Datenschutzbericht

2005 - 2007

Impressum: Medieninhaber, Herausgeber und Redaktion: Datenschutzkommission (DSK, Bundesbehörde gemäß §§ 35ff DSG 2000), Ballhausplatz 1, 1014 Wien.
Kontakt: dsk@dsk.gv.at
Website: http://www.dsk.gv.at
RIS-Entscheidungsdokumentation der DSK: http://www.ris.bka.gv.at/dsk/

Zusammenfassender Überblick

Geschäftsgang

Der Arbeitsanfall bei der DSK sah im Berichtszeitraum wie folgt aus:

1. Es wurden rund 550 **Beschwerden** erhoben, von welchen etwas weniger als die Hälfte in förmlichen Bescheidverfahren abzuhandeln war, während der Rest im – relativ formlosen – Ombudsmannverfahren erledigt werden konnte (vgl. hiezu das Kapitel 4.2).

1.1 Bei der Erledigungsdauer der Beschwerdeverfahren konnte die DSK – erstmals in ihrer Geschichte – eine maximale 6-Monatsfrist weitestgehend einhalten und in vielen Fällen auch unterschreiten (vgl. im Kapitel 4.2. die Graphiken über die Verfahrensdauer).

1.2. Von den Beschwerden waren am häufigsten die Verwendung von Bonitätsdaten bei Kreditauskunfteien oder Inkassobüros und die Datenverwendung im Rahmen kriminalpolizeilicher Ermittlungen betroffen; daneben haben eine Reihe von Beschwerden die Löschung von Daten bei Polizeidienststellen als Folge der Aufhebung des § 209 StGB begehrt; auch die internationale Amtshilfe in Verkehrsstrafsachen war mehrfach Gegenstand von Beschwerden. Die Anzahl der Beschwerden über den Direktmarketingbereich sind im Berichtszeitraum stark zurückgegangen (vgl. hiezu die Kapitel 6.1. und 6.2.).

1.3. Die DSK hat im Zusammenhang mit Beschwerden 11 **Empfehlungen** nach § 30 Abs. 6 DSG 2000 an Auftraggeber zur Herstellung des rechtmäßigen Zustands bei Datenanwendungen erlassen, die u.a. Folgendes betrafen:

- die Verwendung von Bonitätsdaten,
- die Verwendung der Sozialversicherungsnummer bei der Lehrerfortbildung,
- die zulässige Speicherdauer von (dynamischen) IP-Adressen,
- die Mitteilung der Führerscheinabnahme an den Arbeitgeber,
- die Einholung von (gesetzwidrigen) Zustimmungserklärungen zur Übermittlung von Behandlungsdaten durch Spitälern an private Versicherungsunternehmen,
- die Ermittlung von Daten zur führerscheinrechtlichen Verlässlichkeitsprüfung aus polizeilichen Unterlagen.

2. In etwa 1000 Fällen ersuchten Bürger schriftlich um **Rechtsauskunft** zu konkreten Problemen mit Datenschutzbezug – die Zahlen der telefonischen Rechtsauskunftsbegehren liegen noch weit höher.

3. Im Datenverarbeitungsregister, das ein Teil der DSK ist, wurden etwa 6000 **Meldungen** über neue Datenanwendungen eingebracht, wovon aber nur in etwa 100 Fällen besondere Auflagen erteilt werden mussten (vgl. Kapitel 8.2.).

Die signifikantesten Rechtsprobleme im DVR im Berichtszeitraum waren:

- die Schaffung von Systemen zur integrierten Patientenversorgung,
- die Schaffung von Informationsverbundsystemen zur Beurteilung des Kreditrisikos von Personen und
- die Videoüberwachung.

Im ANHANG zum Datenschutzbericht werden die **Leitlinien** dargestellt, die vom DVR bei der Registrierung von Meldungen **über Videoüberwachung im privaten Bereich** angewendet werden.

4. (Amtswegige) Prüfverfahren nach § 30 Abs. 2 und 3 DSG 2000 wurden im Berichtszeitraum v.a. im Bereich der Kreditauskunfteien und Inkassobüros durchgeführt.

5. **Genehmigungen** für den Export von personenbezogenen Daten in Länder außerhalb der EU wurden in etwa 100 Fällen beantragt.

6. Im Bereich der **EU-Zusammenarbeit** (vgl. Kapitel 7) in der sog. „Art. 29-Gruppe“ in Brüssel, an der sich die DSK sehr aktiv beteiligt, werden alle aus europäischer Sicht aktuellen Datenschutzfragen beraten, wobei die Ergebnisse z.T in so genannten Working Papers (WP) veröffentlicht werden. Aus jüngster Zeit stammt etwa WP 131, das die daten-

schutzrechtliche Beurteilung von Projekten zur umfassenden elektronischen Speicherung von Gesundheitsdaten enthält (zu finden auf der Website der DSK, http://www.dsk.gv.at/).

Im Berichtszeitraum hatte man sich in dieser Arbeitsgruppe v.a. mit der Datenverwendung im Rahmen der Terrorismusbekämpfung auseinanderzusetzen – dies betrifft etwa die Übermittlung von Flugpassagierdaten an die Heimatschutzbehörde der USA, die Speicherung von biometrischen Daten (digitales Photo, Fingerabdrücke) im neuen europäischen Sicherheits-Pass, die verbindliche Telekommunikations-Verkehrsdatenspeicherung über einen mehrmonatigen Zeitraum, oder die Kontrolle von im SWIFT-Netz versendeten europäischen Zahlungsverkehrsdaten durch das US-Finanzministerium. Daneben ergeben sich aus der Internet-Entwicklung wichtige Datenschutzprobleme wie gefälschte Identitäten oder die Speicherung von Daten über das Benutzerverhalten bei Suchmaschinen. Aber auch die allgemeine technologische Entwicklung auf dem IT-Sektor schafft kontinuierlich neue Fragestellungen wie etwa die Einflüsse der RFID-Technologie auf die Nachvollziehbarkeit von menschlichem Verhalten oder die Nutzbarkeit von Geolokalisationssytemen zur Lokalisierung von Menschen z.B. bei Autounfällen („e-call“) etc.

Forderungen an den Gesetzgeber

Aus den Erfahrungen der DSK in den oben dargestellten Tätigkeitsbereichen (vgl. Kapitel 6.3.), ergibt sich ihrer Ansicht nach besonderer **gesetzlicher Handlungsbedarf** in Fragen der

- Sammlung und Verwendung von Bonitätsinformationen,
- Videoüberwachung, insbesondere soweit sie von Privaten durchgeführt werden soll,
- Herausgabe von Daten über Internet-Kommunikationen, insbesondere auch im Zusammenhang mit der Vorratsdatenspeicherung,
- Übermittlung von Behandlungsdaten von Gesundheitsdiensteanbietern an private Versicherungsunternehmen,
- Verwendung der Sozialversicherungsnummer zur Identifikation außerhalb des Gesundheitsbereichs.

Personal- und Sachausstattung des Geschäftsapparats der Datenschutzkommission

Die Personalsituation der DSK ist nach wie vor schwierig. Aus dem im Kapitel 3.2.3. enthaltenen Vergleich mit anderen Datenschutz-Kontrollstellen in der EU lässt sich ablesen, dass das Personal der DSK gemessen am – mit der Einwohnerzahl gewichteten – Durchschnitt nur etwa 50 % beträgt. Die Folge davon sind noch immer zu lange Verfahrensdauer, insbesondere bei den Registrierungsverfahren, und mangelnde Ressourcen für die Durchführung von Prüfungen von Datenanwendungen vor Ort bei den Auftraggebern.

Auch die verteilte Unterbringung des Geschäftsapparats in unterschiedlichen Amtsgebäuden ist hinderlich.

