechung dieser Art kann nicht unbeachtet bleiben”.*

[427] EGMR- Urteil vom 02.08.1984, Malone gg. Vereinigtes Königreich, Ziffer 67, EGMR-E 2, 452 ff.; EGMR-Urteil vom 16.02.2000, Amann gg. Schweiz, Ziffer. 56, ÖJZ 2001, 71ff .

[428] EGMR Urteil vom 25. März 1983, Silver u.a. gegen Vereinigtes Königreich, Ziffer 88 f., EGMR-E 2, S. 227 ff..

[429] EGMR Urteil vom 06.09.1978, Klass u.a. gegen Deutschland, Ziffer 48, EGMR-E 1, S. 320 ff..

Abgesehen von der Verfolgung eines legitimen Zweckes müssen Eingriffe in die Privatsphäre in einer demokratischen Gesellschaft notwendig sein und einem dringenden sozialen Bedürfnis entsprechen[430], also verhältnismäßig in Bezug auf den verfolgten legitimen Zweck und die eingesetzten Mittel sein. Die Behörden haben hier einen Beurteilungsspielraum, dessen Reichweite nicht nur von dem verfolgten rechtmäßigen Ziel, sondern auch von der Schwere des Eingriffs abhängt. Das Interesse des Staates, seine nationale Sicherheit zu schützen, muss gegen die Schwere des Eingriffs in das Recht auf Achtung des Privatlebens abgewogen werden.[431] In Fragen der nationalen Sicherheit und der Verhütung von Straftaten räumt der Gerichtshof den nationalen Behörden einen weiten Beurteilungsspielraum ein.[432] Wie schon mehrfach ausgeführt, dürfen geheime Überwachungsmaßnahmen zur Gewinnung von Daten und Erkenntnissen aber nicht ohne Anlass durchgeführt werden. Eine allgemeine und „ausforschende" Überwachung darf nicht erfolgen.[433] Als Anlass für derartige Maßnahmen hat der Gerichtshof den Verdacht angesehen, dass jemand bestimmte Straftaten plant oder begangen hat.

Ungeachtet des eingeräumten Beurteilungsspielraumes insbesondere in Fragen der öffentlichen Sicherheit hält der Gerichtshof es im Rahmen der Verhältnismäßigkeit des Eingriffs für erforderlich, dass ausreichende Sicherheiten gegen einen Missbrauch der staatlichen Befugnisse bestehen.[434] Dabei hält das Gericht eine richterliche Kontrolle für wünschenswert, aber nicht für zwingend erforderlich, wenn die Kon-

---

[430] EGMR-Urteil vom 04.05.2000 Rotaru gg. Rumänien, OJZ 2001, S. 74 ff..

[431] EGMR Urteil vom 26. März 1987 Leander gg. Schweden, Ziffer 59, EGMR-E 3, 430 ff.; EGMR Urteil vom 25.02.1997. Z. gg. Finnland, (9/1996/627/811), ÖJZ 1998, 152 ff..

[432] EGMR Urteil vom 29.06. 2006 Weber u. Saravia gg. Deutschland, NJW 2007, S. 1433 ff.(1437), Ziffer 106: *"…. Bei der Abwägung des Interesses des beklagten Staates, die nationale Sicherheit durch geheime Überwachungsmaßnahmen zu schützen, mit der Schwere des Eingriffs in das Recht eines Bf. Auf Schutz seines Privatlebens haben die Behörden bei der Wahl der Mittel zum Erreichen des berechtigten Ziels des Schutzes der nationalen Sicherheit einen ziemlich weiten Ermessensspielraum"*; siehe auch Klass gg. Deutschland, EGMR-E 1, S. 320 ff., Ziffer 48 ,.

[433] EGMR Urteil vom 06.09.1978, Klass gg. Deutschland, Ziffer 51, EGMR-E 1, S. 320 ff.

[434] EGMR Urteil vom 05.04.2005, Brinks gg. Niederlande, Ziffern 77 und 78 http://www.hrr-strafrecht.de/hrr/egmr/04/9940-04.php, letzte Abfrage 25.05.2012, Ziffer 78: „*In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain safeguards established by law which apply to the supervision of the relevant services' activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure.".*

trolle durch eine anderweitige Institution erfolgt, die eine ausreichende Unabhängigkeit und Unparteilichkeit gewährleistet.[435]

Unabhängig von wirksamen Kontrollen während der Durchführung von geheimen Maßnahmen und damit verbundenen Verwendungen personenbezogener Daten, stellt sich die Frage, ob die Betroffenen nach Abschluss der Maßnahmen zu unterrichten sind, um diese ggf. auf dem Rechtswege nachträglich anfechten zu können. Der Gerichtshof ist der Auffassung, dass dies erfolgen sollte, sobald das ohne Gefährdung des Zwecks der Maßnahmen und der dabei verwandten Methoden geschehen kann.[436]

Hinsichtlich der Übermittlung von Daten ist der Grundsatz der Zweckbindung zu beachten. Eine Weitergabe von Daten an eine andere Behörde sieht der EGMR nur dann als mit Art. 8 Abs. 2 EMRK vereinbar an, wenn die Daten vor der Übermittlung gekennzeichnet werden und Ihre Verwendung an den Zweck der ursprünglichen Erhebung gebunden wird.[437]

Zu Speicher- und Löschungsfristen vertritt der EGMR die Auffassung, dass personenbezogene Daten zu löschen sind, sobald sie für den ursprünglich verfolgten legitimen Zweck nicht mehr benötigt werden. Eine Prüfung der Notwendigkeit zu einer Aufrechterhaltung der Speicherung in kürzeren Abständen wird als erforderlich erachtet.[438] Eine Überprüfungsperiode von sechs Monaten hat er als angemessen angesehen.[439]

In einem Fall aus dem Jahre 1987 hat der EGMR entschieden, dass keine Verpflichtung zur Auskunft über personenbezogene Daten aus dem Polizeiregister an Betroffene besteht.[440] Andererseits hat der Gerichtshof im Jahre 2002 auf der Grundlage von Art. 8 Abs. 1 EMRK als Ausfluss der Verpflichtung zum Schutz des Familienlebens und der Privatsphäre eine positive Verpflichtung der Staates auf Auskunft aus

---

[435] EGMR Urteil vom 06.09.1978, Klass u.a. gegen Deutschland, Ziffern 53 bis 56, EGMR-E 1, S. 320 ff..

[436] EGMR Urteil vom 29.06. 2006, Weber u. Saravia gg. Deutschland, NJW 2007, S.1433 ff.(1439), Ziffer 135 *"Sobald das (*Offenlegung der Maßnahmen, Anm. des Verfassers*) aber ohne Gefährdung des Überwachungsziels nach Abschluss der Überwachungsmaßnahmen geschehen kann, sollten die Betroffenen davon unterrichtet werden.".*

[437] EGMR Urteil vom 29.06. 2006, Weber u. Saravia gg. Deutschland, (54934/00),NJW 2007, S. 1433 ff., Ziffern 121,122.

[438] EGMR Urteil vom 29.06. 2006, Weber u. Saravia gg. Deutschland, (54934/00),NJW 2007, S.1433, Ziffern 116, 132.

[439] EGMR Urteil vom 06.09.1978, Klass u.a. gegen Deutschland, Ziffer 53, EGMR-E 1, S. 320 ff.

[440] EGMR Urteil vom 26.03.1987, Leander gg. Schweden, Ziffer 74, EGMR-E 3, S. 430 ff.

Sozialversicherungsakten an den Betroffenen anerkannt. Dabei hat er auf einen gerechten Ausgleich zwischen den Interessen der involvierten Gemeinde und denen des betroffenen Bürgers abgehoben. Auch sind die Gründe für eine Verweigerung zu nennen, damit der Bürger ggf. dagegen klagen kann.[441] Grundsätzlich erkennt der Gerichtshof also einen Auskunftsanspruch an, wenn im Einzelfall auf der Grundlage einer gerechten Abwägung die privaten Interessen des Einzelnen gegenüber dem staatlichen Geheimhaltungsinteresse überwiegen.

9.2.1.4.3 Zwischenergebnis

Wenn man bedenkt, dass Europol praktisch kaum begrenzte Möglichkeiten besitzt, auch personenbezogene Daten von Bürgern in Arbeitsdateien zu verarbeiten, die nicht im Verdacht stehen, eine Straftat begangen zu haben oder eine solche zu begehen, dann ist dies unter Berücksichtigung der Rechtsprechung des EGMR als anlasslose Verwendung von personenbezogenen Daten kritisch zu betrachten. Auch eine Vereinbarkeit mit dem ursprünglichen Zweck der Speicherung dürfte in vielen Fällen nicht gegeben sein. Eine wirksame, durchgängige und nicht nur gelegentliche Kontrolle der Analysetätigkeit von Europol durch eine unabhängige Instanz, wie sie auch in Art 8 Abs. 3 GRCh ausdrücklich vorgesehen ist, ist nicht gewährleistet. Die GKI und der Datenschutzbeauftragte bei Europol erfüllen die daran zu knüpfenden Anforderungen nicht. Bei der Übermittlung von Daten an andere Organisationen ist Europol verpflichtet, den Vorgang zu protokollieren. Der Empfänger muss zusichern, dass die Daten nur zu dem Zweck genutzt werden, zu dem sie übermittelt worden sind, Art. 24 Abs. 2 Europolstatut. Sind die Daten ursprünglich aus einen Mitgliedstaat übermittelt worden, so ist auch dessen Zustimmung für eine Weitergabe erforderlich, Art 24 Abs. 1 Europolstatut. Diese Handhabung einer Übermittlung von personenbezogenen Daten dürfte den Anforderungen des EGMR entsprechen. Die für die Prüfung der Erforderlichkeit für eine weitere Speicherung vorgesehene Frist von drei Jahren gemäß Art: 20 Abs. 1 Europolstatut dürfte aber nach den vom EGMR aufgestellten Kriterien zu lang sein. Hinsichtlich des Auskunftsrechts Betroffener erlaubt Art. 30 Abs. 5 die Verweigerung einer Auskunft bei Vorliegen der dort genannten Gründe, lässt aber Ausnahmen unter Berücksichtigung der Interessen der betrof-

---

[441] EGMR Urteil vom 24.09.2002, M.G. gg. Vereinigtes Königreich, Ziffern 27 bis 30, ÖJZ 2004, S. 65 ff.(66) .

fenen Person zu. Es wird jeweils im Einzelfall zu beurteilen sein, ob die vom EGMR geforderte Abwägung zwischen öffentlichem Interesse an der Vertraulichkeit und dem Interesse auf Schutz der Privatsphäre vorgenommen worden ist.

9.2.1.4.4 Rechtsschutz bei Datenübermittlungen an Europol

Hinsichtlich der von der nationalen Kontaktstelle, dem Bundeskriminalamt (BKA) innerhalb des Ministeriums des Inneren (BMI), an Europol übermittelten personenbezogenen Daten ist das BKA dafür verantwortlich, dass die Erhebungen und Übermittlungen im Einklang mit den österreichischen Vorschriften erfolgen, Art. 29 Abs. 1 Buchst. a Europolstatut. Jedermann kann sich an die nationale Europolstelle, das BKA, wenden, um Auskunft zu erhalten, ob Europol ihn betreffende personenbezogene Daten verarbeitet, § 1 Abs. 3 Ziffer 1 DSG 2000, § 16 Abs. 1 EU-PolKG. Die Auskunft kann aus den in § 16 Abs. 2 EU-PolKG aufgeführten Gründen verweigert werden. Die dort genannten Kriterien stellen eine Erweiterung der in § 26 Abs. 2 DSG 2000 aufgeführten Verweigerungsgründe dar. Außerdem haben die Bürger das Recht, unrichtige oder unrechtmäßig verarbeitete Daten, die vom BKA an Europol oder umgekehrt übermittelt worden sind, berichtigen oder löschen zu lassen, § 17 Abs. 1 EU-PolKG, §§ 1 Abs. 3 Ziffer 2, 27 Abs. 1 DSG 2000. Betroffene können wegen Erteilung oder Nichterteilung einer Auskunft oder wegen Verweigerung der Löschung und/oder Berichtigung Beschwerde bei der nationalen Europolstelle einlegen. Diese ist dann an die gemeinsame Kontrollinstanz bei Europol weiterzuleiten, § 18 EU-PolKG. Das ist insofern irreführend, weil die datenschutzrechtliche Verantwortung für die Daten, die an Europol übermittelt worden sind, bei Österreich verbleibt. Gemeint ist wohl, dass eine Stellungnahme der GKI einholt wird, wie über die Beschwerde zu entscheiden ist. Die Bürger haben auch die Möglichkeit, sich unmittelbar an Europol zu wenden und Auskunft zu verlangen, Art. 30 Abs. 1 Europolstatut, und sie betreffende fehlerhafte Daten berichtigen oder löschen zu lassen, Art. 31 Abs. 1 Europolstatut. Sind dabei Daten betroffen, die von österreichischen Behörden an Europol übermittelt worden sind, wird Europol die nationale Kontaktstelle verständigen und in Abstimmung mit ihr handeln, § 31 Abs. 2 und 4 Europolstatut. Gegen die Entscheidungen von Europol kann dann bei der GKI Beschwerde eingelegt werden, Art. 32 Abs. 1 Europolstatut. In jedem Falle verbleibt den österreichischen Bürgern hinsichtlich der Daten, für die Österreich nach dem Europolstatut die daten-

schutzrechtliche Verantwortung trägt, der nationale Rechtsweg. Die Bürger können auch bei der DSK wegen Verweigerung einer Auskunft oder Richtigstellung bzw. Löschung von Daten Beschwerde einlegen, §§ 1 Abs. 5, 31 DSK 2000. Gegen Entscheidungen der DSK kann innerhalb von sechs Wochen nach Zustellung eines Bescheides eine Beschwerde an den VfGH gerichtet werden, Art. 144 B-VG. In derselben Frist ist auch eine Beschwerde an den VwGH möglich, § 40 Abs. 2 DSG 2000. Darüber hinaus besteht für die Bürger die Möglichkeit, beim VwGH Säumnisbeschwerde einzulegen, wenn die DSK nach mehr als sechs Monaten ihrer Entscheidungspflicht nicht nachgekommen ist, § 27 VwG.

9.2.1.4.5 Rechtsschutz gegen Maßnahmen von Europol

Werden Auskünfte verweigert oder Berichtigungen nicht vorgenommen, kann der Betroffene sich bei der gemeinsamen Kontrollinstanz beschweren, Art. 32 Abs. 1 Europolstatut. Die Entscheidung der GKI ist endgültig und kann u.U. auch auf eine Mitteilung an den Antragsteller hinauslaufen, dass eine Prüfung stattgefunden hat, ohne dass daraus entnommen werden kann, ob Daten gespeichert worden sind, Art. 32 Abs. 5 Europolstatut. Auch eine Verweigerung der Information ist möglich, Art. 32 Abs. 3 Europolstatut. Eine nachträgliche Benachrichtigung von Personen, deren personenbezogene Daten in Datenbanken oder Analysedateien verarbeitet worden sind, ist nicht vorgesehen. Stellt die GKI Verstöße gegen Bestimmungen des Statutes bei der Verwendung personenbezogener Daten fest, richtet sie eine Beschwerde an den Direktor; ist sie mit dessen Stellungnahme nicht einverstanden, so wendet sie sich an den Verwaltungsrat, Art. 34 Abs. 4 Europolstatut, der dann eine endgültige Entscheidung trifft.

Art. 52 Abs. 1 Europolstatut ermöglicht Ersatz für Schäden, die durch die Speicherung und Verarbeitung von fehlerhaften Daten bei Europol entstanden sind. Dabei kann der Geschädigte eine Schadenersatzklage gegen den Mitgliedsstaat anstrengen, in dem der Schadensfall eingetreten ist. Dabei soll er sich an die nach innerstaatlichem Recht zuständigen Gerichte wenden.

Weitergehende Rechtsmittel für von Maßnahmen des Europol Betroffene sind im Europolstatut nicht vorgesehen.

Nach Art. 47 Abs. 1 GRCh hat jede Person, deren durch die Gesetze der Union gewährte Rechte verletzt worden sind, Anspruch bei einem Gericht wirksamen Rechts-

behelf einzulegen zu können. Dabei bezieht sich das Recht auch darauf, dass die Sache von einem unabhängigen, unparteiischen und zuvor durch Gesetz errichteten Gericht in einem fairen Verfahren, öffentlich und innerhalb angemessener Frist behandelt wird, Art. 47 Abs. 2 GRCh. Art. 263 Abs. 4 AEUV ermöglicht die Individualklage von natürlichen Personen gegen Handlungen der Organe der EU beim Europäischen Gerichtshof, so dass Bürger, die sich durch Handlungen oder Entscheidungen von Europol verletzt fühlen, grundsätzlich die Möglichkeit hätten, eine gerichtliche Überprüfung der Maßnahmen von Europol zu erzwingen. Aufgrund einer Übergangsregelung in Art. 10 des Protokolls über Übergangsbestimmungen vom 13.12.2007 sind für eine Zeit von fünf Jahren bezüglich der Befugnisse der Organe bei Rechtsakten, die vor Inkrafttreten des Lissabon-Vertrages angenommen wurden, die Befugnisse der Kommission nach Art. 258 AEUV (Vertragsverletzungsverfahren) ausgeschlossen. In Bezug auf die Zuständigkeit des Europäischen Gerichtshofes für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen bleibt es für die Dauer der Übergangsperiode bei den vor Inkrafttreten des Lissabon-Vertrages bestehenden Regelungen nach Titel VI des Vertrages über die Europäische Union.[442] In Ziffer 21 der einführenden Gründe für das Europolstatut heißt es: *„Europol unterliegt der gerichtlichen Kontrolle nach Maßgabe des Artikel 35 des Vertrages über die Europäische Union.*“ In Art. 35 der bis zum 30. November 2009 geltenden Fassung des EU-Vertrages ist das Vorabentscheidungsverfahren geregelt. Individualklagen gegen Handlungen und Rechtsakte der EU-Organe sind nicht vorgesehen. Das bedeutet, dass der eingeschränkte Rechtsschutz in der ehemaligen dritten Säule für Zeit bis zum 01. Dezember 2014 fortbesteht. Allerdings gilt dies nur für Befugnisse der Organe aus bei Inkrafttreten des Lissabon-Vertrages bereits bestehenden Rechtsakten. Sollten neue Vorschriften auf der Grundlage von Art. 87 Abs. 2 AEUV im Konsensverfahren von Parlament und Rat für die Tätigkeit Europol erlassen werden, gelten die Übergangsregelungen insoweit nicht. Erschwert wird die Rechtsverfolgung auch dadurch, dass das Europolpersonal Immunitätsschutz genießt, Art. 51 Abs. 1 Europolstatut. Die Immunitätsregelung war von Anfang an umstritten.[443] Sie erschwert die Beweismöglichkeiten für Betroffene.

---

[442] Protokoll über Übergangsbestimmungen vom 13. Dezember 2007, ABl. C 306, S. 159.

[443] Wagner, „Halt Europol“ Probleme der europäischen Polizeikooperation für parlamentarische Kontrolle und Grundrechtsschutz, HSFK-Report 15/2004, S. 7/8.

Damit stellt sich die Frage, welche gerichtlichen Kontrollmaßnahmen noch bestehen.

9.2.1.4.6 Rechtschutz gegen Europol durch Klage beim EGMR?

Eine Klage unmittelbar gegen Europol als EU-Organ scheidet bis auf weiteres als unzulässig aus. Die EU ist (noch) nicht Vertragspartei der EMRK. Der Beitritt ist in Art. 6 Abs. 2 EUV vorgesehen. Dazu ist jedoch eine Änderung der EMRK erforderlich, der bisher nur souveräne europäische Staaten angehören. Die Anpassung ist inzwischen durch Art. 59 Abs. 2 EMRK in der Fassung des EMRK-Protokolls Nr. 14 (Art. 17) erfolgt. Außerdem ist noch ein Beitrittsabkommen zwischen der EU und dem Europarat auszuhandeln, das von den Mitgliedstaaten der Konvention zu ratifizieren ist und dem der Rat der EU und das Europäische Parlament zustimmen müssen. Das Verfahren ist im Einzelnen in Art. 218 Abs. 6 und 8 AEUV geregelt.

Es stellt sich daher die Frage, ob unter den gegebenen Umständen aufgrund von Maßnahmen und/oder Entscheidungen von Europol eine Individualklage nach Art. 34 EMRK gegen ein Mitgliedsland der EU möglich ist. Dabei kann eine Konfliktsituation in der Form entstehen, dass ein Mitgliedstaat, wenn er im Einklang mit EU-Recht handelt, gegen die EGMR verstößt und umgekehrt. In seinem Urteil im Falle Bosphorus Airways gegen Irland[444] im Jahre 2005 hat der EGMR entschieden, dass staatliches Handeln in Erfüllung von internationalen Verpflichtungen gerechtfertigt sein kann, wenn die internationale Organisation einen der EMRK äquivalenten Grundrechtsschutz aufweist. Mit „äquivalent“ meint der Gerichtshof nicht identische, sondern vergleichbare Regeln. Dies hat er für den Grundrechtsschutz in der EU grundsätzlich bejaht. Die Vermutung gilt jedoch nicht immer, sondern ist im Einzelfall widerlegbar. Eine solche Widerlegung der Vermutung ist u.a. auch in Bereichen möglich, in denen der EuGH keine oder nur eingeschränkte Rechtsprechung ausübt.[445] In jedem Falle ist aber ein direktes oder indirektes Handeln eines Mitgliedstaates erforderlich, um die Zuständigkeit des EGMR zu begründen. Nur ausnahmsweise kann bei Fehlen eines nationalen Hoheitsaktes die Verantwortlichkeit eines Mitgliedslandes nach Art. 1 EMRK begründet sein, wenn an eine im Vorfeld liegende Handlung oder Unterlassung bei der Übertragung der Zuständigkeiten an die internationale Or-

---

[444] EGMR Urteil vom 30.06.2005, Bosphoru Hava Yollari Türzim ve Ticaret Anonim Sirketi gg. Irland, Nr. 45036/98, Ziffer 155 ff., EuGRZ 2007, S. 662 ff..

[445] Baumann, Auf dem Wege zum doppelten EMRK-Schutzstandard?, EuGRZ 2009, S. 1 ff. (S. 3, Anm. 23).

ganisation angeknüpft werden kann, weil die Mitgliedstaaten im Rahmen der Übertragung von Kompetenzen an eine internationale Organisation sicherzustellen haben, dass deren Organisation und Verfahren mit der Menschenrechtskonvention in Einklang stehen.[446] In dem Verfahren Gasparini gegen Italien und Belgien[447], in dem es um strukturelle Mängel des Rechtsbehelfssystem innerhalb der NATO ging, hat der EGMR die Zulässigkeit der Klage bejaht, obwohl die angegriffene Entscheidung von Organen der Nato und nicht von den genannten Mitgliedstaaten getroffen worden sind. Die Beschwerde ist in dem genannten Fall gegen Italien gerichtet worden, weil der Beschwerdeführer die italienische Staatsangehörigkeit besaß und gegen Belgien, weil sich dort der Sitz der NATO befindet.

Bezogen auf die Situation bei Europol und die Tatsache, dass dort bis auf weiteres Einzelne sich nicht gegen Maßnahmen dieses EU-Organs gerichtlich wehren können, wäre die Klage eines Österreichers gegen Österreich und die Niederlande (Den Haag ist Sitz von Europol) beispielweise wegen unzulässiger Verwendung von personenbezogenen Daten oder unzureichender Auskunftserteilung nach Art. 34 EMRK grundsätzlich denkbar,[448] zumindest bis zum Ablauf der Übergangsperiode gemäß Art. 10 Abs. 1 des 8. Protokolls zum Lissabon-Vertrag im Jahre 2014. Voraussetzung wäre allerdings die Erschöpfung des Rechtsweges in Österreich gemäß Art. 35 Abs. 1 EMRK.

9.2.1.5 Zusammenfassende Stellungnahme zu Europol

In den vorstehenden Ausführungen sind die sehr weit gefassten Regelungen zum Datenschutz und der eingeschränkte Rechtsschutz im Verhältnis zu Europol kritisiert worden. Damit soll jedoch nicht der Eindruck erweckt werden, dass Aufgabe und auch der Nutzen der praktischen Tätigkeit von Europol an sich kritisch betrachtet wird. Unter Berücksichtigung der erheblichen Bedrohungen, die von der organisierten Kriminalität und dem internationalen Terrorismus ausgehen, erscheinen die Maßnahmen und damit geschaffenen Möglichkeiten von Europol nicht unangemessen. Im

---

[446] Baumann aaO., S. 4.

[447] Urteil des EGMR vom 12.05.2009, Gasparini gegen Italien und Belgien, Nr. 10750/03, . http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=850884&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649, letzte Abfrage 01.06.2012.

[448] Entsprechend auch: Kistner-Bahr, Die Entwicklungstendenzen Europols im europäischen Integrationsprozess, Diss. 2010, S. 159-165; Schenke, „Rechtsschutz gegen Europol“ in Wolter/Schenke/Hilger/Ruthig/Zöller (Hrsg.) Alternativentwurf Europol und europäischer Datenschutz, 2008, S. 367 ff. (383/384).

Interesse der erfolgreichen und rechtzeitigen Erkenntnisse zu geplanten Straftaten und daran beteiligten Personen erscheint es sachgerecht, auch zunächst nicht verdächtige Personen in die Untersuchungen einzubeziehen, wenn diese zu gefährlichen Gruppierungen in Beziehungen stehen und potentielle Gefährder sind. Dies setzt jedoch wirksame und fortlaufende und nicht nur stichprobenartige Kontrollen durch eine unabhängige Institution voraus. So hat der Datenschutzbeauftragte der Bundesrepublik Deutschland in seinem letzten Tätigkeitsbericht die Kontrolle von Europol im Hinblick auf deren gestiegenen Aufgabenumfang als nicht mehr zeitgemäß bezeichnet.[449] Zu beanstanden ist daher, dass Europol ein von rechtsstaatlichen Kontrollen weitgehend losgelöstes Eigenleben führt. Dass es auch anders geht, verdeutlicht das Datenschutzregime von Eurojust, das in Kapitel 7.2.3 beschrieben wird.

Der Umstand, dass nach § 10 Abs. 1 Eu-PolKG die österreichische nationale Kontaktstelle und die Verbindungsbeamten berechtigt sind, an Europol alle Daten zu übermitteln, die die Sicherheitspolizei selbst nach § 53 a Abs. 2 SPG für Analysezwecke nutzen darf, erscheint auf ersten Blick unbedenklich. Während im innerstaatlichen Bereich die erweiterte Gefahrenforschung im Sinne von § 21 Abs. 3 SPG der Kontrolle durch den Rechtsschutzbeauftragten unterliegt und mit der Möglichkeit der Beschwerde an die DSK und einer darauf folgenden Anrufung der VfGH und/oder des VwGH ein rechtsstaatlichen Anforderungen entsprechendes Verfahren gewährleistet ist, fehlen z.Zt. bei Europol vergleichbar wirksame Kontrollmechnismen. Es besteht auch die Gefahr, dass die österreichischen Polizeibehörden auf der Grundlage von § 10 Abs. 1 Eu-PolKG Daten an Europol übermitteln und dort auswerten lassen, für deren Verwendung sie im Inland den erwähnten Kontrollen unterworfen wären.

Aus diesen Gründen war es zu begrüßen, dass die Europäische Kommission u.a. auch eine Verbesserung des Datenschutzes im Bereich der polizeilichen und

---

[449] Bundesbeauftragter für den Datenschutz, Tätigkeitsbericht zum Datenschutz für die Jahre 2009 und 2010, S. 148 *„Vor dem Hintergrund des Bedeutungszuwachses von Europol stellt sich auch die Frage, ob die derzeitige Struktur der Datenschutzkontrolle, die durch eine Gemeinsame Kontrollinstanz aller 27 EU-Mitgliedstaaten wahrgenommen wird, noch zeitgemäß ist und den Anforderungen an eine effektive, effiziente und flexible Datenschutzaufsicht genügt.“* http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23_TB_09_10.pdf;jsessionid=E40C32A55DC355821F11E8D2304D8A97.1_cid134?__blob=publicationFile, letzte Abfrage 17.01.2012.

justiziellen Zusammenarbeit innerhalb der Union plante.[450] Sie begründete dies u.a. damit, dass der Rahmenbeschluss 2008/977/JI[451] nur für den grenzüberschreitenden Datenverkehr und nicht innerhalb der Mitgliedstaaten gelte, dass er zu viele Ausnahmen vom Zweckbindungsgrundsatz enthalte und im Übrigen u.a. auch für Europol, Eurojust, SIS und ZIS keine Anwendung finde, weil für diese Einrichtungen sektorspezifische Regelungen gelten. Die Kommission beabsichtigte, die Einbeziehung der polizeilichen und justiziellen Zusammenarbeit in die allgemeinen Datenschutzregelungen, die Schaffung unterschiedlicher Vorschriften für verschiedene Gruppen von Betroffenen (Zeugen, Verdächtigte usw.) im Bereich der Zusammenarbeit zwischen den Polizeibehörden und der justiziellen Zusammenarbeit in Strafsachen, die Anpassung der in einzelnen Rechtsakten enthaltenen sektorspezifischen EU-Vorschriften für die polizeiliche und justizielle Zusammenarbeit in Strafsachen zu prüfen. Die derzeit vorliegenden Entwürfe für eine Datenschutz-Grundverordnung und eine Richtlinie für den Datenaustausch bei der polizeilichen und justiziellen Zusammenarbeit sehen keine Änderungen für Europol vor. Möglicherweise werden die Regelungen zum Datenschutz im Europolstatut später dann an die neuen Vorschriften angepasst.

9.2.2 Das Schengener Informationssystem (SIS)

Das System wurde im Zuge des Wegfalls der Binnengrenzen in der EU entwickelt und geht ursprünglich auf einen Vertrag zwischen Deutschland, Frankreich, Belgien, die Niederlande und Luxemburg aus dem Jahre 1985 zurück.[452] Mittlerweile sind über 20 EU-Staaten dem Vertrag beigetreten und außerdem die Nicht-EU-Mitglieder Schweiz, Norwegen und Island. Im Jahre 1995 ist das Schengener Durchführungsübereinkommen (SDÜ) in Kraft getreten[453] Dieses Übereinkommen regelt in Kapitel

---

[450] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 04.11.2010, Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM(2010) 609 endgültig, S. 15-16, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf, letzte Abfrage 17.01.2012.

[451] 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 350 vom 30.12.2008, S. 60).

[452] Schengen-Besitzstand gemäß Artikel 1 Absatz 2 des Beschlusses 1999/435/EG des Rates vom 20. Mai 1999, ABl. L 239 vom 22.09.2000, S. 13 ff..

[453] Siehe vorstehende Quelle S. 19 ff.

IV auch die Handhabung des Informationssystems. Es ist ein dezentrales System und besteht aus einem nationalen Teil n-SIS und einer zentralen Unterstützungseinheit in Frankreich c-SIS, Art. 92 Abs. 3 SDÜ. Die Eingaben erfolgen im nationalen Teil und werden dann im zentralen Teil gesichert. Nach Art. 94 Abs. 2 SDÜ gibt es zwei Kategorien von Daten: Ausgeschriebene Personen sowie Sachen gemäß Art. 100 SDÜ und Fahrzeuge gemäß Art. 99 SDÜ. Nach Art. 2 Abs. 3 SDÜ können folgende personenbezogene Daten gespeichert werden:

a) Name und Vorname, gegebenenfalls Aliasname in einem neuen Datensatz;
b) besondere unveränderliche physische Merkmale;
c) erster Buchstabe des zweiten Vornamens;
d) Geburtsort und -datum;
e) Geschlecht;
f) Staatsangehörigkeit;
g) der personenbezogene Hinweis „bewaffnet“;
h) der personenbezogene Hinweis „gewalttätig“;
i) Ausschreibungsgrund;
j) zu ergreifende Maßnahme.

Ausgeschrieben werden können Personen zur Festnahme zwecks Auslieferung, Art. 95 Abs. 1 SDÜ, Vermisste und Personen, die im Interesse des eigenen Schutzes in Gewahrsam zu nehmen sind, Art. 97 SDÜ, Zeugen sowie Personen, die im Rahmen eines Strafverfahrens wegen Taten vor Gericht erscheinen müssen, derentwegen sie verfolgt werden oder Personen, denen ein Strafurteil oder die Ladung zum Antritt einer Freiheitsentziehung zugestellt werden muss, Art 98 Abs. 1 SDÜ. Bei schweren Straftaten im Sinne von Art. 99 Abs. 2 SDÜ ist eine verdeckte Registrierung möglich, Art. 99 Abs. 1 SDÜ.

Für die Eingaben ist die jeweilige nationale Stelle verantwortlich, eine Bearbeitung darf nur durch sie erfolgen, Art. 106 Abs. 1 SDÜ. Jedes Land benennt eine Stelle, die als Zentrale für den nationalen Teil des SIS zuständig ist, Art. 108 Abs. 1 SDÜ (in Österreich das BMI, § 20 Abs. 2 EU-PolKG).

Der Datenschutz für das SIS ist so aufgebaut, dass für den nationalen Teil, n-SIS, die jeweiligen nationalen Datenschutzvorschriften maßgeblich sind, für den zentralen Teil, c-SIS, die Bestimmungen des SDÜ sowie das Übereinkommen des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener

Daten, EuDSK, und die Empfehlung des Ministerkomitees des Europarates zur Regelung der Benutzung personenbezogener Daten durch die Polizei[454] , Art. 115 Abs. 1 SDÜ. Das Datenschutzniveau der beteiligten Nationalstaaten muss mindestens den Anforderungen des genannten Übereinkommens des Europarates und der Empfehlung von dessen Ministerkomitee entsprechen, Art. 117 Abs. 1 SDÜ. Sowohl die nationale Stelle als auch die Zentraleinheit in Frankreich werden durch unabhängige Kontrollinstanzen überwacht, Art. 114 Abs. 1 und 115 Abs.1 SDÜ. Dem Bundesminister für Inneres kommt bei der Führung des nationalen Schengener Informationssystems die Aufgabe des Betreibers gemäß § 50 DSG 2000 zu, § 33 Abs. 1 letzter Satz EU-PolKG. Im Gegensatz zur Zusammenarbeit mit Europol ist für das SIS im EU-PolKG die Datenschutzkommission nicht ausdrücklich als nationale Kontrollstelle benannt, siehe für Europol § 14 EU-PolKG. Für die DSK als nationale Kontrollstelle spricht aber der Umstand, dass im SIS für den nationalen Teil die nationalen Datenschutzvorschriften maßgeblich sind. Die Gemeinsame Kontrollinstanz für die Zentrale wird aus je zwei Vertretern der nationalen Kontrollinstanzen gebildet, Art. 115 Abs. 1 SDÜ.

Ungeachtet des umfangreichen Regelwerkes zum Datenschutz werden die praktischen Ergebnisse zum Teil kritisch beurteilt. Die nationalen Kontrollstellen und die gemeinsame Kontrollstelle haben bei ihren Untersuchungen erhebliche Defizite in Bezug auf den Datenschutz festgestellt. Außerdem wird bemängelt, dass in den Nationalstaaten sehr viele Behörden auf die Daten zugreifen können. Allein aus Deutschland erfolgen jährlich ca. 70 Mio. Zugriffe von 200.000 Terminals.[455] Obwohl die im SIS gespeicherten Daten gemäß Art. 102 Abs.1 SDÜ einer Zweckbindung unterliegen und nach Art. 102 Abs. 2 SDÜ grundsätzlich nicht in andere nationale Systeme übernommen werden dürfen, geschehe das häufig.[456] Nach §§ 101 a und 101 b SDÜ haben auch Europol und Eurojust Zugriff auf bestimmte Daten des SIS.

---

[454] Übereinkommen zum Schutz des der Menschen bei der Verarbeitung personenbezogener Daten, Übereinkommen 108 des Europates vom 28.01.1981, http://conventions.coe.int/treaty/ger/treaties/html/108.htm, letzte Abfrage 17.01.2012; Empfehlung des Ministerkommitees des Europarates Nr. R (87) 15 vom 17.09.1987, http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1987_15.pdf, letzte Abfrage 17.01.2012.

[455] Töpfer, Zum Datenschutz in der europäischen Polizeizusammenarbeit, http://www.rav.de/publikationen/infobriefe/infobrief-104-2010/im-gleichschritt-mit-der-sicherheit/, letzte Abfrage 17.01.2012.

[456] Töpfer aaO..

Zwischenergebnis zum Schengener Informationssystem

Wie schon in den Ausführungen zu Europol näher dargestellt bieten die auch für das SIS maßgeblichen Datenschutzstandards, die EuDSK und die Empfehlung des Ministerkomitees von 1987, nur einen eingeschränkten Datenschutz, der nach den erfolgten Prüfungen offensichtlich nicht einmal eingehalten wird.

9.2.3 Eurojust

Die von der organisierten Kriminalität und dem Terrorismus ausgehenden Gefahren, die schon zu einer verstärkten Zusammenarbeit auf polizeilichem Sektor bei der Erkennung und Abwehr von Straftaten durch Europol führten, waren auch der Hauptgrund für eine stärkere Zusammenarbeit bei der Ermittlung von Straftaten durch die Strafverfolgungsbehörden. Im Jahre 2002 wurde dafür die Organisation Eurojust gegründet.[457] Im Interesse einer besseren Effizienz wurde der Gründungsbeschluss 2008 geändert.[458] Die Stellung der nationalen Mitglieder bei Eurojust und die Kommunikation zwischen Eurojust und den zuständigen nationalen Stellen sollte verbessert werden (Erwägungsgründe Nr. 4-12). Der Rahmenbeschluss 2008/977/Ji des Rates vom 27.11.2008 über den Schutz der im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeiteten personenbezogenen Daten wurde für Eurojust für anwendbar erklärt, ohne dass damit die speziellen Vorschriften des Gründungsbeschlusses berührt werden sollten (Erwägungsgründe Nr. 13). Im Lissabon-Vertrag wird die Stellung von Eurojust in Art. 85 Abs. 1 AEUV primärrechtlich abgesichert. Nach Art. 86 Abs. 1 AEUV kann die bestehende koordinierende Aufgabenstellung von Eurojust im Wege eines besonderen Gesetzgebungsverfahrens durch Einsatz einer Europäischen Staatsanwaltschaft erweitert werden.

Eurojust besteht aus von den Mitgliedstaaten an den Sitz von Eurojust in Den Haag für mindestens vier Jahre entsandten Mitgliedern, die Staatsanwälte, Richter oder Polizeibeamte mit gleichwertigen Befugnissen sein müssen, Art. 2 und 9 Abs. 1 Eurojuststatut.[459] Aufgabe von Eurojust ist die Förderung und Verbesserung der Zu-

---

[457] Beschluss des Rates vom 28.02.2002 über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität, (2002/187/JI), ABl. 2002 L 63 , S. 1 ff..

[458] Beschluss 2009/426/JI des Rates vom 16. 12. 2008 zur Stärkung von Eurojust und Änderung des Beschlusses 2002/187/JI über die Errichtung von Eurojust und zur Verstärkung der Bekämpfung der schweren Kriminalität, ABl. 2009 L 138 S. 14 ff.

[459] Eurojuststatut bedeutet im Folgenden die konsolidierte Fassung des Beschlusses 2002/187/JI des Rates vom 28.02.2002 über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schwe-

sammenarbeit bei Ermittlungen und Strafverfolgungsmaßnahmen im Bereich der schweren Kriminalität und des organisierten Verbrechens, sofern die Maßnahmen regelmäßig (Ausnahme Art. 3 Abs. 3 Eurojuststatut) mindestens zwei Mitgliedstaaten betreffen, Art. 3 Eurojuststatut. Dabei erstreckt sich die Zuständigkeit auf alle Kriminalitätsformen und Straftaten, die in die Zuständigkeit von Europol fallen und Straftaten, die damit in Zusammenhang stehen, Art. 4 Eurojuststatut. Die Funktionen von Eurojust beschränken sich dabei auf die Koordinierung. Erforderliche Prozesshandlungen werden von den zuständigen Behörden in den Mitgliedstaaten durchgeführt, Art. 85 Abs. 2 AEUV. Die Mitgliedstaaten sind gehalten, Eurojust eine oder mehrere nationale Anlaufstellen zu benennen und bis 04.06.2011 ein nationales Eurojust-Koordinierungssystem zu errichten, Art. 12 Abs. 1 und 2 Eurojuststatut.

Eurojust ist berechtigt, im Rahmen seiner Zuständigkeit und Aufgaben personenbezogene Daten zu verarbeiten Art. 14 Abs. 1 Eurojuststatut, deren Art und Umfang in Art. 15 Europolstatut näher festgelegt ist. In Bezug auf den Schutz personenbezogener Daten wird auf das Datenschutzniveau der EuDSK vom 28. 01. 1987[460] verwiesen. Im Gegensatz zu Europol werden jedoch in Art. 14 Abs. 3 Eurojuststatut ausdrücklich die Grundsätze der Erforderlichkeit und Zweckbindung aufgeführt. Darüber hinaus hat das Kollegium von Eurojust (Gesamtheit der nationalen Mitglieder, Art. 10 Abs. 1 Geschäftsordnung) mit Zustimmung des Rates für Eurojust spezielle Regeln für die Verarbeitung und den Schutz personenbezogener Daten verabschiedet.[461] Es wird auf die Menschenrechte und Grundfreiheiten, insbesondere den Schutz der Privatsphäre Bezug genommen und dadurch eine Verbindung auch zur EMRK hergestellt, Art. 4 Geschäftsordnung. Dabei werden die Grundsätze der Rechtmäßigkeit, Erforderlichkeit und Zweckbindung betont, Art. 5 Geschäftsordnung. Die Dauer der Speicherung wird ausdrücklich an deren ursprünglichen Zweck geknüpft, Art. 6 Abs. 2 Geschäftsordnung. Die Voraussetzungen für eine rechtmäßige Verarbeitung wer-

---

ren Kriminalität in der durch Beschluss 2003/659/JI des Rates und den Beschluss 2009/426/JI des Rates vom 16.12.2008 zur Stärkung von Eurojust geänderten Fassung.

[460] Übereinkommen zum Schutz des der Menschen bei der Verarbeitung personenbezogener Daten, Übereinkommen 108 des Europates vom 28.01.1981, http://conventions.coe.int/treaty/ger/treaties/html/108.htm, letzte Abfrage 17.01.2012.

[461] Bestimmungen der Geschäftsordnung betreffend die Verarbeitung und den Schutz personenbezogener Daten bei Eurojust, angenommen durch das Kollegium von Eurojust am in der Sitzung vom 21.10.2004 und vom Rat am 24.02.2005 genehmigt, ABL. 2005, C 68 S. 1 ff, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:068:0001:0010:DE:PDF , letzte Abfrage 17.01.2012.

den in den Art. 13 bis 18 der Geschäftsordnung näher definiert. Ausdrücklich wird noch einmal betont, dass personenbezogene Daten, die von Eurojust im Rahmen von Ermittlungen und Strafverfolgungen verarbeitet werden, unter keinen Umständen für einen anderen Zweck verarbeitet werden dürfen, Art. 15 Geschäftsordnung. Eine Ausnahme gilt lediglich für nicht fallbezogene Daten. Diese dürfen in der Folge weiterverarbeitet werden, wenn dies mit dem ursprünglichen Zweck der Verarbeitung nicht unvereinbar ist, Art. 31 Abs. 1 Geschäftsordnung. Personenbezogene Daten, die im Interesse der Sicherheit und Verwaltung der System erfasst werden, dürfen mit Ausnahme der Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten für keinen anderen Zweck verwendet werden, Art. 31 Abs. 2 Geschäftsordnung. Beabsichtigte Verarbeitungen nicht fallbezogener Daten und damit verfolgte Zwecke sind dem Datenschutzbeauftragten vorab zu melden, Art. 34 Abs. 1 Geschäftsordnung. Übermittlungen an andere Organisationen werden protokolliert und die Empfänger müssen zusichern, dass die Daten nur zu dem Zweck verwendet werden, zu dem sie übermittelt worden sind, Art. 27 Abs. 2 Eurojuststatut.

Die Fristen für die Speicherung personenbezogener Daten sind begrenzt. Maßgeblich für eine Sperrung oder Löschung sind u.a. der Ablauf der Verjährungsfrist, rechtskräftige Entscheidung über einen Freispruch und drei Jahre nach Eintritt der Rechtskraft in dem Fall, zu dem ermittelt worden ist, Art. 21 Abs. 2 Eurojuststatut.

Wie bei Europol wird ein Datenschutzbeauftragter bestellt, der zum Personalstab von Eurojust gehört, dem Kollegium unterstellt ist und in Bezug auf seine Aufgaben unabhängig handelt, Art. 17 Abs. 1 Eurojuststatut.

Entsprechend der Organisation bei Europol wird eine gemeinsame Kontrollinstanz gebildet, die die Aufgabe hat, Eurojust in Bezug auf die Einhaltung der für ihre Tätigkeit vorgesehenen Regelungen zu überwachen, Art. 21 Abs. 1 Eurojuststatut. Aber anders als bei Europol, wo die GKI durch Abgesandte der Kontrollinstanzen der Mitgliedstaaten gebildet wird, besteht das Gremium aus drei ständigen und drei ad hoc-Richtern, Art. 21 Abs. 2 Eurojuststatut. Die ständigen und Ad hoc-Richter werden aus einem Pool gewählt, für den jedes Mitgliedsland einen Richter oder eine andere fachlich geeignete unabhängige Person benennt. Die ständigen Richter werden von der Plenarversammlung der Richter in geheimer Abstimmung für drei Jahre gewählt, Die Ad-hoc-Richter werden aus dem Kreis der Richter, die die Mitgliedstaaten für die Wahl der ständigen Richter benannt haben, zu den Beschwerden, die personenbe-

zogene Daten aus ihrem Entsendestaat betreffen, jeweils hinzugezogen, soweit sie nicht bereits ständiges Mitglied sind, Art. 23 Abs. 4 Eurojuststatut und Art. 3 Abs. 1 und 11 Abs. 1 Geschäfts- und Verfahrensordnung GKI. Die GKI tritt mindestens einmal halbjährlich zur Erfüllung ihrer ständigen Kontrollaufgaben zusammen und außerdem bei Eingang von Beschwerden spätestens binnen drei Monaten zu deren Behandlung, Art. 23 Abs. 1 Geschäfts-und Verfahrensordnung GKI.

Im Falle unbefugter oder unrichtiger Verarbeitung von Daten haftet Eurojust für den einer Person entstandenen Schaden nach dem Recht des Landes, in dem es seinen Sitz hat (Niederlande). Die dortigen Gerichte sind auch für entsprechende Klagen zuständig, Art. 24 Abs. 1 und 2 Eurojuststatut.

Jede Person hat Anspruch auf Auskunft über die sie betreffenden personenbezogenen Daten, Art. 19 Abs. 1 Eurojuststatut, sowie ggf. auf Berichtigung dieser Daten, Art. 19 Abs. 3 und 20 Abs. 1 Eurojuststatut. Der entsprechende Antrag kann direkt an Eurojust gerichtet oder bei der zuständigen Behörde eines Mitgliedslandes eingereicht werden, die ihn dann an Eurojust weiterleitet, Art. 21 Abs. 1 Geschäftsordnung Mitgliedslandes (In Österreich ist nationale Anlaufstelle für Eurojust das Bundesministerium der Justiz, Abt. IV 4: Internationale Strafsachen)[462]. Die zuständigen nationalen Mitglieder bei Eurojust prüfen die Anträge und schalten den Datenschutzbeauftragten ein, der der betroffenen Person die endgültige Entscheidung mitteilt, Art. 21 Abs. 3 bis 5 Geschäftsordnung. Gegen diese Entscheidung kann der Betroffene Beschwerde bei der GKI einlegen, Art. 19 Abs. 8 Eurojuststatut. Gegen die Entscheidung der GKI ist grundsätzlich eine Individualklage nach Art. 263 Abs. 4 AEUV beim EuGH möglich, allerdings erst nach Ablauf der Übergangsfrist von fünf Jahren nach Art. 10 Abs. 1 und 3 des Protokolls über die Übergangsbestimmungen.[463]

Zwischengebnis

Wenn man die Vorschriften über den Datenschutz bei Eurojust insgesamt betrachtet, wird eine Anlehnung an die Datenschutzrichtlinie 95/46/EG und die EMRK sowie die dazu ergangene Rechtsprechung deutlich. Die Erforderlichkeit und die Zweckbindung der erhobenen Daten haben deutlich mehr Gewicht als bei Europol. Die Spei-

---

[462] Geschäfts- und Personaleinteilung des Bundesministeriums für Justiz vom Dez. 2011, S. 47, http://www.justiz.gv.at/internet/file/8ab4ac8322985dd501229ce310cb0098.de.0/gesch%C3%A4ftseinteilung+zum+stichtag+1.dezember+2011.pdf , letzte Abfrage 17.01.2012.