Zur Zukunft der Datenschutzkommission

Im Entwurf zum ersten Teil der so genannten „Staatsreform“ wird die DSK aufgelöst. Ihre Kompetenzen sollen auf verschiedene andere Institutionen aufgeteilt werden. Abgesehen davon, dass es weitgehend ungewiss ist, wie diese Aufteilung erfolgen soll, würde sich aus einer solchen Zersplitterung der Kompetenzen der DSK eine entscheidende Schwächung der Durchsetzung des Datenschutzgedankens, insbesondere Verteuerungen und Verzögerungen für die Bürger, in Österreich ergeben. Sie würde auch dem europäischen Standard, der von **einer unabhängigen** nationalen Datenschutz-Kontrollstelle mit umfassenden Kompetenzen ausgeht, zuwiderlaufen. Eine eingehende Darstellung der juristischen und praktischen Gegenargumente gegen die geplante Neuregelung findet sich in Kapitel 5.3.2.

INHALT

1. Einleitung

Die Datenschutzkommission (DSK) ist die nationale Datenschutz-Kontrollstelle im Sinne des Art. 28 der Datenschutzrichtlinie 95/46/EG.

Ihr hiermit vorgelegter zwölfter Datenschutzbericht umfasst den Zeitraum vom 1. Juli 2005 bis 30. Juni 2007. Dies sind gleichzeitig die ersten beiden Jahre der mit 1. Juli 2005 begonnenen Funktionsperiode der derzeit amtierenden Datenschutzkommission.

Im letzten Datenschutzbericht wurden auch grundsätzliche Erwägungen zur Situation einer Datenschutz-Kontrollbehörde in Österreich (vgl. Pkt. 3.3. des 11. Datenschutzberichtes) angestellt; der vorliegende Bericht wird die seither diesbezüglich gewonnenen Erfahrungen darstellen und kommentieren.

Zur besseren Erkennbarkeit von Entwicklungen nehmen die statistischen Schaubilder auch auf vorhergehende Amtsperioden der Datenschutzkommission Bezug.

Soweit in diesem Bericht auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise.

2. Die Organe der Datenschutzkommission

„Die Mitglieder der Datenschutzkommission sind in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden“ (§ 37 Abs. 1 DSG 2000, Verfassungsbestimmung).

Die DSK als Kollegialorgan hat die Stellung eines Tribunals iSd EMRK; ihre Mitglieder sind unabhängig, ihr Vorsitzender ist Richter. Die DSK ist allerdings keine Art. 133 Z. 4 B-VG Behörde, sondern auch organisatorisch eine Behörde sui generis (vgl. die §§ 36 ff DSG 2000).

Der DSK als Kollegialbehörde obliegt vor allem die Beschlussfassung hinsichtlich ihrer rechtsförmlichen Entscheidungen (vgl. § 38 Abs. 1 DSG 2000 und die in Ausführung hiezu ergangenen Geschäftsordnung der DSK).

Seit 1. Juli 2000 beträgt die Zahl der Kommissionsmitglieder und Ersatzmitglieder jeweils 6 Personen, die vom Bundespräsidenten ernannt werden. Sämtliche Mitglieder nehmen ihre Tätigkeit in der DSK nur neben ihrem Hauptberuf wahr.

Der für die Ernennung notwendige Vorschlag der Bundesregierung wird hinsichtlich

- des richterlichen Mitglieds und des richterlichen Ersatzmitgliedes aufgrund eines Dreiervorschlages des Präsidenten des OGH ,
- zweier Mitglieder und zweier Ersatzmitglieder aufgrund eines Vorschlags der Länder
- eines Mitglieds und eines Ersatzmitglieds aufgrund eines Dreiervorschlags der Bundeskammer für Arbeiter und Angestellte, sowie hinsichtlich
- eines Mitglieds und eines Ersatzmitglieds aufgrund eines Dreiervorschlags der Wirtschaftskammer Österreich

erstattet. Ein Mitglied und eine Ersatzmitglied sind von der Bundesregierung aus dem Kreis der Bundesbeamten vorzuschlagen.

Neben der DSK als Kollegialorgan werden als Organe der DSK noch der Vorsitzende und aufgrund der Verfassungsbestimmung des § 38 Abs. 1 DSG 2000 das von der Geschäftsordnung bestimmte geschäftsführende Mitglied (gfM) tätig.[1]

Die Zusammensetzung der DSK im Berichtszeitraum 1. Juli 2005 bis 30. Juni 2007 war wie folgt:

Mitglieder:

- Dr. Anton SPENLING, Vorsitzender (richterliches Mitglied)
- Dr. Waltraut KOTSCHY, geschäftsführendes Mitglied
- Dr. Ludwig STAUDIGL
- Mag. Helmut HUTTERER
- Mag. Daniela ZIMMER
- Dr. Claudia ROSENMAYR-KLEMENZ

Ersatzmitglieder:

- Dr. Gerhard KURAS, stv. Vorsitzender (richterliches Ersatzmitglied)
- Dr. Eva SOUHRADA-KIRCHMAYER, stv. geschäftsführendes Mitglied
- Dr. Klaus HEISSENBERGER
- Dr. Michaela BLAHA
- Mag. Joachim PREISS (bis 31. Jänner 2007), Mag. Gerda HEILEGGER (seit 4. Mai 2007)
- Mag. Huberta MAITZ-STRASSNIG

[1] „Die Datenschutzkommission hat sich eine Geschäftsordnung zu geben, in der eines ihrer Mitglieder mit der Führung der laufenden Geschäfte zu betrauen ist“ (§ 38 Abs. 1 DSG 2000, Verfassungsbestimmung).

3. Der Geschäftsapparat der Datenschutz-kommission

3.1. Die Organisation der Geschäftsstelle

Gemäß § 38 Abs. 2 DSG 2000 hat der Bundeskanzler die notwendige Sach- und Personalausstattung für die Geschäftsführung der Datenschutzkommission zur Verfügung zu stellen.

Zur Unterstützung in der Geschäftsführung ist der DSK eine Geschäftsstelle beigegeben, die derzeit organisatorisch als Abteilung im Verfassungsdienst des Bundeskanzleramtes eingerichtet ist. Die Geschäftsstelle unterstützt die DSK in allen Angelegenheiten der DSK, einschließlich ihrer Aufgaben als Stammzahlenregisterbehörde. Seit Mitte 2006 besitzt die Geschäftsstelle zwei Referate – vorher nur eines –, nämlich das Büro der DSK, das für die vorbereitende Behandlung der Beschwerdefälle zuständig ist, und das Datenverarbeitungsregister (DVR).

Die Bediensteten der Geschäftsstelle sind gemäß § 37 Abs. 2 DSG 2000 (Verfassungsbestimmung) in Anerkennung der Unabhängigkeit der DSK fachlich nur an die Weisungen des Vorsitzenden und des geschäftsführenden Mitglieds der DSK gebunden. Die Dienstaufsicht über die Mitarbeiter der Geschäftsstelle wird vom Bundeskanzleramt ausgeübt.

3.2. Der Personalstand der Geschäftsstelle

3.2.1. Zur Personalsituation der Geschäftsstelle außerhalb des Datenverarbeitungsregisters

Der in der Hofburg untergebrachte Teil der Geschäftsstelle der DSK hat derzeit folgende Personalausstattung:

- 1 A/a Planstelle: Leiterin der Geschäftsstelle (führt die Dienstaufsicht über die Geschäftsstelle und untersteht in diesen Belangen dem Leiter der Sektion Verfassungsdienst; nimmt Leitungsaufgaben in der Geschäftsstelle *in fachlicher Hinsicht* wahr, soweit solche ihm vom Geschäftsführenden Mitglied der DSK delegiert wurden
- 1 A/a Planstelle: Leiter des Büros der DSK, das die Beschwerdeverfahren betreut
- 2 A/a Planstellen: juristische Sachbearbeiter im Büro der DSK
- 0,5 A/a Planstelle: Sachbearbeiter für juristisch/technische Belange der Geschäftsstelle und Verfahren im internationalen Datenverkehr
- 1 A/a Planstelle: Stammzahlenregister
- 1 B/b Planstelle: Sachbearbeiterin für Sitzungsmanagement
- 1 c Planstelle: Teamassistenz/Sekretariat/ Kanzlei
- 1 d Planstelle: Sekretariat/Kanzlei

- **8, 5 Planstellen** insgesamt

Dies ist das Ergebnis folgender Veränderungen im Personalstand seit 1. Juli 2005:

Mit 1. August 2005 wurde eine Planstelle A/a für die Agenden des Stammzahlregisters zusätzlich zugeteilt.

Seit dem 1. Juli 2006 wurde jedoch die Zahl der juristischen Mitarbeiter um eine Planstelle verringert: Es ging die für Angelegenheiten der europäischen und internationalen Zusammenarbeit (insbe-

sondere im Rahmen der Art. 29 Gruppe) gewidmete Planstelle verloren.

Weiters besorgt eine halbe A/a Planstelle seit 1. Juli 2006 eigentliche DVR-Aufgaben, da es sich als rationeller erwiesen hat, die Genehmigungsverfahren im internationalen Datenverkehr nach dem „one-stop-shop"-Prinzip zu führen, d.h. gemeinsam mit dem diesbezüglichen Registrierungsverfahren.

Von dem 1999 im Vorblatt zur Regierungsvorlage zum DSG 2000 unter „Kosten" ausgewiesenen zusätzlichen Bedarf von 4 Planstellen sind daher derzeit nur 2 Planstellen tatsächlich zugeteilt. Von dem im Vorblatt zur Regierungsvorlage zum E-GovG für das Stammzahlenregister veranschlagten Personalbedarf von 2 Planstellen steht nur eine zur Verfügung. Die Situation der DSK darf wohl als gutes Beispiel dafür gelten, dass die Zuteilung neuer Aufgaben an Verwaltungsbehörden nicht mit der Zuteilung des notwendigen Zusatzpersonals Hand in Hand geht.

3.2.2. Zur Personalsituation des Datenverarbeitungsregisters

- 1 A/a Planstelle: Leiterin des Datenverarbeitungsregisters
- 1,5 A/a Planstellen: juristischer. Sachbearbeiter
- 1 Behindertenplanstelle: Sachbearbeiterin
- 3,75 B/b Planstellen: SachbearbeiterInnen
- 2,4 C/c Planstellen: Sachbearbeiterinnen und Kanzlei
- 2 d Planstellen: Hilfstätigkeiten

- **11, 65 Planstellen** insgesamt

Der Geschäftsapparat der DSK verfügt somit über insgesamt 20 Planstellen.

3.2.3. Europäischer Vergleich

Der Vergleich mit den anderen Staaten – innerhalb und außerhalb der Europäischen Union - ist ein signifikanter Gradmesser für die Frage, ob davon ausgegangen werden darf, dass die Personalausstattung der österreichischen Datenschutzkommission ausreichend ist. Nachstehend soll ein Vergleich der Entwicklung der Personalausstattung der Unabhängigen Datenschutz-Kontrollstellen in Europa Auskunft zu dieser Frage geben, wobei eine geänderte Reihung gegenüber 2004 nur dort vorgenommen wurde, wo die Antworten nicht nur auf „Personalstand erhöht (+)" lauteten, sondern tatsächlich Zahlen genannt wurden: siehe nebenstehende Tabelle.

Aus dieser Statistik wird deutlich, dass Österreich nicht nur am unteren Ende der europäischen Skala rangiert, sondern überdies seit dem Ergebnis der Umfrage betreffend das Jahr 2004 vom 24. auf den 27. Platz zurückgefallen ist, da in der Zwischenzeit die meisten Datenschutzbehörden zusätzliches Personal erhalten haben.

Interessant ist vor allem der Vergleich mit Ländern mit ungefähr ähnlicher Bevölkerungszahl, wie Belgien (37 + Mitarbeiter), Bulgarien (40 Mitarbeiter), Griechenland (39 Mitarbeiter), Schweden (40 Mitarbeiter), Ungarn (47 Mitarbeiter), Portugal (15 Mitarbeiter) oder Tschechien (85 Mitarbeiter). Dieser Vergleich zeigt eine frappante Häufung des Wertes „+- 40". Dieser Wert wird noch weiter statistisch bestätigt, wenn etwa bei den Niederlanden mit doppelt so vielen Einwohnern wie Österreich 75 Mitarbeiter, oder in Irland, bei halb so vielen Einwohnern wie Österreich, 20 Mitarbeiter tätig sind. Dass „40" offenbar eine signifikante Zahl für eine angemessene Personalausstattung für eine nationale Datenschutzbehörde eines Landes von der Größe Österreichs wäre, wird schließlich auch am Beispiel Dänemark bestätigt: Die Einwohnerzahl beträgt 65% im Verhältnis zu Österreich, die Mitarbeiterzahl der dänischen Behörde ist 26, das sind 60 % von „40".[2]

Der internationale Vergleich zeigt klar, dass gerade durch die Entwicklungen im internationalen Bereich vermehrte Aufgaben der DSK eine Aufstockung des Personalstandes erfordern, um die Erfüllung dieser Aufgabe in einem dem europäischen Standards entsprechenden Maße gewährleisten zu können.

[2] Ein Vergleich mit Deutschland oder der Schweiz ist nicht ohne weiteres möglich, da dort die Datenschutz-Kontrollstellen föderal organisiert sind, d.h. zusätzlich zur jeweiligen Bundesbehörde noch eine entsprechende Anzahl von Landes-Datenschutz-Kontrollstellen existiert, wodurch insgesamt ungleich mehr Personal für die Durchsetzung von Datenschutz zur Verfügung steht.

AUFSTELLUNG DER VOLLBESCHÄFTIGTEN IN DEN DATENSCHUTZBEHÖRDEN DES EWR (EXKL. DEUTSCHLAND) SOWIE MONACO UND DER SCHWEIZ IM VERGLEICH DER JAHRE 2004 UND 2006

(SORTIERT NACH DEM VERHÄLTNIS DER BESCHÄFTIGTEN ZUR EINWOHNERZAHL)[3]