[463] Protokoll über die Übergangsbestimmungen vom 13.12.2007, ABl. C 306 S. 159 ff..

cherfristen sind eng begrenzt und an dem ursprünglichen Zweck der Erhebung der Daten ausgerichtet. Anders als bei Europol ist die GKI mit Juristen oder gleich qualifizierten Personen besetzt und hat auch keine Beratungsaufgaben für die Organisation. Die Mitglieder der GKI werden nicht von der Leitung bestimmt, sondern von der Vollversammlung der Richterkandidaten, so dass ein hoher Grad an Unabhängigkeit erreicht wird. Aufgrund der Besetzung der GKI mit sechs qualifizierten Richtern, die über die Beschwerden Betroffener zu entscheiden haben, ist auch in der fünfjährigen Übergangsphase bis zur Möglichkeit der Anrufung der europäischen Gerichte ein Rechtsschutz gewährleistet, der einem förmlichen richterlichen Verfahren gleichkommt. Insgesamt kann man deshalb feststellen, dass die Regelungen bei Eurojust deutlich datenschutzfreundlicher sind als bei Europol.

9.2.4 Eurodac

Eurodac ist keine eigenständige Organisation, sondern besteht aus einem bei der Europäischen Kommission eingerichteten Datenverarbeitungssystem[464], in dem die Fingerabdrücke und sonstige Identitätsmerkmale von in der EU Asylsuchenden und illegal einreisenden EU-Ausländern gespeichert werden. Im Rahmen der Anwendung des Dubliner Abkommens[465] soll jeder Mitgliedstaat prüfen können, ob sich in ihrem Mitgliedsland illegal aufhaltende Ausländer schon anderweitig Asyl beantragt haben, Erwägungsgründe Nr. 3 der Eurodac-Verordnung.

Die Daten von Asylbewerbern werden zehn Jahre lang gespeichert, Art. 6 Abs. 1 Eurodac-Verordnung, es sei denn, sie erwerben vor Ablauf dieser Zeit die Staatsangehörigkeit in einem Mitgliedsland, Art. 7 Eurodac-Verordnung. Die Daten von illegal eingereisten EU-Ausländern werden für zwei Jahre gespeichert, Art. 10 Abs. 1 Eurodac-Verordnung. Fingerabdruckdaten, die von einem Mitgliedsland an die Eurodac-Datenbank übermittelt worden sind, werden vom System mit bereits von anderen Mitgliedsländern übermittelten Datensätzen verglichen, Art. 4 Abs. 3 Eurodac-Verordnung. Das Ergebnis, Treffer oder nicht, wird dem Einsendeland mitgeteilt. Die Mitgliedsländer haben nur Zugriff auf die von ihnen übermittelten Informa-

---

[464] Verordnung (EG) Nr. 2725/2000 des Rates vom 11. Dezember 2000 über die Einrichtung von „Eurodac“ für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens, ABl. 2000 Nr. L 316 S 1 ff. Erwägungsgründe Nr. 5.

[465] Übereinkommen über die Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat der Europäischen Gemeinschaften gestellten Asylantrags vom 15.06.1990, ABl. 1997 Nr. C 254 vom 19.8.1997, S. 1.

tionen und eventuelle Treffer-Daten, Art. 15 Abs. 1 Eurodac-Verordnung. Sie sind gehalten, Eurodac die nationalen Behörden zu benennen, die Zugriff auf Eurodac haben, Art. 15 Abs. 2 Eurodac-Verordnung.

Für den Datenschutz sind die Datenschutzrichtlinie 95/46/EG und die speziellen Vorschriften der Eurodac-Verordnung maßgeblich, Erwägungsgrund Nr. 17 zur Eurodac-Verordnung.

Die zuständigen nationalen Behörden sind verpflichtet, die betroffenen Ausländer, über

a) die Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters,

b) die Zwecke der Verarbeitung der Daten im Rahmen von Eurodac,

c) die Empfänger der Daten,

d) die Verpflichtung zur Fingerabdrucknahme bei Personen im Sinne des Artikels 4 oder Artikels 8,

e) die Auskunfts- und Berichtigungsrechte bezüglich sie betreffender Daten zu unterrichten, Art. 18 Abs. 1 Eurodac-Verordnung.

Die betroffenen EU-Ausländer haben Auskunfts- sowie Berichtigungs- und ggf. Löschungsansprüche entsprechend Art. 12 DS-RL, Art. 18 Abs. 2 und 3 Eurodac-Verordnung, die in jedem EU-Land geltend gemacht werden können. Stammen die Daten nicht aus dem EU-Land, in dem der Betreffende sich aufhält, so setzen sich die Behörden dieses Staates mit den Behörden des Staates in Verbindung, der die Daten ursprünglich in Eurodac eingegeben hat, Art. 18 Abs. 4 Eurodac-Verordnung. Dieses Mitgliedsland erteilt dem Betroffenen einen Bescheid, in dem auch mitgeteilt werden muss, welche Rechtsmittel gegen den Bescheid zur Verfügung stehen, wenn der Betroffene mit dem Inhalt des Bescheides nicht einverstanden ist, Art. 18 Abs. 6 Eurodac-Verordnung.

Die Verarbeitungsvorgänge in der Zentraleinheit von Eurodac werden protokolliert, Art. 16 Abs. 1 Eurodac-Verordnung. Für die Richtigkeit der an Eurodac übermittelten Daten sind die nationalen Behörden verantwortlich, die von den nationalen Kontrollstellen im Sinne von Art. 28 Abs. 1 DS-RL zu überwachen sind, Art. 19 Abs. 1 Eurodac-Verordnung.

Ursprünglich bestand auch eine gemeinsame Kontrollstelle, die sich aus höchstens zwei Vertretern der nationalen Kontrollstellen zusammensetzte, Art. 20 Abs. 1 Eurodac-Verordnung. Ihre Aufgabe war es, die Tätigkeit der Zentraleinheit daraufhin zu kontrollieren, ob durch die Verarbeitung oder Nutzung der bei der Zentraleinheit vorhandenen Daten die Rechte der betroffenen Personen verletzt werden. Darüber hinaus sollte sie die Rechtmäßigkeit der Übermittlung personenbezogener Daten an die Mitgliedstaaten durch die Zentraleinheit kontrollieren, Art. 20 Abs. 2 Eurodac-Verordnung. Seit Inkrafttreten der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr ist für diese Aufgaben der Europäische Datenschutzbeauftragte zuständig.[466]

Zwischenergebnis

Der Datenschutzstandard bei Eurodac entspricht dem in den jeweiligen Mitgliedstaaten, die die Eingaben auch übermittelt haben. Er orientiert sich an der der Datenschutzrichtlinie 95/46/EG und entspricht daher den zu stellenden Anforderungen. Für den Verantwortungsbereich von Eurodac als zentrale Stelle bei der Kommission, also der EU, ist die Verordnung (EG) Nr. 45/2001 vom 18.12.2000 maßgeblich. Auch insoweit erscheint ein ausreichendes Datenschutzniveau gewährleistet.

9.2.5 Das Visa-Informationssystem VIS

Mit dem Visa-Informationssystem wird einmal der Zweck verfolgt, die gemeinsame Visum-Politik in der EU zu verwirklichen, die Abwicklung der Erteilung von Visa zu erleichtern und Missbräuche zu verhindern, Nr. 5 der Erwägungsgründe und Art. 2 VIS-Verordnung.[467] Zum anderen dient es der Vorbeugung von Gefahren für die innere Sicherheit, die durch Zugriffsmöglichkeiten für nationale Polizeibehörden und

---

[466] Art. 41 der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. 2001 L 8 S. 1 ff..

[467] Verordnung (EG) Nr.767/2008 des Europäischen Parlaments und des Rates vom 09.07.2008 über das Visa-Informationssystem und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung), ABl. 2008 Nr. L 218 S. 60 ff..

Europol gewährleistet werden soll, Art. 3 Abs. 1 VIS-Verordnung. Das Verfahren des Zugriffs ist in einem besonderen Ratsbeschluss geregelt.[468]

Das VIS besteht aus einer zentralen Behörde der EU, die für den Betrieb des zentralen VIS und der nationalen Schnittstellen zuständig ist, Art. 26 VIS-Verordnung. Die Stelle und die entsprechende Technik befinden sich in Straßburg (Frankreich) und ein Backup-System in Sankt Johann im Pongau in Österreich, Art. 27 VIS-Verordnung. Das VIS ist über nationale Schnittstellen mit den nationalen Systemen der einzelnen Mitgliedsländer verbunden, Art. 28 Abs. 1 VIS-Verordnung. Jeder Mitgliedstaat ist gehalten, eine nationale Behörde zu benennen, die den Zugang anderer nationaler Stellen zum VIS-System zu gewährleisten hat, und verbindet diese Behörden mit der nationalen Schnittstelle des VIS, Art. 28 Abs. 2 VIS-Verordnung.

Bei Erhalt eines Antrags stellt die Visabehörde unverzüglich die erforderlichen personenbezogenen und andere Daten in das VIS ein, prüft, ob bereits früher Anträge gestellt wurden und verknüpft ggfs. die entsprechen Datensätze, Art. 8 Abs. 1-3 VIS-Verordnung. Dem Antragsteller wird dabei die für die Verarbeitung der Daten verantwortliche Behörde mitgeteilt, ferner der Zweck der Datenverarbeitung im Rahmen des VIS, die Kategorien der Empfänger von Daten und die Aufbewahrungsfrist für Daten, Art. 37 Abs. 1 VIS-Verordnung. Die datenschutzrechtliche Verantwortung für die Eingaben liegt bei den Mitgliedstaaten, die sie tätigen, Art. 29 Abs. 1 VIS-Verordnung. Die zentrale Behörde ist für den ordnungsgemäßen Betrieb des Systems verantwortlich und auch dafür, dass nur Bedienstete zum Zwecke der Erfüllung ihrer Aufgaben in der Zentrale Zugriff auf das System erhalten, Art. 29 Abs. 2 VIS-Verordnung.

Zugang zu den Daten haben ansonsten grundsätzlich nur die Bediensteten der Visabehörden und anderer Behörden in den Mitgliedstaaten, die nach Art. 15 bis 22 VIS-Verordnung Visadaten für die Erfüllung ihrer Aufgaben benötigen, Art. 6 Abs. 1 und 2 VIS-Verordnung. Die zugangsberechtigten nationalen Behörden sind der Kommission zu melden, Art. 6 Abs. 3 VIS-Verordnung. Zugriff haben auf Antrag auch nationale Polizeibehörden, wenn berechtigte Gründe vorliegen, dass die Abfrage von VIS-Daten erheblich zur Verhütung, Aufdeckung und Ermittlung von terroristischen und

---

[468] Beschluss 2008/633/JI des Rates vom 23.06.2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung von, Aufdeckung und Ermittlung von terroristischer und sonstiger schwerer Straftaten, ABl. 2008 Nr. L 218 S. 129 ff..

sonstiger schwerwiegender Straftaten beitragen wird. Ebenso hat Europol Zugriff auf VIS-Daten, wenn dies zur Wahrnehmung seiner Aufgaben erforderlich ist, Art. 3 Abs. 1 VIS-Verordnung.

Die Speicherfrist für die Visadaten beträgt grundsätzlich fünf Jahre ab Ausstellung eines Visums, Art. 23 Abs. 1 VIS-Verordnung. Die Zugriffe auf das System sind zu protokollieren, Art. 34 Abs. 1 VIS-Verordnung.

Die Rechte Betroffener auf Auskunft, Berichtigung und Löschung sind ähnlich wie bei Eurodac geregelt. Zuständig für diese Aufgaben sind die jeweiligen Behörden in den Mitgliedstaaten, Art. 38 VIS-Verordnung. Für den Fall, dass in einem Mitgliedstaat, Auskünfte nicht zur Zufriedenheit Betroffener oder Berichtigungen und Löschungen nicht vorgenommen werden, so können diese den in dem jeweiligen Mitgliedsland vorgesehenen Beschwerde- und Rechtsweg beschreiten, Art. 38 Abs. 6 VIS-Verordnung, also in Österreich Beschwerde bei der DSK gemäß § 31 Abs. 1 und 2 DSG 2000 und ggf. anschließend Beschwerde an den VwGH gemäß § 40 Abs. 2 DSG 2000.

Die nationalen Kontrollstellen im Sinne von Art. 28 der DS-RL, also in Österreich die DSK, sind gehalten, die Rechtmäßigkeit der Datenverarbeitung durch den Mitgliedstaat einschließlich der Übermittlung an das VIS und vom VIS zu überwachen, Art. 41 Abs. 1 VIS-Verordnung. Die Tätigkeit der zentralen Verwaltungsbehörde der VIS wird durch den Europäischen Datenschutzbeauftragten überwacht, Art. 42 Abs. 1 VIS-Verordnung.

Zwischenergebnis

Die VISA-Verordnung stellt sicher, dass die Verwendung von personenbezogenen Daten in den Nationalstaaten bei der Erteilung von Visa auf der Grundlage der DS-RL und in der Zentrale in Straßburg auf der Grundlage internen Datenschutzregelung der EU, der Verordnung (EG) Nr. 45/2001, erfolgt. Damit wird ein hohes Datenschutzniveau gewährleistet. Soweit Europol Zugriffsrechte in Anspruch nimmt, gilt allerdings nur der dort vorgesehene eingeschränkte Datenschutzstandard der EuDSK und der Empfehlung des Ministerkomitees des Europarates aus dem Jahre 1987.[469]

---

[469] Übereinkommen zum Schutz des der Menschen bei der Verarbeitung personenbezogener Daten, Übereinkommen 108 des Europates vom 28.01.1981,

9.2.6 Das Zollinformationssystem ZIS

Die Errichtung des Zollinformationssystems geht auf ein Übereinkommen aus dem Jahre 1995 zurück.[470] Es wurde inzwischen durch einen Ratsbeschluss vom 30.11.2009 (ZIS-Beschluss)[471] ersetzt, der am 27.05.2011 in Kraft getreten ist, Art. 35 des Beschlusses. Zweck des Systems ist die Verbesserung der Effizienz und der Kooperation der Zollverwaltungen der Mitgliedstaaten bei der Verhinderung, Ermittlung und Verfolgung schwerer Zuwiderhandlungen gegen Rechtsvorschriften der Mitgliedstaaten, Art. 1 Abs. 2 ZIS-Beschluss. Das System wird von der Kommission betrieben und besteht aus einer zentralen Datenbank, auf die die Behörden der Mitgliedstaaten via Terminals zugreifen können, Art. 3 ZIS-Beschluss. Von den Mitgliedstaaten werden im Wesentlichen Daten zu Waren, Transportmitteln, Unternehmen und Personen eingegeben, Art. 3 Abs. 1 ZIS-Beschluss. Die Kategorien der für die Speicherung zulässigen personenbezogenen Daten sind genau aufgelistet. Art. 4 Abs. 2 ZIS-Beschluss. Sensible Daten dürfen nicht gespeichert werden. Art. 4 Abs. 5 ZIS-Beschluss. Die Daten dürfen nur zum Zweck der Feststellung und Unterrichtung, der verdeckten Registrierung und der strategischen sowie operativen Analyse in das ZIS eigegeben werden, personenbezogene Daten nur dann, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die betreffende Person eine schwere Zuwiderhandlung begangen hat, begeht oder begehen wird, Art. 5 Abs. 2 ZIS-Beschluss. Neben den nach Art. 3 ZIS-Beschluss eingegebenen Daten umfasst das ZIS auch noch einen besonderen Datenbestand als „Aktennachweissystem für Zollzwecke“. Zweck dieses Nachweissystems ist es, den zuständigen Behörden der Mitgliedstaaten sowie Europol und Eurojust zu ermöglichen, herauszufinden, welche Behörden anderer Mitgliedstaaten mit Ermittlungen gegen dieselben Personen oder Unternehmen befasst sind. Das Aktennachweissystem findet nur Anwendung im Falle von Zuwiderhandlungen, die mit mehr als 12 Monaten Freiheitsentzug oder mindestens 15.000,- € Geldstrafe bedroht sind.

---

http://conventions.coe.int/treaty/ger/treaties/html/108.htm, letzte Abfrage 17.01.2012;
Empfehlung des Ministerkommitees des Europarates Nr. R (87) 15 vom 17.09.1987, http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1987_15.pdf, letzte Abfrage 17.01.2012

[470] Übereinkommen aufgrund von Art. K 3 des Vertrages über die Europäische Union über den Einsatz der Informationstechnologie im Zollbereich, ABl. C 316 vom 27.11.1995, S. 34 ff..

[471] Beschluss 2009/917/JI des Rates vom 30.11.2009 über den Einsatz der Informationstechnologie im Zollbereich, ABl. 2009 Nr. 323 vom 10.12.2009 S.20 ff..

Zugang zu dem System haben nur die von den einzelnen Mitgliedstaaten benannten Behörden. Eine entsprechende Liste haben sie den anderen Mitgliedstaaten und dem Ausschuss der Vertreter der Mitgliedstaaten zu übermitteln, Art. 7 Abs. 1 und 2 ZIS-Beschluss. Zugriff haben seit 27.05.2011 auch Europol und Eurojust. Europol darf das System im Rahmen seines Mandates zur Erfüllung seiner Aufgaben nutzen, die Informationen allerdings nur mit Zustimmung des Mitgliedslandes, das die Daten eingeben hat. Dasselbe gilt für die Übermittlung der Daten an Stellen in Drittländern, Art. 11 Abs. 1 und 3 ZIS-Beschluss. Bei Eurojust haben die nationalen Mitglieder von Eurojust, ihre Stellvertreter, die sie unterstützenden Personen und eigens ermächtigte Bedienstete im Rahmen ihrer Aufgaben Zugriffsrechte, Art. 12 Abs. 1 ZIS-Beschluss. Mit Zustimmung des eingebenden Mitgliedslandes dürfen Europol und Eurojust personenbezogene Daten aus dem ZIS auch für andere von Art. 1 Abs. 2 ZIS-Beschluss abweichende Zwecke verwenden, Art. 8 Abs. 1 ZIS-Beschluss. Die anderweitige Verwendung erfolgt nach Maßgabe von Art. 3 Abs. 2 des Rahmenbeschlusses 2008/977/JI vom 27.11.2008.[472]

Die Eingabe der Daten erfolgt auf der Grundlage der Vorschriften des jeweiligen Mitgliedslandes, Art. 9 ZIS-Beschluss. Jedes Mitgliedsland bestimmt eine für das System zuständige Zollbehörde (für Österreich das Bundesministerium für Finanzen), die für den ordnungsgemäßen Betrieb und die Einhaltung der Bestimmungen des ZIS-Beschlusses verantwortlich ist, Art. 10 Abs. 1 und 2 ZIS-Beschluss. Damit sind die Mitgliedsländer für die Qualität der von ihnen eingegeben Daten verantwortlich.

Eine Verwendung der Daten erfolgt nur so lange, wie es zur Erfüllung des angestrebten Zweckes erforderlich ist. Die weitere Notwendigkeit der Speicherung wird jährlich einmal von den zuständigen Behörden des eingebenden Staates geprüft, Art. 14 Abs. 1 ZIS-Beschluss. Die maximale Dauer der Speicherung richtet sich nach den Vorschriften des eingebenden Mitgliedstaates. Daten über laufende Ermittlungen werden höchstens drei Jahre gespeichert, wenn keine Zuwiderhandlung festgestellt worden ist, maximal sechs, wenn zwar eine Zuwiderhandlung vorliegt, aber eine Verurteilung nicht erfolgt ist, höchstens zehn im Falle einer Verurteilung, Art. 19 Abs. 1 ZIS-Beschluss.

---

[472] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. V L 350/60 vom 30.12.2008.

Für den Datenschutz im ZIS-System ist der Rahmenbeschluss 2008/977/JI maßgeblich, soweit der ZIS-Beschluss keine speziellen Regelungen enthält, Art. 20 ZIS-Beschluss. Dieser Rahmenbeschluss wurde erlassen, weil die Datenschutzrichtlinie 95/46/EG im Bereich der polizeilichen und justiziellen Zusammenarbeit in der EU nicht gilt und um einerseits in diesem Bereich in der EU den Datenaustausch zu erleichtern, aber andererseits auch die Grundrechte betroffener Personen in vollem Umfange zu gewährleisten, Ziffer 5 der Erwägungsgründe. Der Beschluss kam erst nach längeren Diskussionen zustande und stellt einen Kompromiss dar, der unter Gesichtspunkten des Datenschutzes die Anforderungen an Erforderlichkeit, Zweckbindung und Verhältnismäßigkeit nicht ausreichend erfüllt. Diese Grundsätze werden in der Regelung zwar angesprochen, aber in einer Form, die Interpretationsspielräume eröffnet und damit nicht ausreichend zur Sicherung der Grundrechte beiträgt. Zwar wird festgelegt, dass die Verarbeitung der Daten rechtmäßig sein und den Zwecken entsprechen muss, für die sie erhoben werden, dafür erheblich sein und nicht darüber hinausgehen dürfen, Art. 3 Abs. 1 Rahmenbeschluss. Allerdings ist die Weiterverarbeitung zu einem anderen Zweck zulässig, wenn diese mit den ursprünglichen Zwecken nicht unvereinbar ist und die Verarbeitung zu einem anderen Zweck notwendig und verhältnismäßig ist. Da die Beurteilung dieser Umstände dem Verwender der Daten obliegt und eine Kontrolle nicht erfolgt, wird der anderweitigen Verwendung von Daten hier ein weites Feld eingeräumt. Dies gilt z.B. auch für die Nutzung von ZIS-Daten durch Europol, Art. 8 Abs. 1 ZIS-Beschluss. Auch bei der Verwendung von personenbezogenen Daten, die von einem Mitgliedsland bereitgestellt wurden aber anderweitig genutzt werden, liegt eine Zweckänderung vor. Allerdings darf die anderweitige Verarbeitung nur zum Zwecke der Verfolgung von Straftaten und Abwendung von Gefahren oder mit Zustimmung des übermittelnden Mitgliedstaates erfolgen, Art. 11 Rahmenbeschluss. Auch eine Weiterleitung an Drittstaaten oder internationale Einrichtungen ist möglich, allerdings nur, soweit dies zur Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten erforderlich ist, der betreffende Mitgliedsstaat zugestimmt hat und der betreffende Drittstaat oder die internationale Einrichtung ein angemessenes Schutzniveau für die beabsichtigte Datenverarbeitung gewährleistet, Art. 13 Abs. 1 Rahmenbeschluss. Beurteilungskriterien dazu enthält Art. 13 Abs. 4 Rahmenbeschluss. Auch an private Organisationen ist eine Übermittlung personenbezogener Daten aus dem ZIS grundsätzlich möglich,

wenn die übermittelnde Behörde zugestimmt hat, keine überwiegenden schutzwürdigen Interessen des Betroffenen entgegenstehen und die Weiterleitung für die zuständige Behörde unerlässlich ist für die Erfüllung ihrer rechtmäßigen Aufgaben zur Verhütung, Ermittlung und Verfolgung von Straftaten oder Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Dritter, Art. 14 Abs. Rahmenbeschluss. Darüber hinaus enthält das ZIS spezielle Regelungen. Von anderen Mitgliedstaaten eingegebene Daten dürfen grundsätzlich nicht in nationale Dateien übernommen werden, ausgenommen für so genannte Risikomanagementsysteme zur Steuerung von Zollkontrollen durch die nationalen Behörden und für operative Analysen zur Koordinierung von Maßnahmen, Art. 21 Abs. 2 ZIS-Beschluss. In Dateisysteme von Europol dürfen Daten aus dem ZIS aber nicht übernommen werden; das Zugangsrecht von Europol beschränkt sich auf die Abfrage, Art. 11 Abs. 5 ZIS-Beschluss.

Zu den Rechten der betroffenen Personen ist zu sagen, dass die Behörden der Mitgliedstaaten in Einklang mit innerstaatlichen Vorschriften verpflichtet sind, die betroffenen Personen über die Verarbeitung personenbezogener Daten zu unterrichten, Art. Art. 16 Abs. 1 Rahmenbeschluss. Betroffene Personen haben darüber hinaus auch einen Anspruch auf Auskunft, ob und welche Daten an wen bereitgestellt wurden, in jedem Falle auf eine Mitteilung der nationalen Kontrollstelle, dass alle Prüfungen durchgeführt wurden, Art. 22 ZIS-Beschluss, Art. 17 Abs. 1 Rahmenbeschluss. Das Auskunftsrecht kann allerdings nach den in Art. 22 ZIS-Beschluss und Art. 17 Abs. 2 Rahmenbeschluss aufgeführten Kriterien nach innerstaatlichen Vorschriften eingeschränkt werden, wie dies im Falle von Österreich durch § 26 Abs. 2 DSG 2000 geschehen ist. Auch die Rechte auf Berichtigung und Löschung richten sich nach innerstaatlichem Recht, Art. 18 Rahmenbeschluss und Art. 23 ZIS-Beschluss. Maßgeblich ist hier § 27 DSG 2000. Weiter haben Betroffene, die mit der Entscheidung der zuständigen österreichischen Behörde zum Auskunfts-, Berichtigungs- oder Löschungsverlangen nicht einverstanden sind, die Möglichkeit der Beschwerde bei der DSK, § 31 Abs. DSG 2000. Gegen den Entscheid der DSK steht ihnen der Rechtsweg offen.

Die ordnungsgemäße Anwendung der Bestimmungen des ZIS-Beschlusses und des Rahmenbeschlusses wird durch eine gemeinsame Aufsichtsbehörde überwacht, die

aus je zwei Vertretern der nationalen unabhängigen Aufsichtsbehörden (im Falle Österreichs die DSK) gebildet wird, Art. 25 Abs. 1 und 2 ZIS-Beschluss. Der Europäische Datenschutzbeauftragte überwacht die Tätigkeiten der Kommission in Bezug auf den Betrieb des ZIS, Art. 26 ZIS-Beschluss.

Zwischenergebnis

Der Wegfall der Grenzkontrollen in den meisten EU-Staaten schränkt die Möglichkeiten für die nationalen Zollbehörden ein, Verstöße gegen innerstaatliche Zollbestimmungen zu entdecken. Der Informationsaustausch über ein Zollinformationssystem erscheint daher sinnvoll und erforderlich.

Ähnlich wie bei Europol können nationale Analytiker personenbezogene Daten aus dem ZIS, die von Behörden aus anderen Mitgliedsländern eingegeben worden sind, für Risikomanagementsysteme und operative Analysen verarbeiten, Art. 21 Abs. 2 und 3 ZIS-Beschluss, so dass insoweit sicher eine Zweckgebundenheit nicht immer gegeben ist. Von dieser Art der Verarbeitung ihrer Daten erfahren Betroffene nichts, so dass sie sich gegen die Verwendung ihrer Daten auch nicht zur Wehr setzen können. Für strategische Analysen dürfen nur anonymisierte Daten verwendet werden, Art. 2 Abs. 5 ZIS-Beschluss.

Zwar sind die innerstaatlichen Behörden grundsätzlich gehalten, Betroffene über die Verwendung ihrer Daten zu unterrichten, Art. 16 Abs. 1 Rahmenbeschluss. Dies betrifft jedoch nur die Daten, die die betreffende Behörde selbst verwendet und nicht den in § 21 Abs. 2 und 3 geregelten Zugriff von Behörden anderer Mitgliedstaaten.

Zur Verwendung von personenbezogenen Daten aus dem ZIS durch Europol gelten die Ausführungen in Kapitel 7.2.1 zur mangelnden unabhängigen Kontrolle und des eingeschränkten Rechtsschutzes bei Europol.

9.2.7 Multilateraler Datenaustausch zwischen nationalen Polizeibehörden

Neben den beschriebenen zentralen Einrichtungen auf EU-Ebene (SIS, VIS, ZIS Europol, Eurodoc, Eurojust) bestehen Regelungen zum dezentralen Austausch von personenbezogenen zwischen den Mitgliedstaaten der EU.

9.2.7.1 Schwedische Initiative

Ausgelöst durch die Terroranschläge in Madrid im Jahre 2004 beschloss der Rat der EU aufgrund einer Initiative des Königreichs Schweden am 18.12.2006 ein Verfahren zum vereinfachten Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der EU (Schwedenbeschluss).[473] Ziel war die Festlegung von Regeln, nach denen die Strafverfolgungsbehörden der Mitgliedstaaten wirksam und rasch bestehende Informationen und Erkenntnisse zum Zwecke der Durchführung strafrechtlicher Ermittlungen oder polizeilicher Erkenntnisgewinnungsverfahren austauschen können, Art. 1 Abs.1 Schwedenbeschluss. Es kann um Informationen und Erkenntnisse zum Zwecke der Aufdeckung, Verhütung oder Aufklärung einer Straftat ersucht werden, wenn Gründe für die Annahme vorliegen, dass entsprechende sachdienliche Informationen und Erkenntnisse in einem anderen Mitgliedstaat vorliegen, Art. 5 Abs. 1 Schwedenbeschluss. Als Straftat im Sinne des Beschlusses gelten nur solche, die in Art. 2 Abs. 2 des Rahmenbeschlusses über den Europäischen Haftbefehl vom 13.06.2002[474] aufgelistet und mit einer Höchststrafe von mindestens drei Jahren bedroht sind. Der Informationsaustausch erfolgt in der Regel auf der Grundlage von Formularen, die in Anlage B (Ersuchen) und A (Antwort) abgebildet sind. Die Ersuchen sind an die jeweils zuständige Strafverfolgungsbehörde eines Mitgliedslandes zu richten. Entsprechende Aufstellungen der Mitgliedstaaten sind beim Generalsekretariat des Rates zu hinterlegen, Art. 2 Buchst. a Schwedenbeschluss. In dringenden Fällen sollen die Informationen binnen acht Stunden, in nicht dringenden Fällen binnen einer Woche und ansonsten binnen 14 Tagen übermittelt werden, Art. 4 Schwedenbeschluss. Die zuständigen Strafverfolgungsbehörden der Mitgliedstaaten sind in bestimmten Fällen berechtigt, Informationen zurückzuhalten, u.a. wenn wesentliche Sicherheitsinteressen ihres Landes berührt werden, Erfolge in laufenden Ermittlungsverfahren oder die Sicherstellung von Personen gefährdet werden würden oder eindeutig für die Zwecke, für die sie nachgesucht wurden, ungeeignet sind, Art. 10 Abs. 1 Schwedenbeschluss. Zuständige Strafverfolgungsbehörden können auch unaufgefordert von sich aus zuständigen Strafverfolgungsbehörden in

---

[473] Rahmenbeschluss 2006/966/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. 2006 L386, S. 89 ff..

[474] Rahmenbeschluss des Rates (2002/584/JI) vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten, ABl. L 190 vom 18.07.2002, S. 1 ff..

anderen Mitgliedsländern Informationen und Erkenntnisse zur Verfügung stellen, in denen Gründe für die Annahme bestehen, dass diese zur Verhütung oder Aufklärung von Straftaten im Sinne des Beschlusses beitragen könnten, Art. 7 Abs. 1 Schwedenbeschluss.

Für den Datenschutz hinsichtlich der übermittelten Informationen gelten die nationalen Bestimmungen des empfangenden Mitgliedslandes sowie der EuDSK einschließlich des Zusatzprotokolls 181.[475] Außerdem sollten die Grundsätze der Empfehlung R (87) 15 des Ministerkomitees des Europarates über die Nutzung personenbezogener Daten im Polizeibereich beachtet werden,[476] Art. 8 Abs. 2 Schwedenbeschluss. Mit der Bezugnahme auf die EuDSK ist ein recht niederes Datenschutzniveau angesprochen. Auf die entsprechenden Ausführungen im Kapitel 9.2.1.4.2 über Europol wird verwiesen. Aufgrund der getroffenen Regelungen kann auch der Fall eintreten, das übermittelte personenbezogene Daten in den Empfängerländern einem geringerem Datenschutz unterliegen als in den Ländern, aus denen sie übermittelt worden sind, und die Betroffenen dadurch entgegen den nationalen Vorschriften in ihrem Land benachteiligt werden. In den speziellen Bestimmungen des Schwedenbeschlusses ist die Zweckbindung aber deutlich schärfer formuliert als in Art. 5 Buchst. b und c der EuDSK. Während die EuDSK eine Verarbeitung auch für andere Zwecke erlaubt, sofern diese mit den dem ursprünglichen vereinbar ist, dürfen nach Art. 8 Abs. 3 Schwedenbeschluss die übermittelten Daten nur für die Zwecke verwandt werden, für die sie nach dem Rahmenbeschluss übermittelt wurden oder zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit. Eine Verwendung für andere Zwecke ist nur mit Einwilligung des übermittelnden Mitgliedstaates zulässig, die erteilt werden kann, wenn das nationale Recht dies gestattet, Art. 8 Abs. 3 Schwedenbeschluss. Die übermittelnde nationale Strafverfolgungsbehörde ist auch berechtigt, nach Maßgabe des nationalen Rechts Bedingungen für die Verwen-

---

[475] Übereinkommen zum Schutz des der Menschen bei der Verarbeitung personenbezogener Daten, Übereinkommen 108 des Europarates vom 28.01.1981, http://conventions.coe.int/treaty/ger/treaties/html/108.htm, letzte Abfrage 17.01.2012; Zusatzprotokoll zum Europäischen Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr, http://conventions.coe.int/treaty/ger/treaties/html/181.htm, letzte Abfrage 17.01.2012.

[476] Empfehlung des Ministerkommitees Nr. R (87) 15 vom 17.09.1987, http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1987_15.pdf, letzte Abfrage 17.01.2012.

dung der übermittelten Daten festzulegen. Die empfangende Behörde ist grundsätzlich an diese Bedingungen gebunden.
Soweit Informationen und Erkenntnisse übermittelt werden, die Straftaten betreffen, welche in den Zuständigkeitsbereich von Europol oder Eurojust fallen, so sind diese Einrichtungen gleichfalls zu informieren, Art. 6 Abs. 2 Schwedenbeschluss. Dort gelten dann die für diese Organisationen bestehenden Datenschutzbestimmungen.

Zwischenergebnis

Die Qualität des Datenschutzes im Rahmen der Schwedischen Initiative hängt letztendlich davon, ob und in welchem Umfange die nationalen Aufsichtsbehörden (unabhängige Datenschutzbehörden) in der Lage sind, die nationalen zuständigen Strafverfolgungsbehörden in Bezug auf die Beachtung der nationalen Datenschutzvorschriften und des Schwedenbeschlusses zu überprüfen. Wenn Kontrollen nicht durchgeführt werden oder aus rechtlichen Gründen nicht möglich sind, bleibt die Beachtung der Datenschutzbestimmungen dem Belieben der beteiligten Behörden überlassen.

9.2.7.2 Vertrag von Prüm und Ratsbeschluss vom 23. Juni 2008

Im Jahre 2005 schlossen mehrere Mitgliedstaaten, darunter auch die Republik Österreich, einen Vertrag, mit dem die Zusammenarbeit bei der Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration bekämpft werden sollte. Mit dem Beschluss 2008/615/JI des Rates vom 23.06.2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (Prüm-Beschluss)[477], wurde der Vertrag in ein EU-Instrument umgewandelt. Der Vertrag enthält im Einzelnen die Bestimmungen, auf deren Grundlage die Mitgliedstaaten einander Zugriffsrechte auf DNA-Analysedateien, daktyloskopische Identifizierungssysteme und Fahrzeugregister gewähren. Die Zugriffe erfolgen zunächst nach dem Treffer/kein Treffer-System. In einem zweiten Schritt kann dann der abfragende Staat den anderen mitgliedstaat bitten, die zu einem Treffer gehörenden personenbezogenen Daten zu

[477] Beschluss 2008/615/JI des Rates vom 23.06.2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, ABl. 2008 L210, S. 1 ff..

nennen und ggf. weitere Informationen zu geben, Erwägungsgrund Nr. 10 Prüm-Beschluss. Für die Abfragen benennen die einzelnen Staaten nationale Kontaktstellen, Art. 6 Abs. 1, Art. 11 Abs. 1 und Art. 12 Abs. 2 Prüm-Beschluss. Außerdem ist vorgesehen, dass die Mitgliedstaaten einander im Falle von grenzüberschreitenden Großveranstaltungen zur Verhinderung von Straftaten und Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung personenbezogene Daten übermitteln, Art. 13 Abs. 1 Prüm-Beschluss. Entsprechendes gilt für die Verhinderung terroristischer Straftaten, Art. 16 Abs. 1 Prüm-Beschluss. In beiden Fällen läuft der Informationsaustausch gleichfalls über nationale Kontaktstellen, Art. 15 und Art. 16 Abs. 3. Nach dem Prüm-Beschluss haben die Mitgliedstaaten anders als nach der schwedischen Initiative selbst Zugriff auf personenbezogene Daten in anderen Mitgliedstaaten, allerdings nicht direkt, sondern mittelbar über das zweistufige Treffer/keinTreffer-Verfahren. Die polizeiliche justizielle Zusammenarbeit in Strafsachen folgt damit dem im Haager Programm festgelegten Grundsatz der allgemeinen Verfügbarkeit von Informationen (principle of availability), Erwägungsgrund 5 im Rahmenbeschluss vom 27.11.2008[478]. Dies ist mit dem Hinweis kritisiert worden, dass dadurch traditionelle Verfahren des Datenaustauschs verlassen werden. [479]Diese sind jeweils dadurch gekennzeichnet, dass vertraglich zuvor festgelegt worden ist, welche Daten unter welchen Voraussetzungen übermittelt werden. Nach dem Prinzip der allgemeinen Verfügbarkeit können grundsätzlich alle Daten übermittelt werden.

Für das Niveau des Datenschutzes ist auch hier die EuDSK nebst Zusatzprotokoll 181 und die Empfehlung des Ministerkomitees des Europarates Nr. R (87) 15 maßgeblich, Art. 25 Abs. 1 Prüm-Beschluss, was bedeutet, dass Datenschutzgesichtspunkte für die Übermittlung nicht stark ins Gewicht fallen, Art 12 Ziffer 2 EuDSK. Allerdings gilt für die Zusammenarbeit auf der Grundlage der der Schwedischen Initiative und des Prüm-Beschlusses ergänzend der bereits erwähnte 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. In dem Beschlusss wird in der Literatur zum Teil keine wesentliche

---

[478] 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. 2008 L 350, S. 60 ff.

[479] Weichert, Wo liegt Prüm? Der polizeiliche Datenaustausch in der EU bekommt eine neue Dimension, http://www.datenschutzzentrum.de/polizei/060329-pruem.htm, S. 2; letzte Abfrage 17.01.2012

Verbesserung des Datenschutzes gesehen, weil er sich im Wesentlichen auf die Darstellung der Prinzipien des Datenschutzes beschränke und durch die Verwendung von interpretationsfähigen allgemeinen Rechtsbegriffen den Polizeibehörden weiten Ermessensspielraum einräume.[480] Dieser Kritik lag allerdings nicht die endgültige Fassung des Beschlusses zugrunde.

Gemäß Art. 3 Abs. 1 Rahmenbeschluss dürfen personenbezogene Daten grundsätzlich nur für die Zwecke verarbeitet werden, zu denen sie erhoben worden sind. Eine Weiterverarbeitung anderen Zwecken ist allerdings nach Art. 3 Abs. 2 Rahmenbeschluss zulässig, wenn diese Zwecke mit den ursprünglichen nicht unvereinbar und die zuständigen Stellen zu ihrer Verarbeitung berechtigt sind sowie die Verarbeitung zu diesen anderen Zwecken notwendig und verhältnismäßig ist. In Art. 11 Abs. 1 sind diese zulässigen anderen Zwecke näher spezifiziert:

- Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten,
- Zuständigkeit der empfangenden Stelle für die Feststellung und Verfolgung von Straftaten oder Vollstreckung von Sanktionen für Straftaten,
- Zustimmung des abgebenden Mitgliedstaates entsprechend den Anforderungen innerstaatlichen Rechts,
- angemessenes Datenschutzniveau des empfangenden Mitgliedstaates.

Abgesehen von dem Zustimmungserfordernis des Mitgliedstaates, von dem die Informationen stammen, sind die Anforderungen sehr allgemein gehalten und erlauben praktisch die Nutzung der Daten für jede Art von Ermittlungstätigkeit. Auch die EU-Kommission ist offenbar der Auffassung, dass die Zweckbindung im Rahmenbeschluss nicht stringent genug ist und erwägt Änderungen im Rahmen ihrer Gesamtstrategie zum Datenschutz nach Inkrafttreten des Lissabon-Vertrages. Der Rahmenbeschluss lasse zu viele Ausnahmen zu und darüber hinaus werden in den Bestimmungen Datenkategorien nicht nach ihrer sachlichen Richtigkeit und Zuverlässigkeit unterschieden.[481]

Der Prüm-Beschluss selbst regelt grundsätzlich, dass personenbezogene Daten nur zu den Zwecken genutzt werden dürfen, zu denen sie übermittelt worden sind, lässt

---

[480] Weichert aaO., S. 3.

[481] 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, S. 15 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf, letzte Abfrage 17.01.2012.

aber Ausnahmen mit Zustimmung des Mitgliedslandes zu, aus dem die Informationen stammen, Art. 26 Abs. 1 Prüm-Beschluss. DNA-Daten und daktyloskopische Daten dürfen allerdings nur zur Feststellung einer Übereinstimmung und ggf. der Vorbereitung eines förmlichen Amts- oder Rechtshilfeersuchens sowie der Protokollierung verwendet werden, Art. 26 Abs. 2 Prüm-Beschluss.

Zwischenergebnis

Der Vertrag von Prüm und der nachfolgende Ratsbeschluss für die Überführung in ein EU-Instrument bedeuten eine neue Stufe in der polizeilichen und justiziellen Zusammenarbeit innerhalb der EU. Während früher der Informationsaustausch entweder über zentrale Einrichtungen wie z.B. Europol und Eurojust oder zentrale Informationssysteme Schengener Informationssystem bzw. ´über schriftliche Anfragen oder Angebote (Schwedische Initiative) erfolgte, räumen sich die Mitgliedstaaten nunmehr nach dem Prinzip der allgemeinen Verfügbarkeit (principle of availabilty) unmittelbare Zugriffsrechte auf ihre Datenbestände ein. Den unterschiedlichen datenschutzrechtlichen Regelungen in den verschiedenen Mitgliedstaaten und auch solchen, mit denen Assoziierungsabkommen bestehen, wird nicht Rechnung getragen. Es kann also der Fall eintreten, dass Daten einer Person einer vom Recht des Heimatstaates unterschiedlichen Regelung unterworfen und entsprechend verarbeitet werden. Dem versucht die EU-Kommission zwar durch eine umfassende Kodifizierung für den gesamten Aufgabenbereich der EU einschließlich der Aktivitäten innerhalb der ehemaligen „dritten Säule“ entgegenzuwirken. Aber derzeit sind noch keine entsprechenden detaillierten Regelungen verfügbar. Mit dem Entwurf für eine neue Richtlinie zum Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit ist ein erster Schritt eingeleitet worden. Die Richtlinie würde sicherstellen, dass in diesem Bereich ein einheitliches Datenschutzniveau entsteht.

Besonders der Prüm-Beschluss macht deutlich, dass der Datenschutz mit der im Prinzip zu begrüßenden fortschreitenden innereuropäischen polizeilichen und justiziellen Zusammenarbeit nicht Schritt gehalten hat.

9.2.7.3 Richtlinie über Vorratsdatenspeicherung

Als weiteres EU-Instrument zur Bekämpfung des Terrorismus und der schweren Kriminalität ist die die Richtlinie über Vorratsdatenspeicherung zu nennen.[482] Der Erlass der Richtlinie wurde damit begründet, dass einige europäische Staaten bereits eine Vorratsdatenspeicherung praktiziert haben, allerdings in sehr unterschiedlicher Weise (Erwägungsgründe Nr. 5). Die rechtlichen und tatsächlichen Unterschiede zwischen den nationalen Vorschriften zur Vorratsdatenspeicherung würden den Binnenmarkt für die elektronische Kommunikation beeinträchtigen, da die Diensteanbieter mit unterschiedlichen Anforderungen in Bezug auf die zu speichernden Verkehrs- und Standortdaten und die Dauer der Vorratsdatenspeicherung konfrontiert seien (Erwägungsgründe Nr. 6). Andererseits werde die Vorratsdatenspeicherung insbesondere in der elektronischen Kommunikation als ein wertvolles Mittel bei der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten angesehen (Erwägungsgrund 7).
In den Erwägungsgründen wird mehrfach auf die Datenschutzrichtlinie 95/46/EG, die Datenschutzrichtlinie für die elektronische Kommunikation 2002/58/EG, Art. 8 EMRK und die EuDSK von 1981 Bezug genommen und dazu festgestellt, dass diese neben den jeweiligen nationalen Vorschriften im Interesse der Grundrechte der betroffenen Personen vollständig zu beachten sind (Erwägungsgründe 17 und 18).

Ausdrücklich wird ausgeführt, dass die Richtlinie nicht das Recht der Mitgliedstaaten berührt, Rechtsvorschriften über den Zugang zu und die Nutzung von Daten durch von ihnen benannte nationale Behörden zu erlassen (Erwägungsgrund Nr. 25)

Nach Art. 5 der Richtlinie 2006/24/EG ist u.a. die Speicherung folgender Daten vorgesehen:
- die genutzten Rufnummern und Kennungen
- Datum und Uhrzeit zu Beginn und Ende der Verbindungen
- Art des Dienstes
- bei Mobilfunk Standort der Zelle (Cell-ID) bei Beginn der Verbindung
- bei der Internet-Kommunikation die IP-Adresse.

---

[482] Richtlinie 2006/24/EG, ABl. L 105 vom 13.04.2006 S. 54.

Mit dem Inkrafttreten des Lissabon-Vertrages sind die Rechtsakte der Union auch den Bedingungen der Charta der Grundrechte der EU unterworfen. Für eine Prüfung kommen die Art. 7 GRCh (Achtung des Privat- und Familienlebens), Art. 8 (Datenschutz) , Art. 11 (Meinungsfreiheit) sowie Art. 15 und 16 (Berufs- und wirtschaftliche Betätigungsfreiheit) in Betracht.

Verstoß gegen Art. 7 GRCh

Die Kommunikation ist als ein Teilbereich der durch Art. 7 GRCh geschützten Privatsphäre zu betrachten.[483] Das gilt eindeutig für die Inhalte einer Kommunikation. Da es möglich ist, aus den Verkehrsdaten Bewegungsprofile zu erzeugen und andere Rückschlüsse auf die Gewohnheiten einer Person zu ziehen, kann man davon ausgehen, dass die Verkehrsdaten auch in den Schutz einbezogen sind.[484] Nach Art. 6 Abs. 1 der Datenschutzrichtlinie für die Kommunikation (DSRLK) sind die Betreiber von Telekommunikationseinrichtungen an sich grundsätzlich verpflichtet, die Verkehrsdaten nach Beendigung der Kommunikation zu löschen oder zu anonymisieren, soweit sie nicht zur Gebührenabrechnung benötigt werden, Art. 6 Abs. 2 DSRLK, oder der Nutzer seine Einwilligung zu einer Speicherung für bestimmte Zwecke gegeben hat, Art. 6 Abs. 3 DSRLK. Nach Art. 15 Abs. 1 DSRLK können die Mitgliedstaaten Rechtsvorschriften erlassen, durch die u.a. die Rechte und Pflichten aus Art. 6 im Interesse der nationalen Sicherheit, der Verteidigung, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von Kommunikationseinrichtungen beschränkt werden. Durch die Richtlinie über Vorratsdatenspeicherung ist in Art. 15 DSRLK ein Absatz 1a eingefügt worden, der regelt, dass die Bestimmung nicht gilt, soweit eine Speicherung von Verkehrsdaten nach Art. 1 Abs. 1 der Richtlinie über Vorratsdatenspeicherung ausdrücklich vorgeschrieben worden ist. Mit der Richtlinie 2009/136/EG[485] ist ein weiterer Abs. 1b in Art. 15

---

[483] Schorkopf in Ehlers (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Aufl. 2009, Kap. 16 Anm. 25; Grabenwarter, Europäische Menschenrechtskonvention, 4. Aufl. 2009, § 22 Anm. 10

[484] Uerpmann-Wittzak in Ehlers (Hrsg.) Europäische Grundrechte und Grundfreiheiten, 3. Aufl.2009, Kap. 3 Anm. 6.

[485] Richtlinie 2009/136/EG des Europäischen Parlaments und des vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, Art. 2 Ziffer 9: In Artikel 15 wird folgender Absatz eingefügt:

DSRLK eingefügt worden. Danach sind die Diensteanbieter gehalten, Verfahren zur Beantwortung von Anfragen über den Zugang zu den personenbezogenen Daten der Nutzer einzurichten.