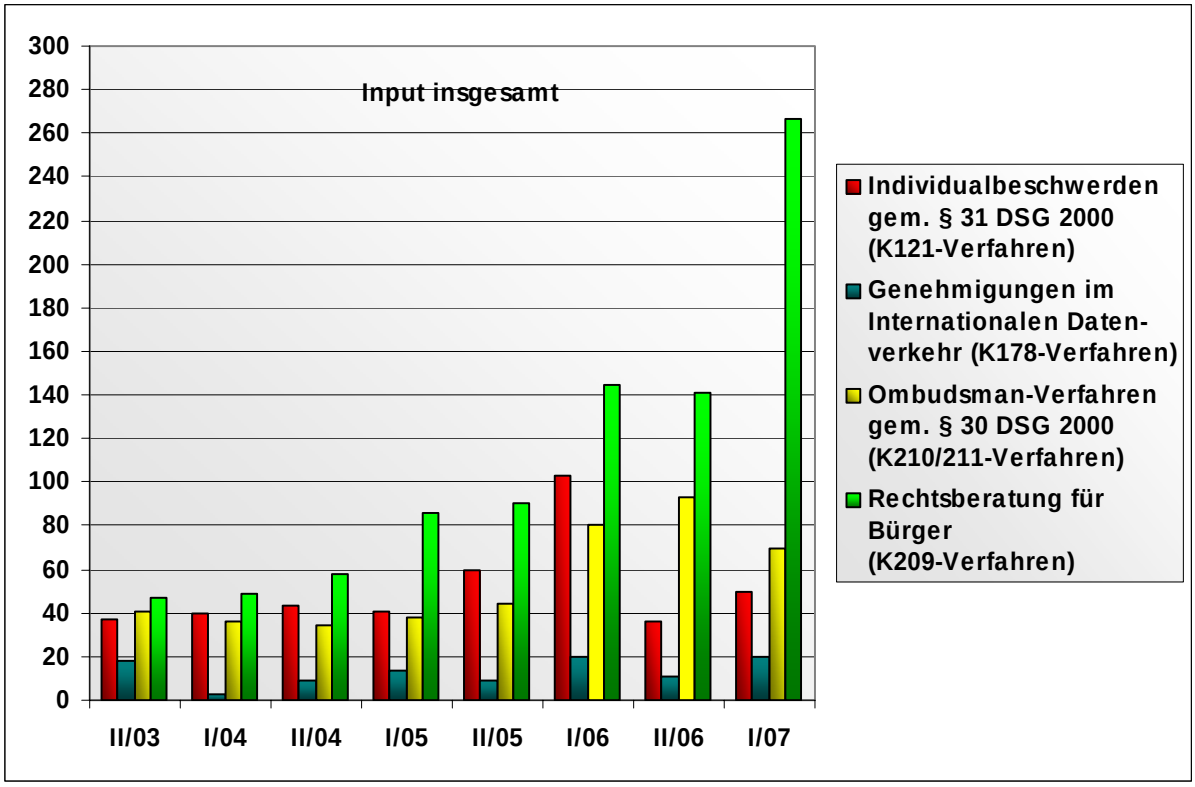
REIHUNG 2004/ 2006	LÄNDER	EINWOHNER	VOLLZEIT-BESCHÄFTIGTE 2004	2006	VERHÄLTNIS BESCH. : EINW. (GERUNDET)
1/1	MONACO	30.000	7	+	1 : 4.000
2/2	ISLAND	300.000	11	+	1 : 27.000
3/3	MALTA	400.000	10	---	1 : 40.000
4/4	ZYPERN	700.000	12	+	1 : 58.000
29/5	SLOWENIEN	2.000.000	3	26	1 : 76.000
6/6	ESTLAND	1.400.000	15	18	1 : 78.000
5/7	LUXEMBURG	450.000	5	+	1 : 90.000
8/8	LITAUEN	3.000.000	30	+	1 : 100.000
7/9	LETTLAND	2.300.000	23	---	1 : 100.000
21/10	LIECHTENSTEIN	340.000	1	3	1 : 113.000
9/11	TSCHECHISCHE REP.	10.000.000	79	85	1 : 118.000
10/12	NORWEGEN	4.500.000	29	32	1 : 141.000
11/13	SLOWAKEI	5.370.000	33	32	1 : 168.000
14/14	IRLAND	4.000.000	19	21	1 : 190.000
26/15	BULGARIEN	8.000.000	15[1)]	40	1 : 200.000
13/16	DÄNEMARK	5.300.000	26	---	1 : 204.000
12/17	UNGARN	10.000.000	54	47	1 : 212.700
16/18	NIEDERLANDE	16.000.000	65	75	1 : 213.400
19/19	U.K.	59.500.000	205	265	1 : 224.500
15/20	SCHWEDEN	9.000.000	39	40	1 : 225.000
23/21	GRIECHENLAND	10.000.000	27	39	1 : 256.000
17/22	FINNLAND	5.200.000	20	+	1 : 260.000
18/23	BELGIEN	10.300.000	36	+	1 : 286.000
20/24	POLEN	38.200.000	115	113	1 : 338.000
22/25	SCHWEIZ	7.000.000	20	---	1 : 350.000
26/26	SPANIEN	43.200.000	97	115	1 : 376.000
24/27	**ÖSTERREICH**	**8.000.000**	**20**		1 : **400.000**
28/28	ITALIEN	58.000.000	94	100	1 : 580.000
29/29	RUMÄNIEN	22.000.000	37	---	1 : 595.000
30/30	FRANKREICH	62.000.000	83	95	1 : 651.000
31/31	PORTUGAL	10.400.000	15	+	1 : 693.000

[3] Die Angaben sind jeweils einem Fragebogen entnommen, der jährlich für die Frühjahrskonferenz der Europäischen Unabhängigen Datenschutzbehörden erstellt wird.

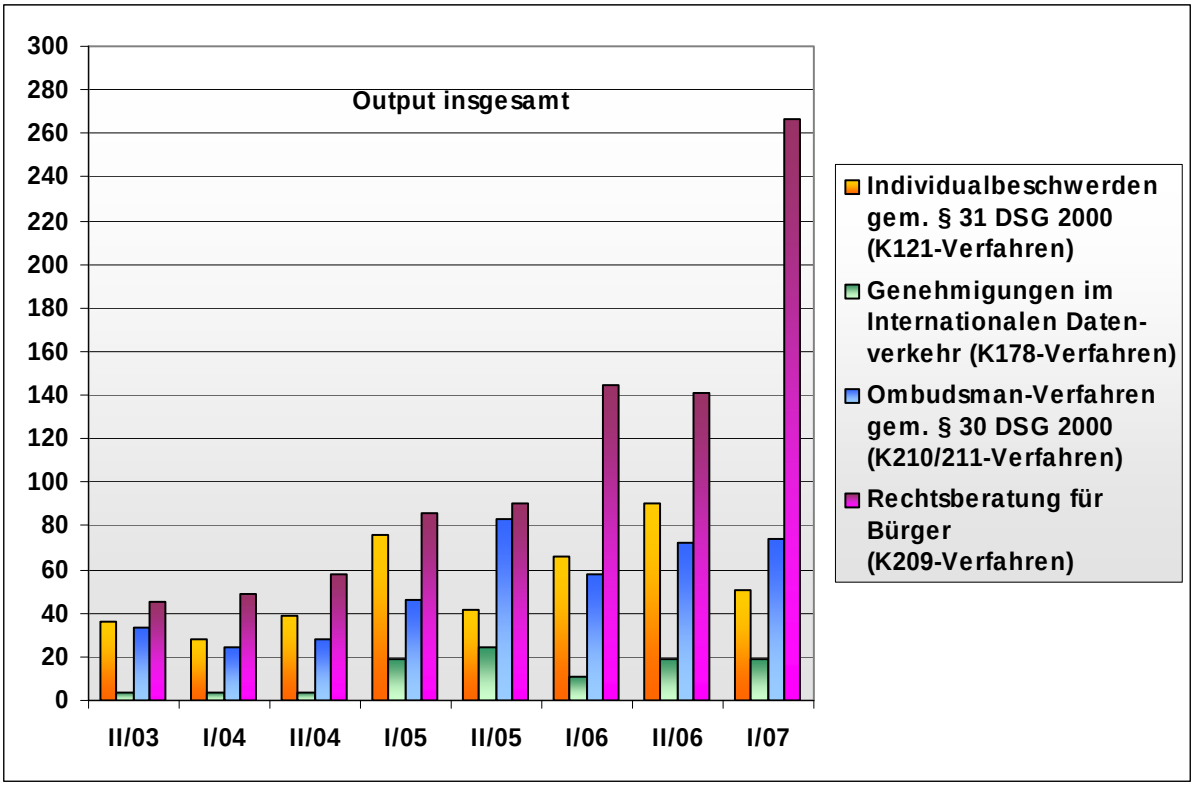
4. Geschäftsgang

4.1. Statistische Darstellung des Geschäftsganges (Gesamtübersicht)

Geschäftsfälle - Input



Geschäftsfälle - Output



		Eingangsstücke					Erledigungen			
		2. Halbjahr 2005	1. Halbjahr 2006	2. Halbjahr 2006	1. Halbjahr 2007		2. Halbjahr 2005	1.Halbjahr 2006	2. Halbjahr 2006	1. Halbjahr 2007
Individualbeschwerden (K120 und K121-Verfahren)		60 (10)[4]	103	36	50		42	66	90	51
Ombudsmannverfahren nach § 30 DSG 2000 (K210 + K211)		44	80	93	70		83	58	72	74
Rechtsauskünfte (K209)		90	145	141	267		90	145	141	267
Genehmigungen nach § 46 und 47 DSG 2000 (K202)		4	3	4	1		2	7	2	1
Genehmigungen im Internationalen Datenverkehr (K178)		9	20	11	20		23	11	19	19[5]
Entscheidungen der Kommission im Registrierungsverfahren (K503 und K 600)		**80 Fälle in der Zeit vom 01.07.05 bis 30.06.07**					**79 Fälle in der Zeit vom 01.07.05 bis 30.06.07**			
Verf.- und Verwaltungsgerichtshofsbeschwerden (K078 und K079)[6]		22	21	12	16		12	9	6	8
Auskunft Schengen (K250)		10	28	25	9		10	28	25	9

[4] 10 Eingangsstücke nachträglich als § 30 Verfahren umprotokolliert
[5] 12 Verfahren waren Rest aus der vorigen Berichtsperiode
[6] nicht bei allen Beschwerden wurden Gegenschriften erstattet (z. B. bei Erledigung nach § 35 Abs. 1 VwGG oder Art. 144 Abs. 2 B-VG).