Die Verkehrsdaten der Kommunikation einer Person liefern sehr weitgehende Aufschlüsse über deren Lebensweise, Kontakte und Aktivitäten, vor allem, wenn die Daten mit anderen frei zugänglichen Daten einer Person angereichert und durch geeignete Software aufbereitet werden.[486] Daher kann man feststellen, dass die Speicherung von Verkehrsdaten und die Vorschriften, die dies regeln, einen Eingriff in die von Art. 7 GRCh geschützte Privatsphäre einer Person darstellen. Der Eingriff kann aufgrund einer Schrankenregelung gerechtfertigt sein. Art. 7 GRCh gehört zu den Grundrechten, die denen der EMRK entsprechen, hier Art. 8 Abs. 1 EMRK, so dass sie laut Art. 52 Abs. 3 GRCh die gleiche Bedeutung und Tragweite haben. Die Bedeutung und Tragweite werden dabei nicht nur durch den Wortlaut der Vertragswerke, sondern auch durch die Rechtsprechung des EGMR und des EuGH bestimmt.[487]

Der Eingriff wäre daher nur unter den Voraussetzungen des Art 8 Abs. 2 EMRK gerechtfertigt.

„(1b) Die Anbieter richten nach den gemäß Absatz 1 eingeführten nationalen Vorschriften interne Verfahren zur Beantwortung von Anfragen über den Zugang zu den personenbezogenen Daten der Nutzer ein. Sie stellen den zuständigen nationalen Behörden auf Anfrage Informationen über diese Verfahren, die Zahl der eingegangenen Anfragen, die vorgebrachten rechtlichen Begründungen und ihrer Antworten zur Verfügung.“

[486] Der deutsche Politiker bei den Grünen, Malte Spitz, hat der Wochenzeitung „Zeit“ seine Verkehrsdaten aus einem Zeitraum von sechs Monaten zwecks Auswertung zur Verfügung gestellt, nachdem er sie zuvor bei der Deutschen Telekom eingeklagt hatte. Freiwillig wollte das Unternehmen ihm die nicht geben. (http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten, letzter Abruf 17.01.2012) Mit frei zugänglichen Daten von Malte Spitz (Blogeinträge, Twitter) angereichert, ergibt sich ein deutliches Profil. Es enthüllt, wann Malte Spitz durch die Straßen läuft, wann er Bahn fährt, wann er fliegt. Es zeigt, in welchen Städten und an welchen Orten er sich aufhält, zu welchen Zeiten er arbeitet und zu welchen er schläft, wann man ihn am besten erreichen kann und wann eher nicht. Es zeigt, wann er lieber telefoniert oder eine SMS schickt. Es lässt erkennen, in welchem Biergarten er gerne sitzt. Es zeigt ein Leben. (http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz, letzter Abruf 17.01.2012.

[487] Erläuterungen zur Grundrechte-Charta der EU, EuGRZ 2000, S. 559 ff (569).

1. Gesetzliche Grundlage

Die Richtlinie 2006/24/EG kommt als geeignete Rechtsgrundlage in Betracht. Man könnte argumentieren, dass es an der erforderlichen Bestimmtheit mangelt, weil die Richtlinie die zu Zugriffen berechtigten nationalen Behörden und die Kriterien für den Zugang nicht nennt. Dabei ist jedoch zu berücksichtigen, dass die Richtlinie einen noch in nationales Recht umzusetzenden Rechtsakt darstellt und der europäische Gesetzgeber dafür nur den Rahmen vorgibt. Außerdem hat der Richtliniengeber hinsichtlich des Zugangs zu den Vorratsdaten in Art. 4 der Richtlinie Rahmenbedingungen gesetzt, die bei der Umsetzung zu beachten sind: Benennung der zuständigen Behörden, Beachtung nationaler Gesetze, Beachtung des Völkerrechts, insbesondere der EMRK in der Auslegung des EGMR, Festlegung von Verfahren und Bedingungen des Zugangs.

2. Legitimes Ziel

Nach den Erwägungsgründen Nr. 7 und 8 der Richtlinie 2006/24/EG soll die Vorratsdatenspeicherung der Bekämpfung der schweren Kriminalität und des Terrorismus dienen. Die Verfolgung dieser Ziele dient der nationalen Sicherheit, der Aufrechterhaltung der Ordnung, der Verhütung von Straftaten und dem Schutz der Rechte und Freiheiten von Bürgern. Ein legitimes Ziel im Sinne von Art. 8 Abs. 2 EMRK ist daher gegeben.

3. Verhältnismäßigkeit des Eingriffs

Beim Schutz der nationalen Sicherheit räumt der EMRK den Staaten grundsätzlich einen weiten Ermessensspielraum bei der Auswahl der Mittel und der Notwendigkeit ihres Einsatzes ein.[488] Der Gerichtshof hat auch eine Gesetzgebung zur Überwachung der Telekommunikation im Rahmen der Bekämpfung des Terrorismus als zu-

---

[488] EGMR-Urteil vom 26.03.1987, Leander gg. Schweden, EGMR-E 3, S. 230 ff. (447), Ziffer 59: "*Der Gerichtshof erkennt jedoch an, dass die nationalen Behörden einen Beurteilungsspielraum (margin of appreciation / marge d'appréciation) genießen, dessen Reichweite nicht nur von dem jeweils verfolgten rechtmäßigen Ziel abhängt, sondern auch von der Eigenart des jeweiligen Eingriffs. Im vorliegenden Fall muss das Interesse des betreffenden Staates, seine nationale Sicherheit zu schützen, gegen die Schwere des Eingriffs in das Recht auf Achtung des Privatlebens des Bf. abgewogen werden. Ohne Zweifel besteht für die Vertragsstaaten die Notwendigkeit, zum Zweck des Schutzes der nationalen Sicherheit die zuständigen Behörden gesetzlich zu ermächtigen, erstens Daten über Personen zu sammeln und in nichtöffentlichen Registern zu speichern und zweitens diese Daten zu verwenden, wenn die Geeignetheit von Bewerbern für Stellen zu beurteilen ist, die für die nationale Sicherheit von Bedeutung sind.".*

lässig angesehen, vorausgesetzt es bestehen angemessene und wirkungsvolle Sicherheiten gegen staatlichen Missbrauch der Überwachungsbefugnisse.[489] Insoweit enthält die Richtlinie keine präzisen Regelungen. Allerdings enthält die Richtlinie Auflagen an die Mitgliedstaaten, Zuständigkeit, Zugang, Verfahren und Bedingungen des Zugriffs (Art. 4) eindeutig zu regeln, den Datenschutz und die Datensicherheit zu beachten (Art. 7) und für geeignete Kontrollen durch unabhängige Instanzen zu sorgen (Art. 9). In Bezug auf die zu erlassenden nationalen Vorschriften wird ausdrücklich auf die Beachtung der EMRK in der Auslegung des EGMR hingewiesen, Art. 4 Satz 2 der Richtlinie.
Nach Art. 8 Abs. 2 EMRK muss eine Maßnahme in einer demokratischen Gesellschaft notwendig sein, wenn sie gerechtfertigt sein soll. Nach der bereits mehrfach angezogenen Rechtsprechung des EGMR setzt der Begriff der Notwendigkeit voraus, dass der Eingriff einem dringenden sozialen Bedürfnis entspricht und insbesondere in Bezug auf das rechtmäßig verfolgte Ziel verhältnismäßig ist. Obwohl den Vertragsstaaten einen gewissen Ermessensspielraum eingeräumt ist, müssen die maßgeblichen Rechtsvorschriften und Vollzugspraktiken angemessene und wirksame Sicherungen gegen Missbrauch bieten.[490] Letzteres hängt von der Ausgestaltung der Bestimmungen im Rahmen der nationalen Umsetzung der Richtlinie ab.

Unabhängig davon stellt sich aber die Frage, ob für die Vorratsdatenspeicherung und damit auch für die Richtlinie selbst ein soziales Bedürfnis besteht und die mit der Vorratsdatenspeicherung verbundenen Eingriffe verhältnismäßig sind. Ein soziales Bedürfnis wäre zu bejahen, wenn das angestrebte Ziel, hier die Bekämpfung schwerer Kriminalität und des Terrorismus, ohne die Maßnahme nicht erreicht werden könnte.

Die Wirkung und Bedeutung der Vorratsdatenspeicherung für die Aufklärung und Verfolgung von Straftaten ist umstritten. Nach Auffassung von Kritikern hat die Ein-

---

[489] EGMR vom 06.08.1978, Klass u.a. gg. Deutschland, Ziffern 48 ff., EuGRZ 1979, S. 278 ff.; NJW 1979, S. 1755 ff.; Ziffer 50: *"Welches Überwachungssystem auch immer angewandt worden sein mag, der Gerichtshof muss davon überzeugt sein, dass angemessene und wirksame Garantien gegen Missbrauch vorhanden sind. Diese Beurteilung hat nur relativen Charakter: sie hängt von allen Umständen des Falles ab, wie Art, Umfang und Dauer der möglichen Maßnahmen, die für ihre Anordnung erforderlichen Gründe, die für ihre Zulassung, Ausführung und Kontrolle zuständigen Behörden und die Art des im nationalen Recht vorgesehenen Rechtsbehelfs. Demnach ist im Licht der Konvention zu prüfen, wie das System der geheimen Überwachung funktioniert, welches durch die umstrittene gesetzliche Regelung, in seiner durch das Urteil des BVerfG vom 15. Dezember 1970 modifizierten Fassung, errichtet worden ist."* , EGMR-E 1, S. 320 ff. (335).
[490] EGMR Urteil vom 28.04.2005, Buck gg. Deutschland, Leitsatz 1, NJW 2006, S.1495 ff..

führung der Vorratsdatenspeicherung nichts zur Verbesserung der Aufklärungsquote beigetragen, was durch entsprechendes statistisches Material unterlegt wird.[491] Insbesondere die mangelnde Festlegung in Bezug auf eine Kostenerstattung für den mit der Speicherung der Verkehrsdaten und der Auskunftserteilung verbundenen Aufwand an die Betreiber von Kommunikationseinrichtungen und die unterschiedlichen Speicherfristen haben sich die Wettbewerbsbedingungen eher verschlechtert als verbessert. Bei der Vorbereitung der Richtlinie hatte die Kommission eine Kostenerstattung noch für zwingend erachtet, um Marktstörungen zu vermeiden.[492] Entsprechend hatte sie dies auch in Art. 10 ihres ursprünglichen Entwurfes vorgesehen.[493]

In einem Bericht vom 18.04.2011 bewertet die EU-Kommission die Richtlinie über die Vorratsdatenspeicherung und ihre Anwendung durch die Mitgliedstaaten, um festzustellen, ob ihre Bestimmungen, insbesondere in Bezug auf die Datenkategorien und die Speicherfristen geändert werden müssen. Insgesamt sind die EU-Kommission und die Vertragsstaaten überwiegend der Auffassung, dass die Vorratsdatenspeicherung zu einer Verbesserung der Aufklärungsquote beigetragen habe und zur Verhütung und Verfolgung der Kriminalität unverzichtbar sei.[494] Verbessert werden müssten aus Sicht der Kommission folgende Punkte:

- Vereinheitlichung der Zweckbindung der Vorratsdatenspeicherung sowie der Straftaten, für deren Aufklärung sie genutzt werden kann,
- Harmonisierung der Speicherfristen,
- Festlegung der zugangsberechtigten Behörden,
- Festlegung von Sicherheitsmaßnahmen und Verwendungsbeschränkungen,

---

[491] www.vorratsdatenspeicherung.de , letzte Abfrage 17.01.2012.
[492] European Digital Rights, Shadow evaluation report on the Data Retention Directive (2006/24/EC), S. 6, http://www.edri.org/files/shadow_drd_report_110417.pdf , letzte Abfrage 17.01.2012.
[493] Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0438:FIN:EN:PDF., letzte Abfrage 22.04.2012.
[494] Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung, S. 1 und 28, http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_de.pdf, letzte Abfrage 17.01.2012

- Kriterien für geeignete Mess- und Berichtsverfahren.[495]

Abgesehen von den möglicherweise zu behebenden Mängeln der Richtlinie bleibt die Kernfrage, ob die anlasslose Speicherung der Verkehrsdaten von ca. 500 Mio. EU-Bürgern und ihr Einfluss auf die Ermittlung und Aufklärung von Straftaten in einem angemessenen Verhältnis stehen. Bedenkt man, dass die mit den Verkehrsdaten erzeugten Profile u.U. einen tieferen Einblick in die Lebensweise einer Person bieten als die Inhalte einzelner abgehörter Telefongespräche, muss man in der Vorratsdatenspeicherung einen schwerwiegenden Eingriff in die Privatsphäre der EU-Bürger sehen. Das Max Planck Institut für ausländisches und internationales Strafrecht stellt in einem Gutachten für das deutsche Bundesministerium für Justiz fest: *„Verkehrsdaten tragen ein hohes Überwachungspotential in sich, sie sind – besser als andere Daten- dazu geeignet, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren.“* [496] Der europäische Datenschutzbeauftragte bezeichnet die Richtlinie 2006/24/EG als “the most privacy invasive instrument ever adopted by the EU”.[497] Auf der anderen Seite muss man berücksichtigen, dass außer verbalen Aussagen der Befürworter der Vorratsdatenspeicherung über einzelne Ermittlungserfolge eindeutige Fakten über die Bedeutung für die Aufklärung Straftaten fehlen. Verfügbare Zahlen sprechen eher für einen geringen Einfluss. Nach einer Untersuchung des wissenschaftlichen Dienstes des Deutschen Bundestages haben sich die Aufklärungsquoten von Straftaten zwischen 2005 und 2010 in den europäischen Ländern nicht wesentlich verändert[498]

Untersuchungen in Deutschland haben ferner ergeben, dass die Zahl der Fälle, in denen mangelnde Verfügbarkeit von Verkehrsdaten die Ermittlungen beeinflusst haben, verhältnismäßig gering ist.[499] Nach Angaben des Bundeskriminalamtes in Deutschland gab es im Jahre 2005 381 Ermittlungsfälle, in denen Verkehrsdaten

---

[495] Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung, aaO. S. 39.
[496] Max-Planck-Institut für ausländisches und internationales Privatrecht, Forschungsgruppe Kriminologie, Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO, Forschungsbericht im Auftrag des Bundesministeriums der Justiz, S. 90
[497] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf. letzte Abfrage 17.01.2012.
[498] Wissenschaftlicher Dienst des Deutschen Bundestages, Bericht WD 7 – 3000 – 036/11, Seite 9, http://www.vorratsdatenspeicherung.de/images/Sachstand_036-11.docx, letzte Abfrage 17.01.2012.
[499] Polizeiliche Kriminalstatistik (PKS) 2010, S. 6, http://www.bka.de/nn_205960/DE/Publikationen/PolizeilicheKriminalstatistik/pks__node.html?__nnn=true , letzte Abfrage 17.01.2012.

fehlten[500]. Bei einer Gesamtzahl von sechs Millionen Ermittlungen pro Jahr liegen die Fälle, in denen Verkehrsdaten von Bedeutung sind, damit im Promillebereich. Kritiker der Vorratsdatenspeicherung verweisen daher auch auf die Statistiken des deutschen Bundeskriminalamtes, aus den sich ergebe, dass die Vorratsdatenspeicherung keinen messbaren Einfluss auf die Aufklärungsquote von Straftaten habe.[501] Nach einer Untersuchung im Auftrage des deutschen Bundesministeriums für Justiz hat die Auswertung von Verkehrsdaten in erster Linie Bedeutung für die Gewinnung von Ermittlungsansätzen für weitere Maßnahmen, weniger als selbständiges Beweismittel.[502] In einer Untersuchung dieses Institutes aus dem Jahre 2011, inwieweit sich Schutzlücken durch den Wegfall der Vorratsdatenspeicherung in Deutschland ergeben haben, konnte kein Zusammenhang zwischen Vorratsdatenspeicherung und Aufklärungsquote festgestellt werden. Auch im Vergleich mit anderen Ländern, die zum Teil schon länger eine Vorratsdatenspeicherung betreiben, konnte kein Einfluss auf die Aufklärungsquote festgestellt werden.[503]

Ferner ist zu fragen, welchen Wert und welche Bedeutung z.B. IP-Adressen für die Ermittlungstätigkeiten haben, die ja Ansatzpunkte für die Feststellung der Identität eines Nutzers und die Einleitung von Überwachungsmaßnahmen darstellen. Zunächst muss hervorgehoben werden, dass über die IP-Adresse lediglich der Anschlussinhaber eindeutig festgestellt werden kann und nicht die Person, die den Anschluss zu einem bestimmten Zeitpunkt genutzt hat. Im Übrigen kann man davon ausgehen, dass eine Person, die das Internet für unerlaubte Zwecke nutzen möchte, wohl geeignete Maßnahmen zur Verschleierung ihrer Identität ergreifen würde. Das ist offensichtlich einfacher als allgemein bekannt. In der Fachliteratur werden Möglichkeiten aufgezeigt, mit Hilfe modifizierter Firmware oder Nutzung von Anonymisierungsdiensten die Identität eines Nutzers zu verbergen.[504] Letzteres ist besonders wirksam, wenn Server in Ländern genutzt werden, auf die die Sicherheitsbehörden

---

[500] Eva Mahnken, Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten, S. 8 http://www.vorratsdatenspeicherung.de/images/bka_vorratsdatenspeicherung.pdf ,

[501] http://www.vorratsdatenspeicherung.de/content/view/378/79/lang,de/ , letzte Abfrage am 18.01.2012.

[502] Forschungsbericht im Auftrag des Bundesministeriums der Justiz, S. 223, http://dip21.bundestag.de/dip21/btd/16/084/1608434.pdf, letzte Abfrage 18.01.2012.

[503] Max Planck Institut, „Schutzlücken durch den Wegfall der Vorratsdatenspeicherung?“, S. 219/220, http://www.mpg.de/5000721/vorratsdatenspeicherung.pdf , letzte Abfrage 27.01.2012.

[504] Alsbih, Der reale Wert einer IP-Adresse, DuD 2011, S. 482 ff. (485)

im Inland keinen Zugriff haben. Ferner erscheint es ohne größeren technischen Aufwand möglich, die MAC-Adresse der Netzwerkschnittstelle, die bei der Verwendung von dynamischen IP-Adressen für die Identifizierung des Inhabers genutzt wird, entweder zu verfälschen oder die Identität durch Nutzung einer fremden MAC-Adresse zu verbergen.[505]

Unter Berücksichtigung dieser Gegebenheiten, insbesondere des Umstandes, dass sich ein Zusammenhang zwischen Vorratsdatenspeicherung und einer verbesserten Aufklärung von Straftaten nicht eindeutig nachweisen lässt, kann man nicht sagen, dass die Strafverfolgungsbehörden nicht ohne diese Maßnahme auskämen. Es besteht daher kein dringendes soziales Bedürfnis dafür, und deshalb erscheint die anlasslose Speicherung von Verkehrsdaten der Kommunikation unverhältnismäßig und im Sinne von Art. 8 Abs. 2 EMRK nicht notwendig in einer demokratischen Gesellschaft.

In einigen Mitgliedstaaten haben Gerichte die Vorratsdatenspeicherung bereits für unzulässig erklärt, entweder weil sie mit nationalen Grundrechten kollidiert oder gegen Art. 8 EMRK verstößt. Der rumänische Verfassungsgerichtshof befand, dass die fortgesetzte Speicherung von Verkehrsdaten den Wesensgehalt des Rechts auf Privatsphäre beseitige, weil alle Bürger betroffen seien, unabhängig davon, ob sie einer Straftat verdächtigt werden oder nicht.[506]

Der tschechische Verfassungsgerichtshof erklärte die nationalen Vorschriften zur Vorratsdatenspeicherung für nichtig und hatte im Hinblick auf die Intensität des Eingriff durch die anlasslose Speicherung von Verkehrs- und Bewegungsdaten bei der großen Zahl von Nutzern grundsätzliche Zweifel an der Zulässigkeit der Vorratsdatenspeicherung, vor allem weil nach statistischen Daten geringe Auswirkungen auf einen Rückgang begangener Straftaten bestünden.[507]

---

[505] Alsbih aaO. S. 484 f..
[506] Constitutional Court of Romania, decision of 8 October 2009, http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html ,letzte Abfrage 18.01.2012.
[507] Constitutional Court of the Czech Republic, decision of 31 March 2011, http://www.concourt.cz/clanek/GetFile?id=5075 , letzte Abfrage 18.01.2012.

Der EuGH hat sich in einem Verfahren der Republik Irland gegen das Europäische Parlament (Nichtigkeitsklage) mit der Richtlinie 2006/24/EG befasst.[508] Da Irland die Klage auf eine mangelnde Rechtsgrundlage für die Richtlinie gestützt und der Gerichtshof auf der Grundlage des Art. 95 EG die Richtlinie als Vorschrift für die Errichtung und das Funktionieren des Binnenmarktes ansah, brauchte er sich ex pressis verbis nicht mit den Bestimmungen zum Datenschutz auseinander zu setzen. Nach Lage der Dinge wird sich der EuGH in aber absehbarer Zeit unmittelbar mit datenschutzrechtlichen Aspekten der Vorratsdatenspeicherung zu befassen haben und dann möglicherweise endgültige Klarheit schaffen. Pressemeldungen zufolge hat der irische High Court im Januar 2012 den EuGH im Rahmen eines Vorabentscheidungsverfahren wegen der Brüsseler Vorgaben in der Richtlinie zur Vorratsdatenspeicherung angerufen. U.a. soll geklärt werden, ob bei einer nationalen Umsetzung auch die Bestimmungen der EMRK zu beachten sind.[509]

Das deutsche Bundesverfassungsgericht hat die deutschen Vorschriften, mit denen die Richtlinie 2006/24/EG umgesetzt worden ist, gleichfalls für unzulässig erklärt. Der Grundsatz der Verhältnismäßigkeit verlange, dass die gesetzliche Ausgestaltung eines solchen Datenspeicherung dem besonderen Gewicht des mit der Speicherung verbunden Grundrechtseingriffs angemessen Rechnung trägt. Erforderlich seien hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes. Der Abruf und die unmittelbare Nutzung der Daten sei nur verhältnismäßig, wenn sie überwiegend wichtigen Aufgaben des Rechtsgüterschutzes dienen. Im Bereich der Strafverfolgung setze dies einen durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraus.[510] Damit hält das Gericht die anlasslose Speicherung von Verkehrsdaten ohne konkreten Verdacht auf eine schwere Straftat für unzulässig.

Verstoß gegen Art. 16 Abs. 1 AEUV und Art. 8 GRCh

---

[508] EuGH, Urteil vom 10. 2. 2009 - C-301/06, http://lexetius.com/2009,105 , letzte Abfrage 19.01.2012.

[509] http://www.heise.de/newsticker/meldung/Vorratsdatenspeicherung-vs-Grundrechte-1424117.html, letzte Abfrage 31.01.2012.

[510] BVerfG Urteil vom 02.03.2010, 1 BVR 256,263,586/08, http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html, letzte Abfrage 18.01.2012.

Verkehrsdaten der Kommunikation in Verbindung mit Namen von Personen sind Daten über eine bestimmte oder bestimmbare Person und unterliegen daher grundsätzlich dem Datenschutz. Nach Art. 8 Abs. 2 GRCh dürfen personenbezogene Daten ohne Einwilligung des/der Betroffenen nur auf einer gesetzlichen legitimen Grundlage verarbeitet werden. Da die EMRK keine Art. 8 GRCh vergleichbare Bestimmung enthält, der EGMR behandelt den Datenschutz als Teil der durch Art. 8 Abs. 1 EMRK geschützten Privatsphäre, kommt als ergänzende Schrankenregelung Art. 52 Abs.1 GRCh in Betracht.[511]

Danach muss jede Einschränkung der in der Charta anerkannten Rechte gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Einschränkungen dürfen unter Wahrung des Grundsatzes der Verhältnismäßigkeit nur vorgenommen werden, wenn sie erforderlich sind und Zielen des Gemeinwohls oder dem Schutz der Rechte und Freiheiten anderer dienen. Hinsichtlich der Verhältnismäßigkeit hat der EuGH entschieden, dass die Mittel, die zu einer Einschränkung des Grundrechts führen, geeignet und nicht über dazu Erforderliche hinausgehen dürfen. Dabei seien die öffentlichen Interessen, hier die Strafverfolgung, und die privaten Belange gegeneinander abzuwägen. Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten seien auf das absolut Notwendige zu beschränken.[512] Berücksichtigt man die Intensität der mit der Vorratsdatenspeicherung verbundenen Eingriffe bei fast allen EU-Bürgern einerseits und auf der anderen Seite die verhältnismäßig geringe Zahl von Verfahren, in denen die Verkehrsdaten von Bedeutung für die Strafverfolgung sind, muss man den Schluss ziehen, dass die Maßnahme unverhältnismäßig ist.