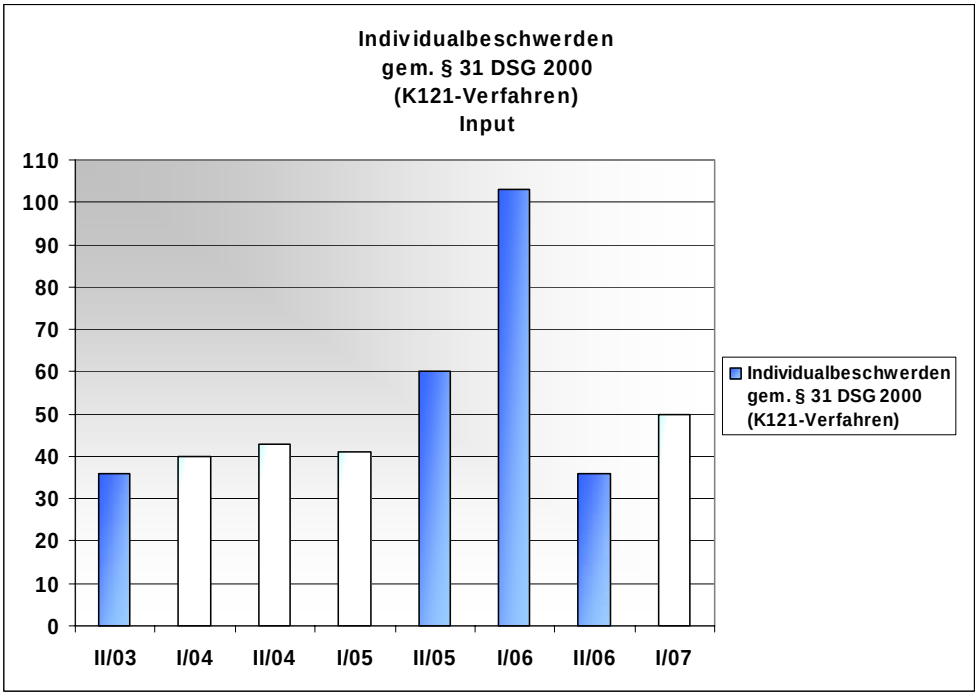
4.2 Die Verfahren vor der DSK

4.2.1 Individualbeschwerdeverfahren (§ 31 DSG 2000)

Gemäß § 31 DSG 2000 kann vor der DSK Beschwerde mit verbindlicher Wirkung der Entscheidung in Auskunftssachen (im privaten und öffentlichen Bereich) sowie in Geheimhaltungs-, Richtigstellungs- und Löschungssachen (nur hinsichtlich des öffentlichen Bereichs) erhoben werden.

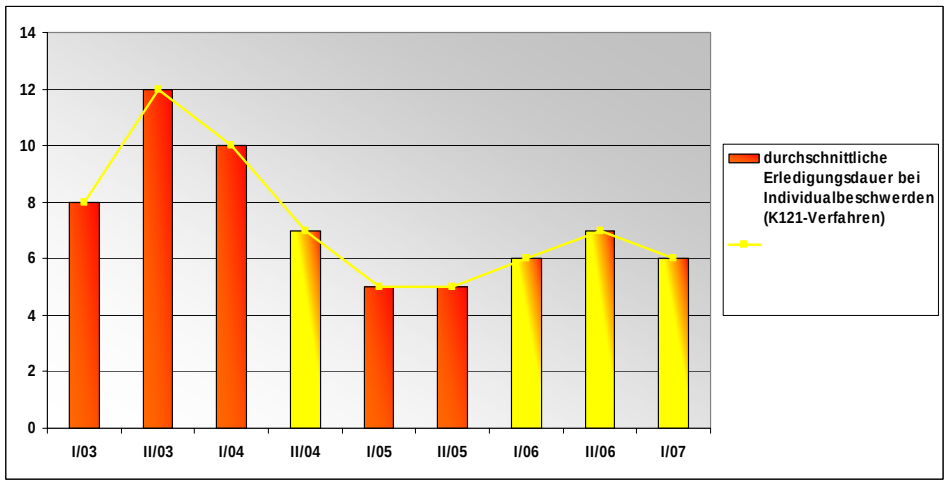
Im Berichtszeitraum zeigt sich um die Jahreswende 2005 /2006 eine ganz ungewöhnlich hohe Anzahl von eingegangenen Beschwerden – diese gingen allein auf zwei Beschwerdeführer zurück. Seither haben sich die Beschwerdezahlen wieder auf ein Maß eingependelt, das sich als leicht steigender Trend beschreiben lässt.

Graphische Übersicht des Arbeitsanfalls:



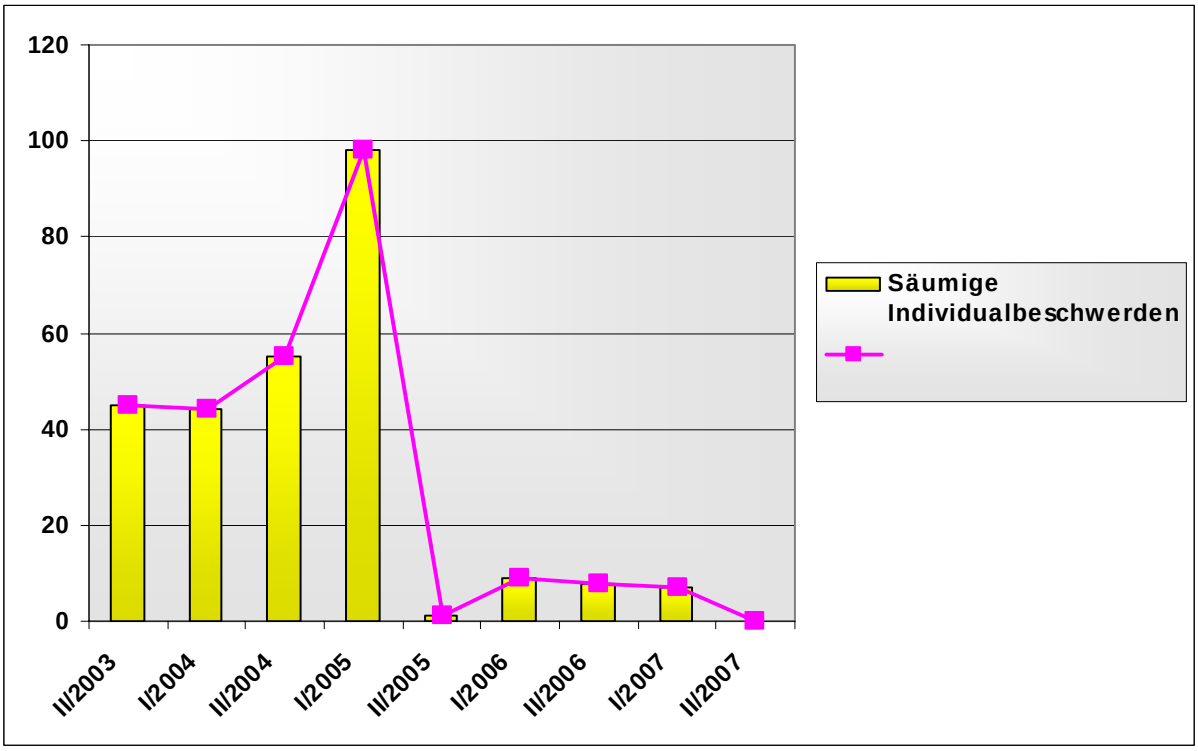
Graphische Übersicht der durchschnittlichen Erledigungsdauer:

Aus dieser Graphik wird deutlich, wie sich die durchschnittliche Erledigungsdauer der Individualbeschwerden durch den beschriebenen extremen Eingangszuwachs um die Jahreswende 2005/2006, der ja nicht durch zusätzliches Personal aufgefangen werden konnte, nachteilig verändert hat: Während im Jahre 2005 die durchschnittlich Erledigungsdauer mit 5 Monaten so niedrig war wie noch nie, ist sie im Jahr 2006 wieder gestiegen, und zwar zunächst auf 6 und dann sogar auf 7 Monate.



In der Zwischenzeit ist es jedoch gelungen, die Folgen dieses außergewöhnlichen Anfalls von Beschwerden zu überwinden und die 6-monatige Entscheidungsfrist des § 73 AVG für Individualbeschwerden wieder einzuhalten. Im Berichtszeitpunkt waren, wie die folgende Graphik zeigt, keine säumigen Verfahren anhängig:

Graphische Übersicht über das Ausmaß säumiger Individualbeschwerden:



Materielle Ergebnisse von Individualbeschwerden

Was das Ergebnis von Beschwerdeverfahren nach § 31 DSG 2000 betrifft, ergibt die statistische Aufbereitung Folgendes:

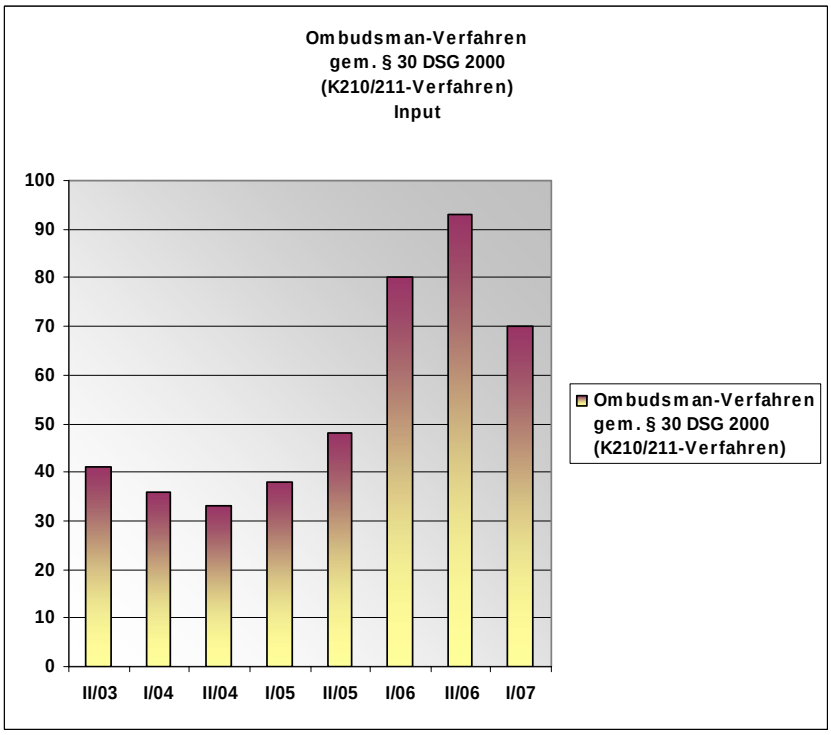
Von 242 im Berichtszeitraum abgeschlossenen Beschwerdeverfahren haben

- 45 mit formloser Erledigung (Einstellung, Weiterleitung; in der überwiegenden Zahl der Fälle Einstellungen wegen expliziter oder impliziter Beschwerdezurückziehung) geendet,
- 41 mit Zurückweisung der Beschwerde,
- 156 mit zumindest teilweise Sachentscheidung, und zwar
  - wurde in 102 Fälle erfolglos Beschwerde erhoben,
  - in 54 Fällen war die Beschwerde zumindest teilweise erfolgreich.

Das bedeutet, dass ungefähr zwei Drittel aller Beschwerden, über die inhaltlich entschieden wird, unbegründet waren.

4.2.2. Ombudsmannverfahren (§ 30 DSG 2000)

Auch hier war der Arbeitsanfalls tendenziell steigend:



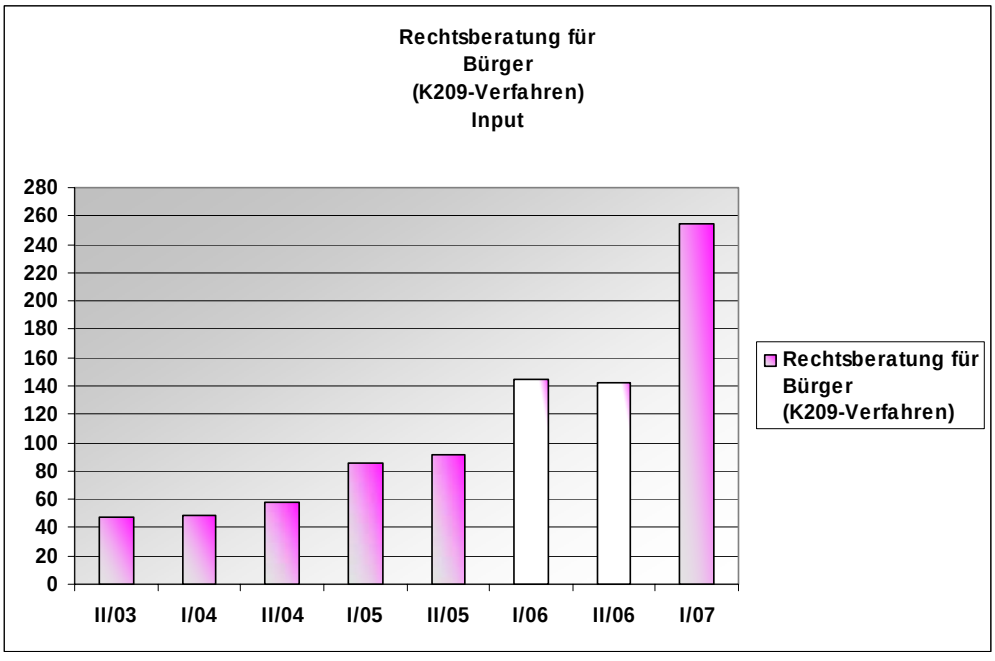
Das Ombudsmannverfahren hat sich als äußerst wertvolles Instrument der Rechtsverwirklichung erwiesen. Die weitgehende Formfreiheit dieses Verfahrens ermöglicht eine besonders rasche Erledigung der Anliegen der Bürger. Obwohl hier keine unmittelbar durchsetzbaren Entscheidungen erlassen werden, führt die Tätigkeit der DSK dennoch in fast allen Fällen zu einem für die Beschwerdeführer zufrieden stellenden Ergebnis.

Bei einer allfälligen Novellierung des DSG 2000 könnte ins Auge gefasst werden, bei Auskunftsbeschwerden – die den größten Anteil der Beschwerdefälle nach § 31 DSG 2000 darstellen – verpflichtend ein Ombudsmann-verfahren vorzu-schalten. Dadurch könnte die Erledigungsdauer der Eingaben insgesamt sicher nicht unwesentlich gesenkt werden.