Verletzung von Art. 11 GRCh

Nach dieser Vorschrift hat jeder Bürger das Recht auf freie Meinungsäußerung. Darin eingeschlossen ist die Freiheit, Informationen und Ideen ohne behördliche Eingriffe zu empfangen und weiterzugeben. Die Verpflichtung zur Speicherung der Verkehrsdaten bedeutet einen Eingriff in dieses Grundrecht. Wie bei anderen Grundrechten wird die Berufsfreiheit nicht schrankenlos gewährt. Im Rahmen von Art. 52 Abs. 1

---

[511] Erläuterungen zur Grundrechte-Charta der EU, EuGRZ 200, S. 559 ff (569).
[512] EuGH Urteil vom 9.11.2010, C-92/09 und C-93/09 – Schecke und Eifert ./. Land Hessen, http://www.eurolawyer.at/pdf/EuGH-C-92-93-09.pdf , letzte Abfrage 18.01.2012.

GRCh können Grenzen festgelegt werden. Diesbezügliche Maßnahmen müssen geeignet, erforderlich und angemessen sein. Angesichts der geringen Zahl der Fälle, in denen die Vorratsdatenspeicherung für Ermittlungen bedeutsam ist, bestehen Zweifel an der Erforderlichkeit der Maßnahme. Die Angemessenheit wird durch die derzeitige unterschiedliche Praxis in den Mitgliedsländern in Frage gestellt. Der mit der Speicherung der Verkehrsdaten aller EU-Bürger über einen Zeitraum von sechs Monaten bis zu zwei Jahren verbundene Aufwand erscheint im Hinblick auf die vergleichsweise geringe Bedeutung für die Ermittlungstätigkeit der Strafverfolgungsbehörden unverhältnismäßig.

Verletzung von Art. 15 und 16 GRCh

Im Rahmen dieser Bestimmungen wird die wirtschaftliche Betätigungsfreiheit gewährleistet und geschützt.[513] Das Grundrecht umfasst die dauerhafte auf Erwerb ausgerichtete Tätigkeit einer Person oder eines Unternehmens. Auch juristische Personen werden vom Schutzbereich erfasst.[514] Mit der Richtlinie 2006/24/EG wird insbesondere in die wirtschaftliche Betätigungsfreiheit eingegriffen, wenn die Speicherung von Verkehrsdaten und die von Behörden geforderten Auskünfte ohne Erstattung der damit verbundenen Kosten erfolgen sollen, denn damit werden den betroffenen Unternehmen wirtschaftliche Nachteile zugefügt, so dass von einem Eingriff in das Grundrecht auszugehen ist.

Auch hier ist die Schranke des Art. 52 Abs.1 GRCh zu berücksichtigen. Die Ausführungen zur Verhältnismäßigkeit oben bei der Prüfung des Art 11 GRCh gelten auch hier.

Rechtsbehelfe gegen die Richtlinie 2006/24/EG

Grundsätzlich wären Nichtigkeitsklagen der Mitgliedsländer oder einzelner EU-Bürger(innen) nach Art. 263 AEUV denkbar. Allerdings dürften die Klagen wegen Ablaufs der Zweimonatsfrist für die Klagerhebung (Art. 262 AEUV) nicht mehr zulässig sein. Anders wäre die Situation, wenn die von der Kommission geplante geänderte Richtlinie zur Vorratsdatenspeicherung erlassen wird. Aber möglich bleiben in jedem Fall Vorlagen an den EuGH nach Art. 267 AEUV, wenn die Frage der Gültigkeit

---

[513] Ruffert in Ehlers (Hrsg.) Europäische Grundrechte und Grundfreiheiten, 3. Aufl. 2009, S. 580.
[514] Ruffert aaO., S. 585.

der Richtlinie in einem Verfahren vor dem Gericht eines Mitgliedstaates für die Entscheidung relevant ist.

Zusammenfassung

Im Ergebnis ist festzustellen, dass die Vorratsdatenspeicherung wegen des mit ihr verbundenen sehr weitgehenden Eingriffs in verschiedene Grundrechte und des damit verbundenen Aufwands im Hinblick auf die verfolgten Zwecke zu weitgehend ist. In einem Gutachten des wissenschaftlichen Dienstes des deutschen Bundestages vom 25. Februar 2011 wird der Richtlinie 2006/24/EG zwar eine erhebliche Grundrechtsrelevanz beigemessen, aber ein offensichtlicher Verstoß gegen die Art. 7 und 8 GRCh verneint, weil die Richtlinie nur die Vorratsdatenspeicherung an sich regele und die Regelung der sensiblen Bereiche wie Zugang und Verwendung der Daten den Mitgliedstaaten überlasse. In Bezug auf den Grundsatz der Berufs- und wirtschaftlichen Betätigungsfreiheit werden aber Zweifel an der Angemessenheit in Hinsicht auf die Zweck/Mittel-Relation angemeldet.[515]

Auch in der Literatur werden Zweifel an der Konformität der Richtlinie mit den europäischen Grundrechten geäußert. Mit Hinweis auf die Entscheidung des Rumänischen Verfassungsgerichts vom 08.10.2009[516] wird deutlich gemacht, dass die Grundrechte der EMRK und der GRCh nur ausnahmsweise und unter strengen Voraussetzungen eingeschränkt werden könnten. Die rechtliche Verpflichtung zur kontinuierlichen Vorratsspeicherung persönlicher Daten durch die Richtlinie 2006/24/EG mache jedoch die Ausnahme vom Grundsatz des Schutzes des Rechts auf Privatsphäre und Meinungsfreiheit zur absoluten Regel und verstoße damit gegen den Wesensgehalt der der Rechte und Freiheiten aus den Art. 7, 8 und 11 GRCh.[517]

Damit ist das Hauptproblem in der Angemessenheit der Vorratsdatenspeicherung an sich, d.h. der anlasslosen Speicherung der Verkehrsdaten aller Bürger in der gesam-

---

[515] Derksen, Wissenschaftliche Dienste des Deutschen Bundestages, Zur Vereinbarkeit der Richtlinie über die Vorratsdatenspeicherung von Daten mit der Europäischen Grundrechtscharta, http://www.vorratsdatenspeicherung.de/images/rechtsgutachten_grundrechtecharta.pdf, letzte Abfrage 22.04,2012.

[516] Entscheidung des Rumänischen Verfassungsgerichts Nr. 1258 vom 08.10.2009, http://www.vorratsdatenspeicherung.de/content/view/342/79/lang,de/#Urteil , letzte Abfrage 19.01.2012.

[517] Petri, Die Richtlinie 2006/24/EG zur Vorratsspeicherung von Telekommunikationsverkehrsdaten- Ein Problem des europäischen Grundrechtsschutzes, DuD 2011, S. 607 ff. (609).

ten EU unabhängig von der Ausgestaltung in den einzelnen Mitgliedsländern, zu sehen. Im Verhältnis zu dem damit verbundenem Aufwand, den Risiken eines Missbrauchs und der Intensität des Eingriffs auf der einen Seite und des im Vergleich dazu insgesamt doch überschaubaren Nutzens für die Strafverfolgung erscheint die anlasslose Speicherung der Verkehrsdaten aller Bürger nicht gerechtfertigt.

10. Die Vorratsdatenspeicherung in Österreich

Wenn man außer Betracht lässt, dass möglicherweise bereits die Richtlinie 2006/24/EG über die Speicherung von Vorratsdaten gegen europäische Grundrechte verstößt, ergibt sich die Frage, ob die Bestimmungen zur Umsetzung der Richtlinie in Österreich dem nationalen Recht entsprechen.

Die nationalen Vorschriften zur Umsetzung sind in zwei Gesetzen enthalten, dem Änderungsgesetz zum Telekommunikationsgesetz 2003[518] und dem Änderungsgesetz zur Strafprozessordnung und zum Sicherheitspolizeigesetz[519] Die entsprechenden Bestimmungen sind am 01.04.2012 in Kraft getreten, § 136a Abs. 4 TKG –neu- und § 514 Abs.15 StPO –neu-.

Als Prüfungsgrundlage kommen § 1 DSG 2000, Art. 8 EMRK und Art. 10a StGG in Betracht.

10.1 Grundzüge der gesetzlichen Regelung

Mit Rücksicht auf die grundsätzliche Kritik an der Vorratsdatenspeicherung entsprechend den Ausführungen im vorangehenden Kapitel hat sich der Gesetzgeber erkennbar bemüht, die Bestimmungen grundrechtskonform auszugestalten.[520] Das Boltzmann Institut für Menschenrechte hat an den Entwürfen mitgewirkt. Leider wurden nicht alle Vorschläge des Instituts berücksichtigt.[521]

Als positiver Gesichtspunkt ist u.a. hervorzuheben, dass gemäß § 94 Abs. 1 TKG -neu- vorgesehen ist, den Anbietern die Kosten, die sie für die erforderliche Infrastruktur zur Erfassung der Vorratsdaten zu 80% zu ersetzen. Maßgeblich für diese Maßnahme war das VfGH-Erkenntnis vom 27.02.2003, in dem der Gerichtshof entsprechende Vorgaben gemacht hatte.[522] Der Gerichtshof hatte in der 100%igen Auferle-

---

[518] BGBl. Teil I Nr. 27 vom 18.05.2011, S. 1-7
[519] BGBl. Teil I Nr. 33 vom 20.05.2011, S. 1-4
[520] Vorblatt zur Novelle des Telekommunikationsgesetzes, Vorblatt zur Änderung der Strafprozessordnung und des Sicherheitspolizeigesetzes, http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/fname_206854.pdf, http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01075/fname_206859.pdf, letzte Abfrage 12.12.2011
[521] http://bim.lbg.ac.at/de/informationsgesellschaft/bimentwurf-zur-vorratsdatenspeicherung-begutachtung, letzte Abfrage 04.04.2012
[522] http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Vfgh&Dokumentnummer=JFT_09969773_02G00037_00&ResultFunctionToken=9a651f2d-7f9e-45f3-b8a5-

gung der Kosten für Überwachungen im Interesse der Strafrechtspflege eine Verletzung des Grundsatzes der Verhältnismäßigkeit gesehen. Veranschlagt werden Gesamtkosten von 15 Mio. €. Die Erstattung der Kosten des laufenden Betriebes für den Unterhalt der Systeme und die Erteilung von Auskünften soll nach der Überwachungskostenverordnung aus Mitteln des Bundesministeriums für Justiz erfolgen, § 94 Abs.2 TKG –neu-. Damit wird auch einem möglichen Vorhalt eines Eingriff in die wirtschaftliche Betätigungsfreiheit (Art. 15 und 16 GRCh) entgegengewirkt.

Für die Dauer der Speicherung ist die von der EU-Richtlinie vorgegebene Mindestfrist von sechs Monaten vorgesehen, § 102a Abs. 1 TKG –neu-. Nach der Regierungsvorlage fällt der Großteil der Anfragen der Sicherheitspolizei in die ersten drei Monate nach Beginn der Ermittlungen, so dass die Frist ausreichend erscheint.

Der Forderung nach Datensicherheit wird durch § 94 Abs.3 und 4 TKG –neu- Rechnung getragen. Der Bundesminister für Verkehr, Innovation und Technologie soll im Verordnungswege die Übertragungs- und eine anspruchsvolle Verschlüsselungstechnologie festlegen, durch die die Integrität der Daten sichergestellt werden soll.

Nach § 102a TKG –neu- erfolgt die Speicherung von Vorratsdaten ausschließlich zu dem Zweck der Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO rechtfertigt. Die Anordnung nach dieser Vorschrift ist zulässig,

2. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder
3. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.
4. wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

9e33d9cf7cb3&Position=1&Entscheidungsart=Erkenntnis&Sammlungsnummer=&Index=&SucheNach
letzte Abfrage 17.01.2012.

Die Anbieter sind verpflichtet, bestimmte im Gesetz (§102a Abs. TKG –neu-) spezifizierte personenbezogene Daten[523] zu speichern.

Nach § 102 b Abs. 1 TKG –neu- ist eine Auskunft über Vorratsdaten ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten zulässig, deren Schwere eine Anordnung nach § 135 Abs. 2 a StPO rechtfertigt. Zu begrüßen ist, dass für das Auskunftsverlangen der Strafverfolgungsbehörden unter dem Vorbehalt einer richterlichen Anordnung steht und damit willkürlichen Maßnahmen entgegengewirkt wird.

Allerdings sind auch die Sicherheitsbehörden zu Auskünften unter Verwendung von Vorratsdaten im Rahmen des § 99 Abs. 5 –neu- berechtigt. Im Wesentlichen geht es hier um Auskünfte nach § 53 Abs. 3 a und 3 b SPG[524] -neu-. Aber der Rechtsschutz-

---

[523] *2) Anbietern von Internet-Zugangsdiensten obliegt die Speicherung folgender Daten:*
1. Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war;
2. Datum und Uhrzeit der Zuteilung und des Entzugs einer öffentlichen IP-Adresse bei einem Internet-Zugangsdienst unter Angabe der zugrundeliegenden Zeitzone;
3. die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss;
4. die eindeutige Kennung des Anschlusses, über den der Internet-Zugang erfolgt ist.
(3) Anbietern öffentlicher Telefondienste einschließlich Internet-Telefondiensten obliegt die Speicherung folgender Daten:
1. Teilnehmernummer oder andere Kennung des anrufenden und des angerufenen Anschlusses;
2. bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Teilnehmernummer, an die der Anruf geleitet wird;
3. Name und Anschrift des anrufenden und des angerufenen Teilnehmers;
4. Datum, Uhrzeit des Beginns und Dauer eines Kommunikationsvorganges unter Angabe der zugrundeliegenden Zeitzone;
5. die Art des in Anspruch genommenen Dienstes (Anrufe, Zusatzdienste und Mitteilungs- und Multimediadienste).
6. Bei Mobilfunknetzen zudem
a) der internationalen Mobilteilnehmerkennung (IMSI) des anrufenden und des angerufenen Anschlusses;
b) der internationalen Mobilfunkgerätekennung (IMEI) des anrufenden und des angerufenen Anschlusses;
c) Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Standortkennung (Cell-ID), an dem der Dienst aktiviert wurde, wenn es sich um vorbezahlte anonyme Dienste handelt;
d) der Standortkennung (Cell-ID) bei Beginn einer Verbindung.
(4) Anbietern von E-Mail-Diensten obliegt die Speicherung folgender Daten:

[524] Sicherheitspolizeigesetz, BGBl. Nr. 566/1991 zuletzt geändert durch BGBl. I Nr. 13/2012, § 3 Abs. 3a und 3b: (3a) *Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001) Auskünfte zu verlangen:*

beauftragte ist über derartige Auskunftsverlangen ehestmöglich zu informieren, § 91 c Abs.1 Satz 3 SPG. Seine vorherige Zustimmung ist nicht erforderlich. Er kann aber nach erhaltener Information aktiv werden, wenn er der Auffassung ist, dass Rechtsverstöße in Zusammenhang mit dem Auskunftsverlangen vorliegen. Weiß der Betroffene nichts von der Erhebung personenbezogener Daten und ist der Rechtsschutzbeauftragte der Auffassung, dass ein Regelverstoß vorliegt, dann ist er verpflichtet, diesen zu informieren oder, wenn dies aus Gründen des § 26 Abs. 2 DSG 2000 nicht erfolgen kann, eine Beschwerde bei DSK zu erheben, § 91 d Abs. 3 SPG. Der Rechtsschutz ist damit schwächer ausgeprägt als im strafrechtlichen Ermittlungsverfahren, von den grundsätzlichen, unter Kap. 8.5.3 b dargelegten, Bedenken gegen die Institution des Rechtsschutzbeauftragten einmal abgesehen. Man muss aber berücksichtigen, dass die von der Sicherheitspolizei geforderten Auskünfte in der Regel eilbedürftig sind, weil es um die Erfüllung der ersten allgemeinen Hilfeleistungspflicht in konkreten Gefahrensituationen und die Abwehr gefährlicher Angriffe geht.

---

1. über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses wenn dies zur Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben erforderlich ist,

2. über die Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr

a) einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19),

b) eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder

c) einer kriminellen Verbindung (§ 16 Abs.1 Z 2) benötigen,

3. über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr

a) einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§19),

b) eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder

c) einer kriminellen Verbindung (§ 16 Abs. 1 Z 2) benötigen,

auch wenn hierfür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 4 iVm § 102a TKG 2003 erforderlich ist,

4. über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer, wenn dies zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder zur Abwehr gefährlicher Angriffe erforderlich ist.

(3b) Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten oder diesen begleitenden Menschen mitgeführten Endeinrichtung zu verlangen, auch wenn hierfür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist, sowie technische Mittel zur Lokalisierung der Endeinrichtung zum Einsatz zu bringen.

Im Rahmen des strafrechtlichen Ermittlungsverfahrens ist nicht ohne weiteres erkennbar, welche Straftaten erfasst werden. § 102a Abs. TKG –neu- verweist auf § 135 Abs. 2 a StPO –neu-. Anordnungen nach dieser Bestimmung setzen voraus, dass es um Straftaten geht, die nach dem Strafgesetzbuch mit mehr als einem Jahr Freiheitsstrafe bedroht sind. Bei näherem Hinsehen zeigt sich, dass zahlreiche Straftatbestände erfasst werden. Dabei handelt es z.B. nicht nur um schwere Straftaten gegen Leib und Leben wie Mord, § 75 StGB, Totschlag, § 76 oder die Sicherheit des Staates wie Hochverrat, § 242 StGB, Staatsfeindliche Verbindungen, § 246 StGB und Verrat von Staatsgeheimnissen, sondern auch sehr viele mittelschwere Straftaten. Dazu zählen z.B. schwere Sachbeschädigung, § 126 Abs. 3 StGB, Einbruchsdiebstahl, § 129 StGB, zahlreiche Vermögensdelikte bei Werten über 50.000 € wie Veruntreuung, § 133 Abs. 2 StGB, Unterschlagung, 134 Abs. 3 StGB, Sachentziehung, § 135 Abs. 2 StGB, Betrügerischer Datenverarbeitungsmissbrauch, § 148a Abs. 2 StGB, Untreue, § 153 Abs.2 StGB, Förderungsmissbrauch, § 153 b Abs. 4 StGB und Hehlerei § 164 Abs. 4 StGB. Weiter sind erfasst Raub, § 142 Abs. 1 StGB, Erpressung, § 144 Abs. 1 StGB, gewerbsmäßiger Betrug, § 148 StGB, gewerbsmäßiger Geldwucher, § 154 Abs. 3 StGB, Betrügerische Krida, § 156 StGB, Schädigung fremder Gläubiger, § 157 StGB, Brandstiftung, § 169 StGB, Vergewaltigung, § 201 StGB, Geschlechtliche Nötigung, § 202 StGB und sexueller Missbrauch von Unmündigen, § 207 StGB. Die Aufzählung ist nicht vollständig, aber verdeutlicht, dass nicht nur schwere Kriminalität, sondern ein breites Spektrum erfasst wird. Praktisch ist nur Bagatellkriminalität ausgeschlossen.

10.2 Bestimmtheit der Vorschriften

Jemand, der sich orientieren möchte, müsste das gesamte Strafgesetzbuch durchsehen, wenn er sich einen Überblick darüber verschaffen wollte, in welchen Fällen ein Zugriff der Strafverfolgungsbehörden auf Vorratsdaten gestattet ist. Deshalb bestehen zunächst unter dem Gesichtspunkt des § 1 Abs. 2 DSG 2000 und Art. 8 Abs. 2 EMRK Zweifel, ob die einen Eingriff gestattenden Vorschriften ausreichend klar und verständlich sind. Der EGMR hat in diesem Zusammenhang gefordert, dass die Tatbestände klar bezeichnet werden, die einen Eingriff erlauben. Diese Qualitätsanforderungen bedeuten, dass die fraglichen Vorschriften für die Betroffenen zugänglich und vorhersehbar sind. Vorhersehbar sind sie nach Auffassung des EGMR nur dann,

wenn sie so präzise und klar formuliert sind, dass der Einzelne sein Verhalten danach ausrichten kann.[525]

10.3 Verhältnismäßigkeit

Unabhängig von den Ausführungen zur Richtlinie über Vorratsdaten 2006/24/EG stellt sich auch für die Umsetzung in Österreich die Frage, ob die dafür getroffenen Regelungen in einer demokratischen Gesellschaft für die Aufrechterhaltung der öffentlichen Ordnung und die Sicherheit des Staates notwendig sind. Aus Sicht des EGMR bedeutet Notwendigkeit im Sinne von Art. 8 Abs.2 EMRK, dass für eine Maßnahme ein dringendes soziales Bedürfnis bestehen und diese in Bezug auf ein rechtmäßig verfolgtes Ziel verhältnismäßig sein muss.[526] Bei Maßnahmen im Interesse der öffentlichen Sicherheit und der Gefahrenabwehr hat der EGMR den nationalen Gesetzgebern zwar einen Ermessensspielraum eingeräumt. Die geheime Überwachung des Post- und Telefonverkehrs sei mit Rücksicht auf die Ausweitung von Spionageaktivitäten und der Entwicklung des Terrorismus im Interesse der öffentlichen Sicherheit und Ordnung in einer demokratischen Gesellschaft notwendig. Der eingeräumte Ermessensspielraum zur Bekämpfung des Terrorismus ermächtige die Staaten jedoch nicht zu jeder beliebigen Regelung, die Ihnen geeignet erscheine, und es müssten auch Maßnahmen gegen Missbrauch getroffen werden.[527] Zur Vorratsdatenspeicherung hat der EGMR zwar noch keine Stellung genommen, aber anlässlich einer Entscheidung zum Abhören von Telefongesprächen hat er u.a. zu Art. 8 Abs. 2 EMRK ausgeführt, dass diese Bestimmung als Ausnahme zu einem von der Konvention geschützten Recht eng ausgelegt werden müsse. Befugnisse zur geheimen Überwachung von Bürgern, wie sie für einen Polizeistaat typisch seien, könnten nur hingenommen werden, wenn sie für die Erhaltung der demokratischen Einrichtungen unbedingt notwendig seien.[528] Mit Rücksicht auf die mit derartigen Eingriffen

---

[525] EGMR Urteil vom 20.06.2002 Al-Nashif gegen Bulgarien, ÖJZ 2003, S. 344 ff., Ziffer 119, „The Court reiterates that the phrase “in accordance with the law” implies that the legal basis must be “accessible” and “foreseeable”. A rule's effects are “foreseeable” if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct.”, http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Al-Nashif&sessionid=92956545&skin=hudoc-en, letzte Abfrage 22.04.2012.

[526] Urteil des EGMR vom 28. 04.2005, Buck gg. Deutschland, Ziffer 44, NJW 2006, 1495 ff..

[527] Urteil des EGMR vom 04.12.2008, Marper gg. Großbritannien, Ziffer 103, EuGRZ 2009, S. 299 ff. (311).

[528] Urteil des EGMR vom 06.09.1978, Klaas gg. Deutschland, Ziffer 42, EuGRZ 1979, 278 ff.

verbundenen Gefahren für die Demokratie sei nicht jede beliebige Maßnahme zur Abwehr von Spionage und Terrorismus zulässig. Außerdem müssten ausreichende Garantien gegen Missbrauch bestehen.[529]
Vor dem Hintergrund dieser Rechtsprechung ist festzustellen, dass die Regelung zur Speicherung von Vorratsdaten in Österreich nicht nur Straftaten erfasst, die existenzielle Grundlagen des Landes gefährden. § 135 Abs. 2 a StPO umfasst ein breites Spektrum an Kriminalität und nicht nur die demokratischen Grundlagen gefährdende Delikte. Praktisch ist im Wesentlichen nur die Bagatellkriminalität ausgeschlossen. Wenngleich die Richtlinie 2006/24/EG den Begriff der schweren Kriminalität nicht definiert und den Mitgliedstaaten die Ausfüllung überlassen hat, ist eine so weit gehende Nutzung von Vorratsdaten sicher nicht gemeint und von Art. 8 Abs. 2 EMRK auf Basis der Rechtsprechung des EGMR nicht gedeckt.

Abgesehen von der Regelung in § 135 a StPO verpflichtet auch § 76 a Abs. 2 StPO die Provider zu Auskünften. Danach sind diese auf Anordnung der Staatsanwaltschaft zur Aufklärung des konkreten Verdachts einer Straftat verpflichtet, E-Mail- und IP-Adressen nebst Teilnehmerkennung sowie Name und Anschrift des Teilnehmers zu nennen. Eine Beschränkung auf bestimmte Straftaten oder einen bestimmten Strafrahmen ist in dieser Vorschrift nicht vorgesehen. Der Beschuldigte ist aber nach Abschluss der Ermittlungen zu unterrichten, § 138 Abs. 5 StPO.