4.2.3 Rechtsauskünfte an Bürger (K 209-Verfahren)

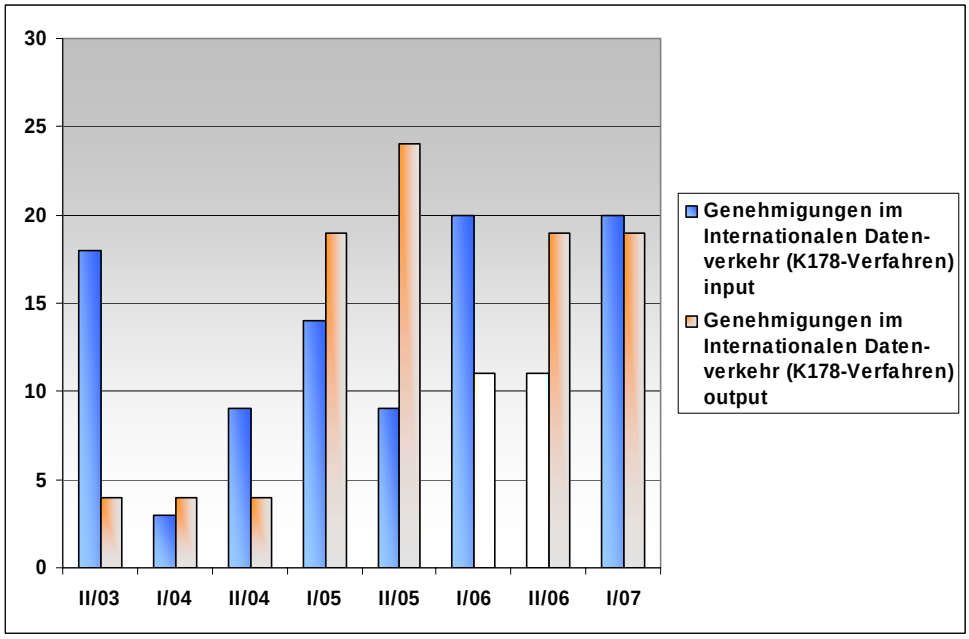
Wie wichtig diese vom Büro der DSK wahrgenommene Funktion geworden ist, ergibt sich anschaulich aus der untenstehenden Graphik.

Hinzu kommt noch die Tätigkeit des DVR auf diesem Gebiet, das von der Bevölkerung nicht immer nur mit Rechtsfragen des Registrierungsverfahrens befasst wird. 90 Anrufe am Tag sind im DSR keine Seltenheit.



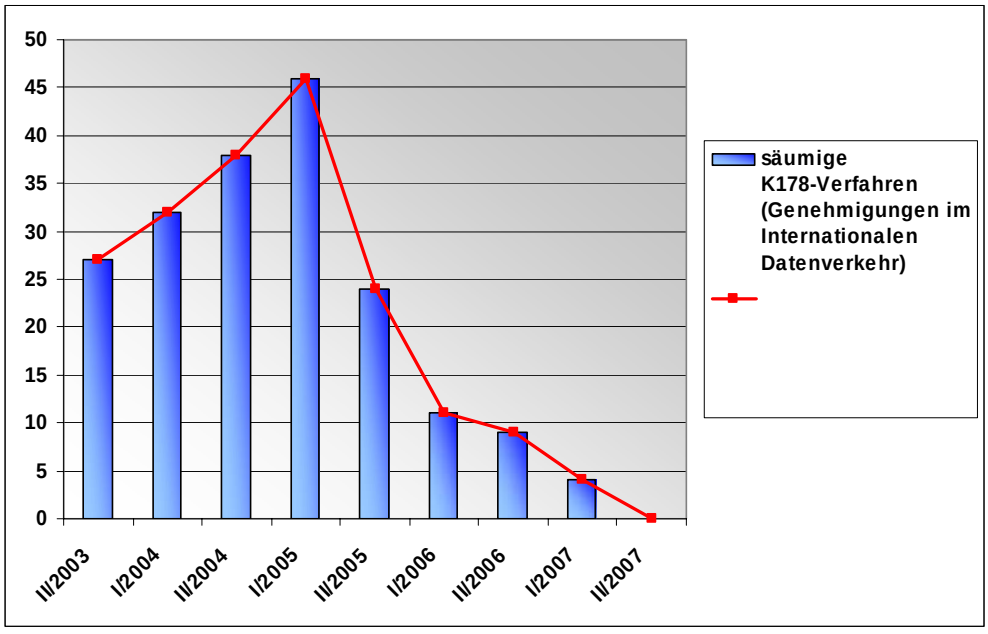
4.2.4 Genehmigungen im Internationalen Datenverkehr (§§12 und 13 DSG 2000):

Graphische Darstellung von Input und Output im Bereich „Internationaler Datenverkehr“:



In diesem Bereich hat seit Inkrafttreten der RL 95/46/EG und ihrer Umsetzung in den §§ 12 und 13 des DSG 2000 zunächst einige Rechtsunsicherheit darüber geherrscht, wie die Art. 25 und 26 der RL in der Praxis tatsächlich zu verstehen sind. Dies hat auch dazu beigetragen, dass die Formulierung der Genehmigungsanträge oft erheblichen Klärungsbedarf verursachen, der oft noch dadurch erhöht wird, dass solche Anträge für eine österreichische Tochter eines internationalen Konzerns mit Sitz in Übersee gestellt werden, wo das Verständnis für Datenschutz europäischer Prägung oftmals gering ist. Hierdurch ist es zu Anfang der Berichtsperiode noch zu einem gewissen Rückstau bei der Erledigung von Genehmigungen gekommen. In der Zwischenzeit konnte anhand der Entscheidung von Einzelfällen jedoch mehr Klarheit über das Aussehen der Genehmigungsvoraussetzungen in der Praxis gewonnen werden, sodass es mit Ende des Berichtszeitraums gelungen ist, keine säumigen Genehmigungs-verfahren mehr zu haben.

Graphische Darstellung der säumigen Verfahren im Internationalen Datenverkehr:



4.2.5. Bescheide der DSK im Registrierungsverfahren (§ 20 Abs. 4 und 21 Abs. 2 DSG 2000)

Die Registrierung der Meldung einer Datenanwendung erfolgt nicht mit Bescheid, sondern mit bloßer Mitteilung, die nicht der Rechtskraft fähig ist (- der meldende Auftraggeber erwirbt durch die Registrierung keinen Rechtsanspruch darauf, die Datenanwendung in der gemeldeten Form durchführen zu dürfen). Ein Bescheid der DSK ergeht nur dann, wenn die Registrierung einer Meldung (ganz oder teilweise) abgelehnt wird oder wenn bei vorabkontrollpflichtigen Datenanwendungen (§ 18 Abs. 2 DSG 2000) Auflagen für die Führung der Datenanwendung im Interesse des Schutzes der Betroffenenrechte notwendig sind.

Im Berichtszeitraum hat sich die Notwendigkeit, Bescheide im Registrierungsverfahren zu erlassen, zum einen im Zusammenhang mit der Meldung von Videoüberwachungen ergeben, zum anderen bei der Einrichtung von Informationsverbundsystemen in einzelnen Branchen (vgl. hiezu auch die Ausführungen in Abschnitt 8). Festzuhalten ist, dass die Zahl der bescheidmäßigen Erledigungen von Registrierungsverfahren zwar insofern groß ist, als es sich oft um „Massenverfahren“ in dem Sinn handelt, dass ein Informationsverbundsystem für alle teilnehmenden Auftraggeber einer gesamten Branche zu registrieren ist, dass aber die Anzahl der Kategorie von Fällen, in welchen Registrierungen abgelehnt oder Auflagen erteilt werden, insgesamt gering ist. Die Hauptlast der Registrierung wird vom DVR allein getragen, das durch seine unterstützende Serviceleistungen für die meldenden Auftraggebern wesentlich dazu beiträgt, dass nur wenige Fälle zu „Streitfällen“ werden, in welchen die DSK förmlich entscheiden muss. Nach Auffassung der DSK ist der dadurch verursachte Ressourceneinsatz im DVR gerechtfertigt und zielführend, da durch fach-männische Hilfestellung seitens des DVR die gesamtwirtschaftlichen Folgekosten der datenschutz-rechtlichen Meldepflicht erheblich verringert werden.