In diesem Zusammenhang sei auch auf die Rechtsprechung des deutschen BVerfG verwiesen, das entsprechende Bestimmungen im deutschen TKG für unwirksam erklärt und die Auswertung von Verkehrsdaten auf die Bekämpfung des durch Tatsachen begründeten Verdachts einer schweren Straftaten beschränkt hatte. Eine katalogmäßige Aufzählung von Straftaten hat er abgelehnt und eine präzise Bezeichnung der zu schützenden Rechtsgüter gefordert. Bei der Abwägung zwischen der Schwere des Eingriffs in das informationelle Selbstbestimmungsrecht, der mit der Speicherung und der Verwendung der Vorratsdaten verbunden ist, und der Bedeutung einer wirksamen Gefahrenabwehr kam das Gericht zu dem Ergebnis, dass ein Abruf der Verkehrsdaten einer Kommunikation nur zur Abwehr von Gefahren für Leib, Leben

---

[529] Urteil vom 04.12.2008, Marper gg. Großbritannien, Ziffer 103, EuGRZ 2009, S. 299 ff. (311).

oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zugelassen werden dürfe.[530]

In der Regierungsvorlage zur Änderung des TKG in Österreich[531] berufen sich die Verfasser u. a. darauf, dass die Sicherheitsbehörden bereits nach den bisherigen gesetzlichen Vorschriften z. B. Name, Anschrift, Teilnehmernummer eines bestimmten Anschlusses und IP-Adresse zu einer Nachricht ganz allgemein für jede Art von Kriminalität erfragen dürfen, § 53 Abs. 3 a SPG alt. Bei Gefahr für Leib und Leben einer Person gilt das auch für die Standortdaten eines Mobiltelefons. Allerdings betrifft das nur Daten, die noch bei den Providern verfügbar sind. Nach den Angaben in der Regierungsvorlage[532] halten diese die Daten aus abrechnungstechnischen Gründen ca. drei Monate vor. Wenn man berücksichtigt, dass die Sicherheitsbehörden die Kommunikationsdaten überwiegend in den ersten drei Monaten nach Beginn der Ermittlungen abfragen, so spricht dies eigentlich eher gegen die Notwendigkeit einer Speicherung von Vorratsdaten.

10.4 Speicherung von Vorratsdaten von zur Amtsverschwiegenheit verpflichteten Personen

In § 93 Abs. 5 TKG -neu- wird zwar nochmals auf das Umgehungsverbot in den §§ 144 und 157 Abs. 2 StPO hingewiesen. Aber eine rechtliche und technische Regelung, die die Speicherung von Kommunikationsdaten der betroffenen Personen vermeidet, wurde nicht. getroffen. In der Regierungsvorlage werden Betroffene auf die Möglichkeit von Rechtsmitteln verwiesen.[533] Es wird argumentiert, dass die Frage, ob eine Umgehung vorliege, nicht den Dienstleistern überlassen werden könne. Die Entscheidung obliege vielmehr dem Richter bzw. Rechtsschutzbeauftragten, weil auch Ermittlungen gegen diesen Personenkreis grundsätzlich nicht ausgeschlossen seien, wenn sie selbst einer Straftat verdächtigt werden. Es gibt sicher praktische Probleme, die Speicherung der Vorratsdaten dieses Personenkreises zu vermeiden. Aber das darf den Gesetzgeber nicht dazu veranlassen, das Umgehungsverbot nicht

---

[530] Urteil des deutschen BVerfG vom 02.03.2010, BvR 256/08, Leitssatz 5 und Rd-.-Nr. 211 und 231, http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html, letzte Abfrage 22.04,2012.
[531] Regierungsvorlage zur Änderung des Telekommunikationsgesetzes 2003, Abschnitt D 1, S. 10 f. http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/fname_206854.pdf, letzte Abfrage 22.04.2012.
[532] RV zur Änderung des TKG, Vorblatt Abschnitt D 1, S. 11 , , letzte Abfrage 22.04.2012.
[533] RV zur Änderung des TKG, Vorblatt, zu § 93 Abs. 5, S. 16

zu beachten. Mit der Speicherung der Daten ist der Grundrechtseingriff bereits geschehen und wird durch Verweis auf die Möglichkeit von Rechtsmitteln im Strafprozess nicht geheilt. Im Anwendungsbereich des SPG sind Rechtsmittel nur dann möglich, wenn der Betroffene davon erfährt, was regelmäßig nicht der Fall sein dürfte. Man kann nur darauf vertrauen, dass der Rechtsschutzbeauftragte aktiv wird.
Der Gesetzgeber beruft sich in diesem Zusammenhang[534] zu Unrecht auf ein Urteil des EGMR.[535] In dieser Entscheidung hat sich das Gericht mit dem geheimen Abhören des Telefonanschlusses eines Anwaltes befasst und festgestellt, dass dies einen Eingriff in die Privatsphäre bedeute, der nur unter den Voraussetzungen des Art. 8 Abs. 2 EMRK gerechtfertigt werden könne. Er stellte besondere qualitative Anforderung zum Merkmal „ gesetzlich vorgesehen“ auf und verlangte im Zusammenhang mit geheimen Überwachungsmaßnahmen und dem Abhören von Telefongesprächen durch staatliche Behörden, dass wegen des Fehlen einer öffentlichen Kontrolle und der Gefahr des Machtmissbrauchs das innerstaatliche Recht dem Einzelnen einen Schutz gegen willkürliche Eingriffe in die Rechte nach Art. 8 Abs. 1 EMRK bieten müsse. In dem vorliegenden Fall bemängelte er weiter, dass ein Widerspruch zwischen dem Wortlaut des Gesetzes, das das Berufsgeheimnis des Anwalts schütze, und der von den Behörden geübten Praxis bestehe. Insbesondere kläre das Gesetz, auf dessen Grundlage die Eingriffe gestützt werden, nicht, wer, wie und unter welchen Bedingungen die Auswahl treffen solle, welche Aufnahmen dem anwaltlichen Berufsgeheimnis unterfielen und welche keinen Bezug dazu hätten.

Entsprechende Bestimmungen sind auch in Österreich im Rahmen der Vorratsdatenspeicherung nicht getroffen worden. Der beschriebene Fall betraf allerdings nicht die Erfassung und Auswertung von Kommunikationsdaten, sondern Inhaltsdaten. In Kapitel 2.3 ist aber bereits dargestellt worden, dass die Auswertung von Kommunikationsdaten im Vergleich zur Aufzeichnung von Inhaltsdaten keinen minderschweren Eingriff in die Privatsphäre bedeutet.[536] Da zumindest nach diesseitiger Auffassung Art. 10 a StGG im Rahmen einer teleologischen Auslegung auch auf Verkehrsdaten

---

[534] RV zum TKG, Anm. zu § 93 Abs. 5, http://www.ris.bka.gv.at/Dokumente/RegV/REGV_COO_2026_100_2_654439/REGV_COO_2026_100_2_654439.html, letzte Abfrage 22.04.2012.
[535] Urteil des EGMR vom 23.03.1998, Kopp gegen Schweiz, OJZ 1999, S. 115 ff..
[536] Siehe auch Urteil des deutschen BVerfG zitiert unter Fußnote

anzuwenden ist, dürften Eingriffe in das Grundrecht auf Datenschutz im Rahmen der Vorratsdatenspeicherung nicht ohne richterliche Einwilligung stattfinden.

10.5 Zusammenfassung zu Vorratsdatenspeicherung

Österreich hat mit der Umsetzung der Richtlinie lange gezögert und dem Drängen der EU schließlich nachgegeben. Für den Entwurf hat die Regierung sich der Unterstützung des Ludwig Boltzmann Institutes versichert, das bereits die europäische Richtlinie 2005/4/EG an für sich grundrechtswidrig hält, sich aber bemüht hat, die Grundrechtseingriffe in der Umsetzung möglichst gering zu halten.[537] Das ist zum Teil auch gelungen, z. B. hinsichtlich des Zugriffs der Behörden auf die Vorratsdaten. Die Daten werden gesondert gespeichert, § 102c Abs. 1 TKG -neu-, die Zugriffe darauf protokolliert, § 102 c Abs. 2 TKG -neu-, und die Übertragung erfolgt verschlüsselt, § 94 Abs. 4 TKG -neu-. Ebenso ist zu begrüßen, dass für die Nutzung von Vorratsdaten im Strafverfahren eine richterliche Bewilligung erforderlich ist. Die Sicherheitsbehörden sind im Falle von Auskunftsverlangen über Vorratsdaten verpflichtet, den Rechtsschutzbeauftragten ehestmöglich zu informieren, § 91 c Abs. 1 Satz 3 SPG -neu-, und dieser ist gehalten, die Meldungen zu prüfen, § 91 c Abs. 1 Satz 4 SPG -neu-. Stellt er eine Verletzung des Grundrechtes auf Datenschutz fest ist er entgegen der bisherigen Regelung nicht nur befugt, sondern verpflichtet, Beschwerde bei der DSK einzulegen, §91 d Abs. 3 SPG -neu-.

Die mangelnde Beschränkung der Bestimmungen zur Vorratsdatenspeicherung im TKG, der StPO und dem SPG auf wirklich schwere Straftaten erscheint aber unter Berücksichtigung der Schwere des Eingriffs und der bereits nach der früheren Rechtslage gegebenen Auskunftsmöglichkeiten der Sicherheits- und Strafverfolgungsbehörden dennoch nicht verhältnismäßig. Die Verwendung von Vorratsdaten sollte auf die Verfolgung von wirklich schweren Straftaten, die die Existenz des Staates gefährden, z. B. terroristische Angriffe, oder Verbrechen gegen Leib und Leben von Personen, beschränkt werden.

---

[537] *„BIM-Entwurf der Vorratsdatenspeicherung in Begutachtung“*, Veröffentlichung des Ludwig Boltzmann Institutes für Menschrechte unter http://bim.lbg.ac.at/de/informationsgesellschaft/bimentwurf-zur-vorratsdatenspeicherung-begutachtung, letzte Abfrage 17.04.2012.

Bei der Erfassung von Vorratsdaten von Personen, die von Amts wegen zur Verschwiegenheit verpflichtet sind, müssten geeignete Mechanismen geschaffen werden, die einen Zugriff der Behörden auf diese Daten verhindern, z. B. dadurch, dass diesem Personenkreis die Möglichkeit gegeben wird, der Speicherung ihrer Verkehrsdaten zu widersprechen (Opt-out-Verfahren). Damit könnten diese ihrer Verpflichtung zur Verschwiegenheit entsprechen und ihre Gesprächsteilnehmer schützen. Ohne eine solche Regelung sind schwerwiegende Grundrechtseingriffe bei den Gesprächspartnern zu befürchten, die auf die Amtsverschwiegenheit ihres Kommunikationspartners vertrauen.

11. Zusammenfassung und Schlussfolgerungen

Die in den vorstehenden Kapiteln vorgenommenen Untersuchungen des Datenschutzes in der öffentlichen Verwaltung lassen sich in zwei Bereiche unterteilen.

Zum einen geht es in den Gebieten E-Government, Bildungs- und Gesundheitswesen sowie Registerzählung um umfangreiche Datensammlungen für die Aufgaben, die sich aus Sicht der Verwaltung in diesen Feldern stellen.

Bei der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung und der Abwehr von Gefahren ist eine durch die so genannte erweiterte Gefahrenforschung bei der Sicherheitspolizei, § 21 Abs. 3 SPG, und die Identifizierung möglicher Gefahrenquellen mittels Arbeitsdateien bei Europol, Art. 14 Europolstatut[538], eine Vorverlagerung der Polizeiarbeit gegenüber der traditionellen Abwehr erkannter und bestehender Gefahren durch die Sicherheitsorgane festzustellen.

11.1 Untersuchungsergebnisse Allgemeine Verwaltung

Als Ergebnis der Untersuchungen des EGovG, des BilDokG, des Registerzählungsgesetzes und des Entwurfes zum GTelG lässt sich eine Tendenz zu einer umfangreichen und dauerhaften Speicherung personenbezogener Daten der Bürger feststellen. Eine Auswertung der im Rahmen der genannten Gesetze erhobenen Daten würde die Erstellung von Persönlichkeitsprofilen erlauben. Zwar werden die Daten überwiegend nur indirekt personenbezogen gespeichert, aber sie sind im Bedarfsfall regenerierbar. Auch indirekt personenbezogene Daten sind zumindest nach europäischem Recht genauso geschützt wie die direkt personenbezogene, so dass z.B. die in Anwendung des BilDokG und des Registerzählungsgesetzes erzeugten Datensammlungen ein unzulässige Speicherung auf Vorrat bedeuten.

Man kann der Verwaltung zugutehalten, dass diese Datenerhebungen nicht willkürlich erfolgen. Um die Verwaltung möglichst effizient zu gestalten und die Regierungsarbeit an den Bedürfnissen der Bürger auszurichten, ist es erforderlich, immer mehr über die Bürger, ihre Verhaltensweisen und Vorlieben, zu erfahren. Auch bei den po-

---

[538] Beschluss des Rates vom 06.04.2009 zur Errichtung eines Europäischen Polizeiamts (Europol), ABl. L 121 S. 17 ff. vom 15. 05. 2009.

litischen Parteien besteht ein Interesse an diesen Informationen, um die Politik für die Bürger attraktiv zu gestalten. Das sind legitime Interessen. Soweit diesen Interessen durch Auswertung anonymer statistischer Daten entsprochen wird, bestehen dagegen unter dem Gesichtspunkt des Datenschutzes auch keine Einwendungen. Wenn aber, wie in den Bereichen des Bildungswesens, der Registerzählung und des Gesundheitsschutzes zumindest tendenziell erkennbar, auch auf die individuellen personenbezogenen Daten einzelner Bürger zugegriffen werden soll, um die Systeme zu steuern, erscheint dies bedenklich. In dem Bereich des Bildungswesens sind diese Bestrebungen zwar nach erheblicher öffentlicher Kritik inzwischen insbesondere durch die Novelle des Bildungsdokumentationsgesetzes im Jahre 2008[539] abgemildert worden, aber die beschriebene Tendenz bleibt auch in dem überarbeiteten Gesetz erhalten. Sie ist im Registerzählungsgesetz gleichfalls erkennbar. Im Gesundheitswesen ist die Diskussion zum Entwurf für ein ELGA-Gesetz (Bundesgesetz betreffend Datensicherheitsmaßnahmen bei der Verwendung elektronischer Gesundheitsdaten – Gesundheitstelematikgesetz 2011, GTelG 2011) z.Zt. noch nicht abgeschlossen.

Es ist erwarten, dass sich die Tendenzen zu extensiven Sammlungen personenbezogener Daten in der öffentlichen Verwaltung aufgrund erkennbarer Entwicklungen eher verstärken als abschwächen werden.

Auch in der öffentlichen Verwaltung werden Methoden des Wissensmanagements eingesetzt.[540] Es ist davon auszugehen, dass dabei auch die in den jeweiligen Verwaltungsorganisationen verfügbaren personenbezogenen Daten von Bürgern mit anderen Informationen und externen Datenquellen zusammengeführt und ausgewertet werden. Im Grunde ist dies bei der Entwicklung zu einer Konzentration der Ansprechpartner für die Bürger (One Stop-Konzept) und zur prozessorientierten Ab-

---

[539] Bildungsdokumentationsgesetz Fassung vom 27.09.2011, http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001727 , letzte Abfrage 19.01.2012

[540] Ebel, Wissensmanagement in der öffentlichen Verwaltung, S. 7: „*In der öffentlichen Verwaltung liegen die Potentiale des Wissensmanagements in der Effizienzsteigerung bei der Bewältigung von komplexen Verwaltungsprozessen, wie bei Genehmigungsverfahren für Bauten oder Produktionsanlagen. Die Herausforderung besteht mit zunehmendem Druck zur Verschlankung der des Verwaltungsapparates und zur gleichzeitigen Qualitäts- und Leistungssteigerung im Sinne von kompetenten Verwaltungshandeln, das an den Bedürfnissen von Wirtschaft und Bürgern orientiert ist.*“, http://www.hfv-speyer.de/hill/Lehrangebot/Sommersemester-2004/Kommunikation/Referate/Ebel-Referat.pdf , letzte Abfrage 19.01.2012

wicklung von Verwaltungsprozessen über Behördengrenzen[541] hinaus auch unvermeidbar. Wichtig ist dabei, dass die Prozesse und die dafür eingesetzten Systeme so gesteuert werden, dass die jeweiligen öffentlichen Angestellten nur Zugriff auf die Informationen erhalten, die sie für die konkrete Aufgabenstellung benötigen. Das wäre ein Weg, um trotz umfangreicher Datensammlungen Datenschutz zu gewährleisten. Darüber hinaus muss sichergestellt sein, dass Zweck, zu dem personenbezogene Daten verarbeitet werden, nach der derzeitigen Rechtslage (Art. 6 Abs. Buchst. b DSRL, § 6 Abs. 1 Ziffer 2 DSG 2000) zumindest mit dem Zweck, zu dem sie ursprünglich erhoben worden sind, vereinbar ist. Andernfalls wird das Grundrecht auf Datenschutz gemäß § 1 DSG 2000 ausgehöhlt. Wenn vom Bürger für einen bestimmten Zweck einmal erhobene personenbezogene Daten seitens der Verwaltung für beliebige andere Zwecke weiterverarbeitet werden können, ist für den Bürger die Verwendung seiner Daten nicht mehr überschaubar, so dass er sich gegen einen denkbaren Missbrauch auch nicht zur Wehr setzen kann und damit in seinem Recht beeinträchtigt wird, über die Verwendung seiner Daten selbst zu entscheiden.

Insoweit zeichnet sich allerdings zumindest in der Rechtsprechung eine Entwicklung von dem stark interpretationsfähigen Begriff der „Vereinbarkeit“ in Richtung einer konkreten und engen Zweckbindung im Sinne der Rechtsprechung des deutschen Bundesverfassungsgerichtes[542] ab. Danach setzt jede Datenverwendung im öffentlichen Bereich voraus, dass der Zweck gesetzlich bestimmt ist und die Daten dafür auch erforderlich sind. Die Verwendung für unbestimmte und nicht bestimmbare Zwecke wäre danach unzulässig. Der EuGH hat in seiner Entscheidung Huber gg.

---

[541] Siehe dazu Lück-Schneider, Dovifat, Klischewski, Wimmer, „Einführung zum Schwerpunkt in wissensbasiertes Prozessmanagement in Verwaltungsnetzwerken“ in Schweighofer/Kummer (Hrsg.) Europäische Projektkultur als Beitrag zur Rationalisierung des Rechts, Tagungsband IRIS 2011, S. 361 ff..

[542] BVerfG 65, S.1 ff. (S. 23), *„Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten und oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren. Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum erreichendes angegebenen Zieles erforderliche Minimum beschränken müssen. Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein – amtshilfefester – Schutz gegen Zweckentfremdung durch Weitergabeverbote und Verwertungsverbote erforderlich.“*, http://www.thm.de/datenschutz/images/stories/volkszaehlungsurteil_bverfger_1983.pdf , letzte Abfrage 19.01.2012.

Deutschland vom 18.12.2008[543] zum Ausländerzentralregister u.a. entschieden, dass nur Daten erhoben werden dürfen, die für den Aufenthalt von Ausländern relevant sind und darauf nur Behörden zugreifen dürfen, die für diesen Bereich eine gesetzliche Zuständigkeit besitzen; nur dann sei das Kriterium der Erforderlichkeit im Sinne von Art 7 Buchst. e DSRL gegeben. Der VfGH betont gleichfalls eine enge Zweckbindung. Im Rahmen einer Entscheidung über die Zulässigkeit automatischer Geschwindigkeitsmess-Systeme hat er mit Hinweis auf § 6 Abs. 1 Ziffer 2 DSG 2000 betont, dass personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke eingesetzt werden dürfen. Da das DSG 2000 von einer strengen Zweckbindung der Ermittlung und Verwendung von Daten ausgehe, dürften auch durch automatische Geschwindigkeitsmess-Systeme ausschließlich zur Feststellung der Überschreitung einer ziffernmäßig festgelegten Höchstgeschwindigkeit ermittelt und verwendet werden.[544] Auch der EGMR hat die Zweckbindung bei Datenverwendungen betont. In einer Entscheidung der großen Kammer des Gerichtshofes, Marper gg. Vereinigtes Königreich[545], hat dieser seine Rechtsprechung zum Datenschutz zusammengefasst und u. a. ausgeführt, dass innerstaatliche Recht solle sicherstellen, dass personenbezogene Daten für die Zwecke, für die sie gespeichert werden, erheblich sind und nicht darüber hinausgehen, und dass sie insbesondere in einer Form aufbewahrt werden, welche die Identifizierung der Betroffenen nur solange erlaubt, wie dies für den Zweck, zu dem sie gespeichert worden sind, erforderlich ist. Das innerstaatliche Recht müsse auch angemessene Garantien gegen eine falsche und missbräuchliche Verwendung aufbewahrter personenbezogener Daten vorsehen.[546]

Auch die EU-Kommission hat erkannt, dass die Zweckbindung bei der Verwendung personenbezogener Daten ein zentrales Element des Datenschutzes darstellt. In ihrem Gesamtkonzept für den Datenschutz in der Europäischen Union vom 04. November 2010 bezeichnet sie die Zweckbindung und die Kontrolle der Betroffenen

---

[543] EuGH-Urteil vom 18.12.2008, Huber gg. Deutschland, Rs. C524/06 Rd.-Nr. 59 und 61, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006CJ0524:DE:HTML, letzte Abfrage 19.01.2012.
[544] Urteil des VfGH vom 15.06.2007, Geschäftszahl: G 147/06, http://www.ris.bka.gv.at/Dokumente/Vfgh/JFR_09929385_06G00147_01/JFR_09929385_06G00147_01.pdf , letzte Abfrage am 19.01.2012.
[545] Urteil des EGMR vom 04.12.2008, Marper gg. Vereinigtes Königreich, EuGRZ 2009, S. 299 ff.
[546] EGMR aaO. S. 311

über ihre Daten als zwei Hauptziele ihrer Initiativen zu einer Verbesserung des Datenschutzes in der Europäischen Union.[547] Zwei wichtige Voraussetzungen für ein hohes Datenschutzniveau seien, dass der für die Datenverarbeitung Verantwortliche Daten nur zu ganz bestimmten Zwecken verarbeiten dürfe (Prinzip der Datensparsamkeit) und der von der Verarbeitung Betroffene weiterhin die Kontrolle über seine eigenen Daten habe. Bedauerlicherweise hat die Kommission diese Ziele bei der Ausarbeitung von konkreten Vorschlägen für eine Novellierung des Datenschutzes in der EU etwas aus den Augen verloren. Sowohl bei der geplanten Verordnung als Ersatz für die Richtlinie 95/46/EG und der geplanten Richtlinie für den Datenaustausch in der polizeilichen Zusammenarbeit zwischen den Mitgliedstaaten wird ausdrücklich auf die zur Zeit bestehenden und zunächst als unzulänglich empfundenen Regelungen zur Zweckbindung zurückgegriffen. In ihrem Gesamtkonzept für den Datenschutz in der EU hatte die Kommission zunächst kritisch bemerkt, dass der 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 350 vom 30.12.2008, S. 60) zu viele Ausnahmen vom Zweckbindungsprinzip aufweise.[548] In ihrem Vorschlag für eine „Richtlinie 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“[549] ist aber keine Tendenz zu einer strengeren Zweckbindung zu erkennen. In Art. 4 des Vorschlages heißt es:

„*Die Mitgliedstaaten tragen dafür Sorge, dass personenbezogene Daten*

a) nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;

b) für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen;“

---

[547] 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, KOM(2010) 609 endgültig, S. 8 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf, letzte Abfrage 19.01.2012.

[548] Siehe Gesamtkonzept aaO. S. 15.

[549] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_de.pdf, letzte Abfrage 31.01.2012

In der Begründung zu Art. 4 des Richtlinienvorschlages wird darauf verwiesen, dass die Bestimmung die für die Verarbeitung von personenbezogenen Daten geltenden Grundsätze entsprechend Artikel 6 der Richtlinie 95/46/EG sowie Art. 3 des Rahmenbeschlusses 2008/977/JI enthalte. Es bleibt also alles beim Alten.

Auch in der geplanten Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)[550] findet sich in Art. 5 eine dem Art. 4 des Richtlinienvorschlages entsprechende Regelung. In der Begründung wird gleichfalls auf die in Art. 6 der Richtlinie 95/46/EG niedergelegten Grundsätze Bezug genommen (siehe Ziffer 3.4.2 der Begründung zum Verordnungsvorschlag). In Art 6. Abs. 4 des Entwurfs zur Datenschutz-Grundverordnung findet sich folgende Regelung:

„Ist der Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten erhoben wurden, nicht vereinbar, muss auf die Verarbeitung mindestens einer der in Absatz 1 Buchstaben a bis e genannten Gründe zutreffen.“

In Abs. 1 der Bestimmung heißt es u. a., eine Verarbeitung sei rechtmäßig, wenn

c) die Verarbeitung zur Erfüllung einer gesetzlichen Verpflichtung erforderlich ist, der der für die Verarbeitung Verantwortliche unterliegt;

e) die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt und die dem für die Verarbeitung Verantwortlichen übertragen wurde.

Im Ergebnis würden diese Vorschriften, die im Falle eines Inkrafttretens der Verordnung in den Mitgliedsländern unmittelbar anzuwenden wären, bedeuten, dass im Anwendungsbereich der Verordnung die Behörden im Rahmen ihrer gesetzlichen Aufgabenstellung auch Daten verarbeiten dürfen, die von anderen Behörden für ganz andere Zwecke erhoben worden sind.

Die als Ersatz für die DS-RL geplante Verordnung würde den Verwaltungsbehörden eine viel weiter gehende Nutzung von Datenbeständen erlauben als dies nach den bisher geltenden Regelungen der Richtlinie 95/46/EG möglich ist und würde bedeuten, dass Bürger sich gegen verwaltungsinterne Weitergabe von Daten grundsätzlich nicht wehren können. Das Konzept des EGovG, das mit der Aufteilung in verschie-

---

[550] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, letzte Abfrage am 31.01.2012

dene Tätigkeitsbereiche auch den Zugriff auf die jeweiligen Datenbestände eingrenzt, wäre wohl überholt.
Unter Berücksichtigung der beschriebenen Rechtsprechung der höchsten nationalen und europäischen Gerichte sowie den von der EU-Kommission mit der DSRL gewonnenen Erfahrungen ist die Forderung gerechtfertigt, dass auch in der öffentlichen Verwaltung erhobene Daten nur für die Zwecke verwendet werden dürfen, für die sie erhoben worden sind, selbst wenn dies Rationalisierungsbestrebungen in der Verwaltung behindert. Die Optimierung von Verwaltungsabläufen darf nicht zu einer Einschränkung des Datenschutzes führen. Letzterem gebührt Vorrang. Dieser Grundsatz darf auch nicht im Wege der Amtshilfe umgangen werden, wenn dies dazu führt, dass Daten abweichend vom ursprünglichen Erhebungszweck verwendet werden.

11.2 Untersuchungsergebnisse Sicherheitsbehörden

In den Kapiteln 8 und 9 ist beschrieben worden, dass die nationalen und europäischen Sicherheitsbehörden über weitreichende Möglichkeiten der Informationsbeschaffung und damit verbunden auch die Verwendung personenbezogener Daten verfügen. Durch die Vorverlagerung polizeilicher Ermittlungstätigkeit zur Erkenntnis nicht nur konkreter, sondern auch potentieller Gefahren werden zunehmend auch Bürger Gegenstand von Untersuchungen, bei denen kein konkreter Verdacht besteht, eine Straftat begangen zu haben. Dies ist z.B. bei der Zugehörigkeit zu einer Gruppe der Fall, von der aufgrund entsprechender Vermutungen der Sicherheitsorgane bestimmte Gefahren ausgehen. Umstrittenes Instrument ist in diesem Zusammenhang die Vorratsdatenspeicherung. Die Verpflichtung des Staates, für die Sicherheit der Bürger zu sorgen, Art. 78 a B-VG, kollidiert mit dem Interesse der Bürger an der Aufrechterhaltung der persönlichen Freiheit, der Unversehrtheit der Privatsphäre und dem Schutz personenbezogener Daten sowie der Verpflichtung des Staates, diese Grundrechte zu gewährleisten und zu schützen. Der Staat ist gehalten, durch geeignete Maßnahmen nach Möglichkeit Verletzungen der Grundrechte zu verhindern und ggf. zu unterbinden.[551] Freiheit und Sicherheit stehen aber nicht unabhängig nebeneinander. Absolute Freiheit würde in Anarchie enden. Im Interesse der Gesamtheit der Bürger sind deshalb Einschränkungen der Freiheit durch Geset-

[551] Grabenwarter, Europäische Menschenrechtskonvention, 4. Auflage 2009, S. 126,127

ze erforderlich, deren Befolgung durch den Staat zu gewährleisten ist. Es wird also etwas Freiheit für die Sicherheit hergegeben. *„Der Kulturmensch hat ein Stück Glücksmöglichkeit gegen ein Stück Sicherheit getauscht“*, sagt Sigmund Freund.[552] Damit entsteht das Problem, wie viel Freiheit für die Sicherheit getauscht werden muss.

Dafür ist zunächst zu klären, was unter „Sicherheit“ zu verstehen ist. Der Staatsphilosoph Thomas Hobbes (1679-1788) hat den Menschen als egoistisches Wesen (homo homini lupus) gesehen, welcher grundsätzlich nach der Vermehrung seiner materiellen Güter ohne Rücksicht auf die Interessen anderer strebe, was zum Krieg aller gegen alle (bellum omnium contra omnes) führen könne. Der Staat wird als Institution angesehen, die auch die Bedürfnisse der Menschen nach Rechtsschutz, Sicherheit und Selbsterhaltung gewährleistet.[553] Seit Montesquieu und der von ihm entwickelten Lehre der Gewaltenteilung[554] geht es auch um die Frage der Begrenzung staatlicher Macht, nach Schutz gegen Übergriffe staatlicher Macht in die Privatsphäre der Bürger.[555] Die derzeitige verfassungsrechtliche Entwicklung ist vom Sozialstaatsgedanken geprägt. Die soziale Absicherung der Menschen und die Erhaltung der Lebensgrundlagen werden als weitere Sicherungsaufgabe des Staates angesehen.[556] Der moderne Staat der Neuzeit habe seine Rechtfertigung in der Gewährleistung von Sicherheit und zunehmend auch dann von Freiheit gefunden, erläuterte der frühere Präsident des deutschen Bundesverfassungsgerichts, Hans-Jürgen Papier, 2007 in einem Vortrag. Wie die Sicherheitsbedürfnisse hätten sich auch die Vorstellungen von Freiheit weiterentwickelt. Beide Elemente ließen sich nur bezogen aufeinander

---

[552] Freud, Das Unbehagen in der Kultur, 1930, S. 86, http://www.archive.org/stream/DasUnbehagenInDerKultur/Freud_1930_Unbehagen_in_der_Kultur#page/n5/mode/2up. letzte Abfrage 19.01.2012.
[553] Möller, Kurzbeschreibung der Philosophie Hobbes', http://philolex.de/hobbes.htm , letzte Abfrage 19.01.2012
[554] Charles de Montesquieu (1689-1755), http://www.raffiniert.ch/smontesquieu.html, letzte Abfrage 19.01.2012.
[555] Glaeßner, Sicherheit und Freiheit, S. 7, https://www.social-science.hu-berlin.de/lehrbereiche/innenpolitik/Sicherheit/apuz.pdf, letzte Abfrage 19.01.2012.
[556] Glaeßner, aaO, S. 8,

nachvollziehen. Das gelte nicht nur für die historische Entwicklung, sondern auch für das gegenwärtige Verhältnis zueinander.[557]

Durch den internationalen Terrorismus und die Verbreitung organisierter Kriminalität sind für die Staaten neue Sicherheitsaufgaben entstanden. Im Hinblick auf das Gewicht dieser Gefahren besteht das Bestreben, diese möglichst frühzeitig zu erkennen und nicht erst dann einzuschreiten, wenn der Angriff auf Rechtsgüter stattgefunden hat oder unmittelbar bevorsteht, sondern bereits im Vorfeld der möglichen Straftaten. Gegenüber dem traditionellen Polizeirecht, dadurch gekennzeichnet, dass für einen Eingriff eine konkrete Gefährdungslage bestehen muss, besteht das Bestreben, den Eingriffszeitpunkt vorzuverlegen und aufgrund von Vermutungen über mögliche künftige Tatabläufe und Täterkreise Ermittlungshandlungen zu rechtfertigen. Kennzeichnend dafür sind die Maßnahmen nach § 53, 53 a, 54 SPG im Rahmen der erweiterten Gefahrenforschung (§§ 21 Abs. 3, 53 Abs. 1 Ziffer 2a, 54 Abs. 2 Ziffer 1 SPG), also Ermittlung personenbezogener Daten auch ohne Vorliegen eines konkreten Tatverdachtes, u.a. Auswertung von Verkehrsdaten der Kommunikation und verdeckte Ermittlungen auch durch Nutzung von Ton-und Bildaufzeichnungsgeräten. Wie in Kapitel 10beschrieben, ist ab 01.04.2012 in Österreich auch die Vorratsdatenspeicherung eingeführt worden. Mit diesen Maßnahmen sind einerseits massive Grundrechtseingriffe, insbesondere auf den Anspruch auf Geheimhaltung personenbezogener Daten nach § 1 Abs. 1 DSG 2000, verbunden. Andererseits sind die genannten Ermittlungsmethoden, wie insbesondere das Beispiel „Europol“ verdeutlicht, durchaus erfolgreich. In der zunehmenden Ausweitung sicherheitspolizeilicher Befugnisse liegt jedoch die Gefahr, dass die Freiheit der Bürger, darunter auch die Freiheit, über die Verwendung ihrer personenbezogenen Daten selbst zu entscheiden, immer mehr eingeschränkt wird. Mit der Zunahme der Datenmengen steigt auch die Gefahr des Missbrauchs. Immer wieder wird in der Presse über derartige Fälle berichtet.[558]

---

[557] Papier, Freiheit versus Sicherheit- Die schwierige Balance zwischen Freiheit und Sicherheit in Zeiten des Terrorismus, http://www.kow-reflexionen.de/wp-content/uploads/2008/01/2007_1210_papier_vortrag.pdf, letzte Abfrage 19.01.2012.

[558] Unerlaubte EKIS-Abfrage durch Polizisten, http://stmv1.orf.at/stories/122478, Illegale EKIS-Abfrage, http://www.kleinezeitung.at/steiermark/leoben/2293002/illegale-ekis-abfrage-fpoe-unter-druck.story, letzte Abfrage am 19.01.2012.

Über die erforderliche Grenzziehung, wo Sicherheitsmaßnahmen im Interesse der Aufrechterhaltung der Freiheit zu unterbleiben haben, kann man unterschiedliche Auffassungen vertreten. Soweit bekannt, haben österreichische Obergerichte noch nicht umfassend zu dieser Problematik entschieden. Vermutlich wird die verdachtsunabhängige Speicherung von Verkehrsdaten der elektronischen Kommunikation dazu einen Anlass geben. In jedem Fall lassen sich aus der EMRK und der Rechtsprechung des EGMR zu Eingriffen in das Brief- und Fernmeldegeheimnis und zu geheimen Überwachungsmaßnahmen[559] Anhaltspunkte für zulässige sicherheitspolizeiliche Präventionsmaßnahmen entnehmen. Eingriffe in die Privatsphäre seitens der Sicherheitsbehörden setzen das Bestehen eines auf tatsächliche Anhaltspunkte begründeten Verdachts voraus, das jemand eine schwerwiegende Straftat plant. Der Gerichtshof erkennt an, dass die Entwicklung des internationalen Terrorismus eine zunehmende Bedrohung demokratischer Gesellschaften darstellt und dass der Staat in der Lage sein muss, derartigen Gefährdungen wirksam zu begegnen. Dazu wird dem Staat ein gewisser Ermessensspielraum eingeräumt. Dieser sei jedoch nicht unbegrenzt. Die Maßnahmen dürften nicht so weit gehen, dass die Demokratie, mit dem Vorwand sie zu verteidigen, letztendlich untergraben werde. Die Gesetze, die derartige Maßnahmen vorsehen müssten hinreichend klar und bestimmt sein und ausreichende Vorkehrungen gegen Missbrauch vorsehen.

Daraus kann man den Schluss ziehen, dass Maßnahmen zur Aufrechterhaltung der inneren Sicherheit das Schutzgut Freiheit nicht völlig untergraben dürfen. In diesem Zusammenhang sei auch eine, Benjamin Franklin zugesprochene Aussage hingewiesen: *„They that can give up Essential Liberty to purchase little Temporary Safety, deserve neither Liberty nor Safety.“*[560] Deshalb sollten Ermittlungen im Vorfeld traditioneller Strafverfolgung, sogenannte proaktive Informationsbeschaffung und Auswer-

---

[559] Urteil des EGMR vom 06.09.1978, Klaas u.a. gg. Deutschland, Ziffer 48 ff., EuGRZ 1979, S. 278ff; NJW 1979, S. 1755 ff; Urteil des EGMR vom 25.03.1998, Kopp gg. Schweiz, Ziffer 62 ff., ÖJZ 1999, S. 115 ff..

[560] Benjamin Franklin - ***“****They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety. This sentence was much used in the Revolutionary period. It occurs even so early as November, 1755, in an answer by the Assembly of Pennsylvania to the Governor, and forms the motto of Franklin's 'Historical Review,' 1759, appearing also in the body of the work. Frothingham, Rise of the Republic of the United States, p. 413.*“
http://www.famousquotes.com/category/deserve/, letzte Abfrage 19.01.2012.

tung[561], nur erfolgen, wenn nicht nur Vermutungen, sondern tatsächliche Anhaltspunkte dafür vorliegen, dass wirklich schwerwiegende Straftaten geplant werden, ohne dass zwingend bereits ein konkreter Verdacht gegen eine bestimmte Person oder Personengruppe vorliegen muss. Als schwerwiegende Straftaten kommen Terrorismus, organisierte Kriminalität und Verbrechen gegen das Leben in Betracht (§§ 274 ff. StGB). Die entsprechenden Ermittlungshandlungen sollten, außer bei Gefahr im Verzuge, unter dem Vorbehalt einer richterlichen Zustimmung stehen.

Unter Berücksichtigung dieser Anforderungen erscheinen die im SPG vorgesehenen Maßnahmen zur erweiterten Gefahrenforschung und die in Österreich jetzt auch erlaubte Nutzung von so genannten Vorratsdaten der elektronischen Kommunikation als zu weitgehend.

Zusammenfassend wird festgestellt, dass moderne Verwaltung und Datenschutz nicht zwangsläufig einen Widerspruch darstellen, aber Tendenzen zur Ausforschung der Bürger im Interesse der Rationalisierung der Verwaltungsabläufe und der Politikgestaltung entgegen getreten werden muss. Im Bereich der inneren Sicherheit sind die Eingriffe in die Privatsphäre auf schwerwiegende Ausnahmefälle zu beschränken.

---

[561] Glaeßner, Sicherheit und Freiheit, S. 11, https://www.social-science.hu-berlin.de/lehrbereiche/innenpolitik/Sicherheit/apuz.pdf, letzte Abfrage 19.01.2012.

Literaturverzeichnis:

Adamovic,Funk,Holzinger, *Österreichisches Staatsrecht, Bd. 2, Springer-Verlag Wien 1998.*

Aden in *Rogan (Hrsg.), Handbuch zum Recht der inneren Sicherheit, Berliner Wissenschafts-Verlag, 2. Aufl. Berlin 2006 .*

Audersch, L., *Datenschutzgerechtes Workflow-Management bei Mehrfachanträgen in ämterübergreifenden Verwaltungsprozessen, in Hochberger/Liskowsky (Hrsg.) Informatik 2006 - Informatik für Menschen Bd. 2, Gesellschaft für Informatik, Bonn 2006.*

Buchinger, *Die Elektronische Gesundheitsakte in Österreich, in Jahnel (Hrsg.) Datenschutzrecht und E-Government 08, Neuer Wissenschaftlicher Verlag, Wien-Graz 2008.*

Dohr,Pollirer,Weiss,Knyrim, *Datenschutzrecht Kommentar,Manz`sche Verlagsbuch-handlung, 2. Aufl. Wien 2002, Loseblattslg. Stand Dez. 2011*

Duschanek, *in Korinek/Holoubek, Österreichisches Bundesverfassungsrecht Bd. III, Springer-Verlag Wien, 7. Lfg. 2005*

Eisner. (2004). *Die Schrankenregelung der Grundrechtscharta der Europäischen Union, Nomos-Verlag Baden-Baden 2005*

Férérvàry,*Europäisierung der Polizeiarbeit“ in Férérvàry/Stangl, Polizei zwischen Europa und den Regionen, facultas wuv universitätsverlag Wien 2001*

Flendrovsky, *Datenverwendung und Datenschutz in der allgemeinen Sicherheitspolizei in Bauer/Reimer, Handbuch Datenschutzrecht, facultas wuv uni-versitätsverlag Wien 2009.*

Forgó,Krügel,Rapp, *Zwecksetzung und informationelle Gewaltenteilung, Nomos Vwerlagsgesellschaft Baden-Baden 2006.*

Frohner . (2009), *Datenschutz im Gesundheitswesen in Bauer/Reimer (Hrsg.), Handbuch Datenschutzrecht, facultas wuv universitätsverlag Wien 2009*.

Grabenwarter, *Europäische Menschenrechtskonvention Verlag C.H. Beck München, 4. Aufl. 2009 .*

Grote/Maraun, *EMRK/GG Konkordanzkommentar zum europäischen Grundrechtsschutz, Mohr Siebeck, Tübingen 2006.*

Hauer/Kepplinger. *Sicherheitspolizeigesetz, Kommentar, Linde Verlag Wien, 4. Auflage 2011.*

Hauer/Kepplinger, *Sicherheitspolizeigesetz, Polizeiausgabe, Pro Libris Verlagsgesellschaft, 11.Auflage, Wien 2010 .*

Hinteregger, *Der Schutz der Privatsphäre durch das österreichische Schadensersatzrecht de lege ferenda und de lege lata in Liber amoricum Pierre Widmer,Tort and Insurance Law, Band 10, Springer-Verlag Wien 2003.*

Hoye, *Digitale Identitäten im Kontext von E-Government-Anwendungen, Diplomica Verlag Hamburg 2010.*

Jahnel, *Handbuch Datenschutzrecht, Jan Sramek Verlag, Wien 2010*

Jahnel/Siegwart/Fercher (Hrsg.) *Aktuelle Fragen des Datenschutzrechtes, facultas wuv universitätsverlag Wien 2007.*

Kistner-Bahr,*Die Entwicklungstendenzen Europols im europäischen Integrationsprozess, Dissertation Köln 2010.*

Martino,*Datenschutz im europäischen Recht, Nomos Verlagsgesellschaft Baden-Baden 2005.*

Mayer-Schönberger/Brandl,*Datenschutzgesetz, Linde Verlag Wien, 2. Aufl. 2006.*

Priglinger. (2008). *Auswirkungen der EU-DL Richtlinie auf die E-Gov-Welt in Jahnel (Hrsg.), Jahrbuch Datenschutzrecht und E-Government 08, Neuer Wissenschaftlicher verlag Wien-Graz 2008.*

Raschauer, *Datenschutzrecht 2010, Jan Sramek Verlag Wien 2011*

Ruffert , „*Grundrecht der Berufsfreiheit*“, *in Ehlers (Hrsg.), Europäische Grundrechte und Grundfreiheiten, De Gruyter Rechtswissenschaften Verlag Berlin, 3. Aufl. 2009.*

Schäffer, „*Die Entwicklung der Grundrechte“, in Mertens/Papier, Handbuch der Grundrechte, Bd. VII/1 Grundrechte in Österreich, Manz Wien 2009*

Schenke *„Rechtsschutz gegen Europol“ in Wolter/Schenke/Hilger/Ruthig/Zöller (Hrsg.) Alternativentwurf Europol und europäischer Datenschutz, C.F. Müller Verlag Heidelberg 2008.*

Schliesky, *Die Europäisierung der Amtshilfe, Richard Boorberg Verlag Stuttgart 2008.*

Schorkopf, „Höchstpersönliche Rechte“, *in Ehlers (Hrsg.), Europäische Grundrechte und Grundfreiheiten, De Gruyter Rechtswissenschaften Verlag Berlin, 3. Aufl. 2009.*

Schubert, *Europol und der virtuelle Verdacht – Die Suspendierung des Rechts auf informationelle Selbstbestimmung,Verlag Peter Lang Frankfurt 2007.*

Schweighofer, „Strukturdenken und Modellbindung im Recht“, in Traunmüller/Wimmer (Hrsg), *Informatik in Recht und Verwaltung: Gestern – Heute – Morgen, Ehrenband für Prof. Fiedler zum 80. Geburtstag, Bonn GI 2010*

Schweizer/Müller*Zwecke, Möglichkeiten und Grenzen der Gesetzgebung im Polizeibereich, Schweizerische Bundeskanzlei, Heft 3 Leges 2008.*

Siemen, *Datenschutz als europäisches Grundrecht, Duncker & Humblot Berlin 2006.*

Tettinger/Stein *Kölner Gemeinschaftskommentar zur Europäischen Grundrechtecharta, C.H. Beck München 2006.*

Thanner/Vogl. (4. Aufl. 2010). *Sicherheitspolizeigesetz, Neuer Wissenschaftlicher verlag Wien-Graz 2010 .*

Traunmüller/Wimmer (Hrsg.), *Informatik in Recht und Verwaltung: Gestern – Heute – Morgen, Ehrenband für Prof. Fiedler zum 80. Geburtstag, GI Bonn 2010.*

Uerpmann-Wittzak, *„Höchstpersönliche Rechte und Diskriminierungsverbot",in Ehlers (Hrsg.), Europäische Grundrechte und Grundfreiheiten, De Gruyter Rechtswissenschaften Verlag Berlin, 3. Aufl. 2009.*

Wettner, *Die Amtshilfe im Europäischen Verwaltungsrecht, Mohr Siebek Verlag Tübingen 2005.*

Wiederin*, Privatsphäre und Überwachungsstaat, Manz Wien 2003.*

Wiederin, S. d. (2009). „*Schutz der Privatsphäre" in Merten/Papier,Handb. d. Grundrechte Band VII/1 Grundrechte in Österreich, Manz Wien 2009.*

Wildhaber/Breitenmoser,*in Karl (Hrsg.) Internationaler Kommentar zur Europäischen Menschenrechtskonvention, Heymann Verlag Köln 1986 Los Blattsmlg. (Stand 2010).*

Winter,Makolm,Weiß, „*Die Rückwirkung von Werkzeugeinsatz auf die Kultur: Wie Informationstechnik unsere Wissens- und Rechtskultur verändert", in* Traunmüller/Wimmer (Hrsg.), *Informatik in Recht und Verwaltung: Gestern – Heute – Morgen, Ehrenband für Prof. Fiedler zum 80. Geburtstag, GI Bonn 2010.*

Yildirim, *Datenschutz im Electronic Government, Deutscher Universitätsverlag Wiesbaden 2004.*

Anhang

Egmar Wolfeil

Lebenslauf und beruflicher Werdegang

Geburtsdatum:	05. Juli 1939
Geburtsort:	Berlin
Familienstand:	verheiratet, 2 Kinder
Schulabschluss:	1959 Abitur am Hans-Thoma-Gymnasium in Berlin-Hermsdorf
Universität:	1959 - 1961 Studium der Rechtswissenschaften an der Freien Universität Berlin 1961 bis 1964 Fortsetzung des Studiums an der Philipps-Universität in Marburg/Lahn
Ausbildung:	1965 - 1968 Referendar in Wiesbaden Januar - Mai 1974 Post-Educational Degree in Business Administration, PED VI IMEDE, L'Institute pour L'Etude des Methodes de L'Entreprise (heute IMD, International Institute for Management Development) in Lausanne/Schweiz
Berufspraxis:	1968 - 1975 Justitiar der Fa. Gebr. Knauf Westdeutsche Gipswerke, ein Unternehmen der Baustoffindustrie 1975 bis 1989 Justitiar bei der Salzgitter Industriebau GmbH, einer Gesellschaft des Salzgitter-Konzerns 1990 - 1992 Kaufmännischer Geschäftsführer der Salzgitter Industriebau GmbH 1993 bis 2003 Kaufmännischer Geschäftsführer der Telcat Kommunikationstechnik GmbH und seit 1995 auch der Telcat Multicom GmbH. Beide Gesellschaften gehören zum Salzgitter-Konzern

Weiterbildung 2009 bis heute
Doktorstudium an der Universität Wien. Neben Teilnahme an Seminaren Vorträge mit dem Schwerpunkt Datenschutz auf dem Internationalen Rechtsinformatik Symposium in Salzburg in 2011 und 2012

Braunschweig, im Juni 2012