4.2.6. Amtswegige Prüfverfahren

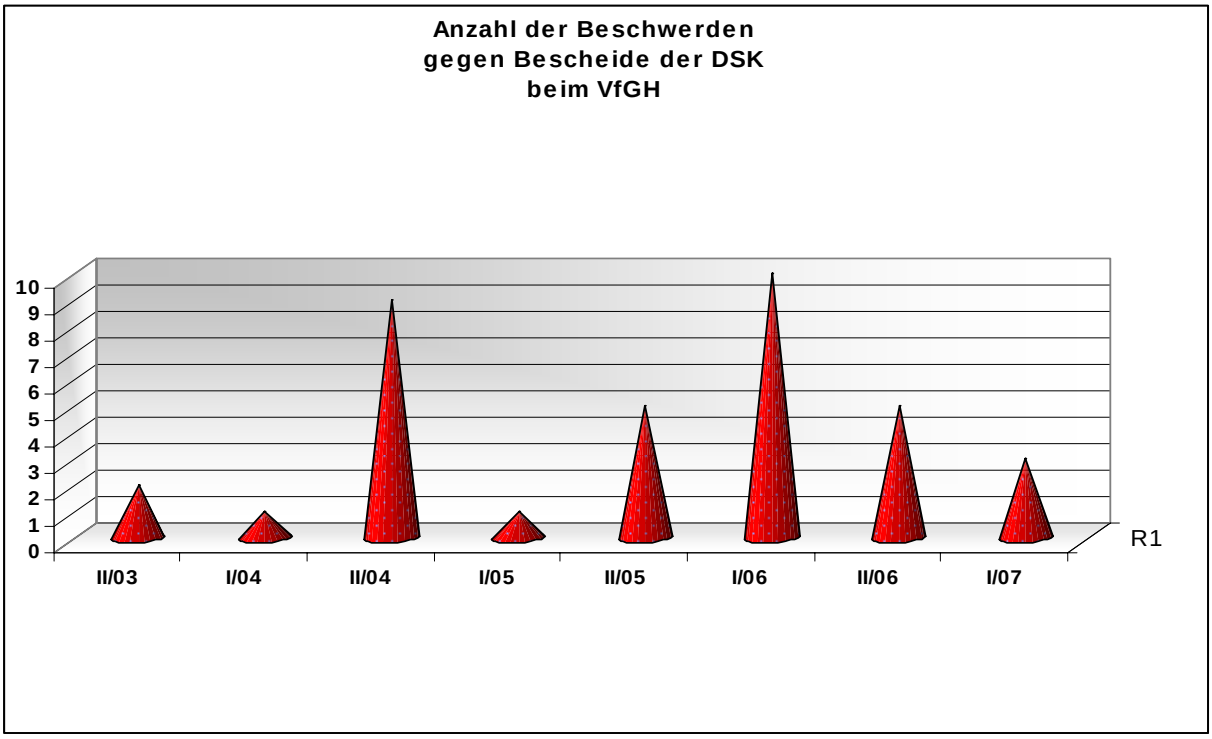
Diese haben sich im Berichtszeitraum hauptsächlich auf den Sektor Kreditinformation und Kreditauskunftei konzentriert (vgl. hiezu die näheren Ausführungen unter Pkt. 6.2 b-d).

Dass die Tätigkeit der DSK auf diesem Sektor nicht die wünschenswerte Dichte erreicht, ist der DSK bewusst und wird außerordentlich bedauert, doch ist nicht absehbar, dass sich dieser Zustand bei der gegebenen Personalsituation verbessern ließe.

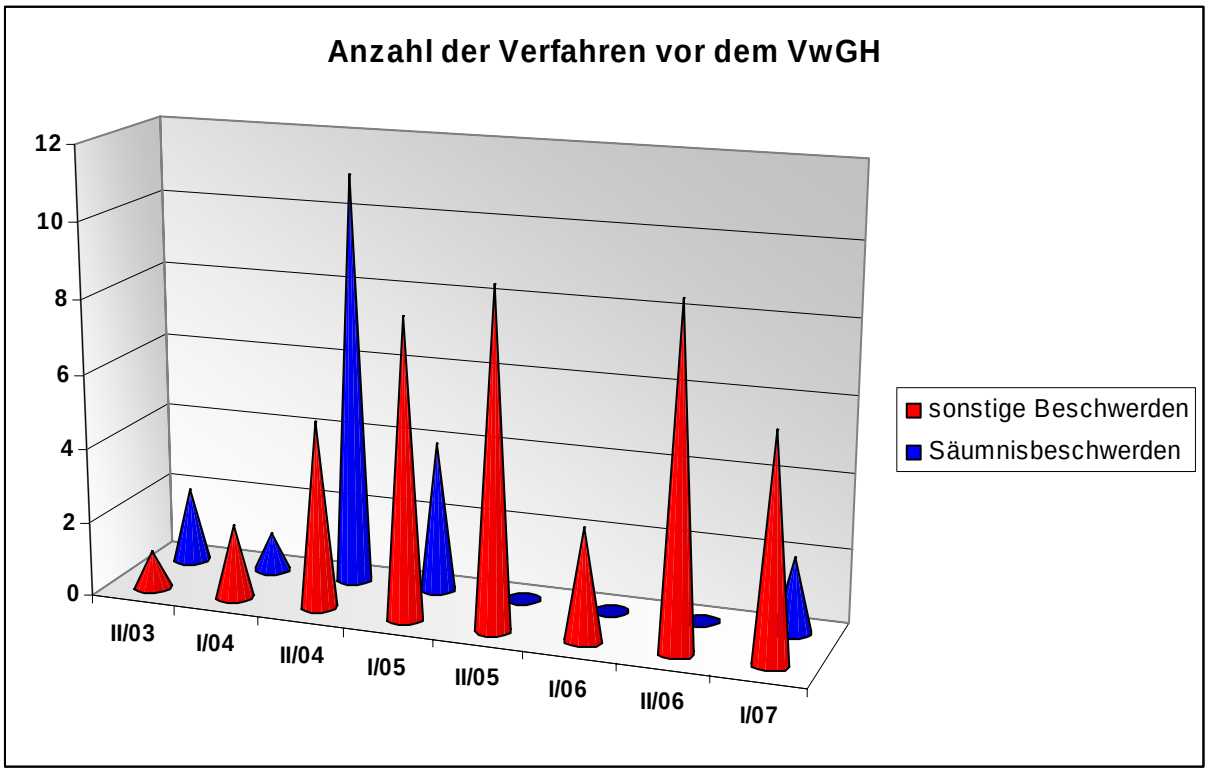
4.2.7. Äußerungen in Beschwerdeverfahren vor dem Verfassungs- und Verwaltungsgerichtshof

Graphische Darstellung der Verfahren vor dem VfGH:

Von den 23 im Berichtszeitraum gegen Bescheide der DSK erhobenen VfGH-Beschwerden sind 14 noch nicht entschieden, 13 wurden abgewiesen, einer Beschwerde (Erk. VfGH B 3517/05-8 v. 7. März 2007) wurde teilweise stattgegeben (Zum Verfahrensgegenstand siehe die ausführliche Darstellung unter Pkt. 6.1.3. b).



Graphische Darstellung der Verfahren vor dem VwGH:



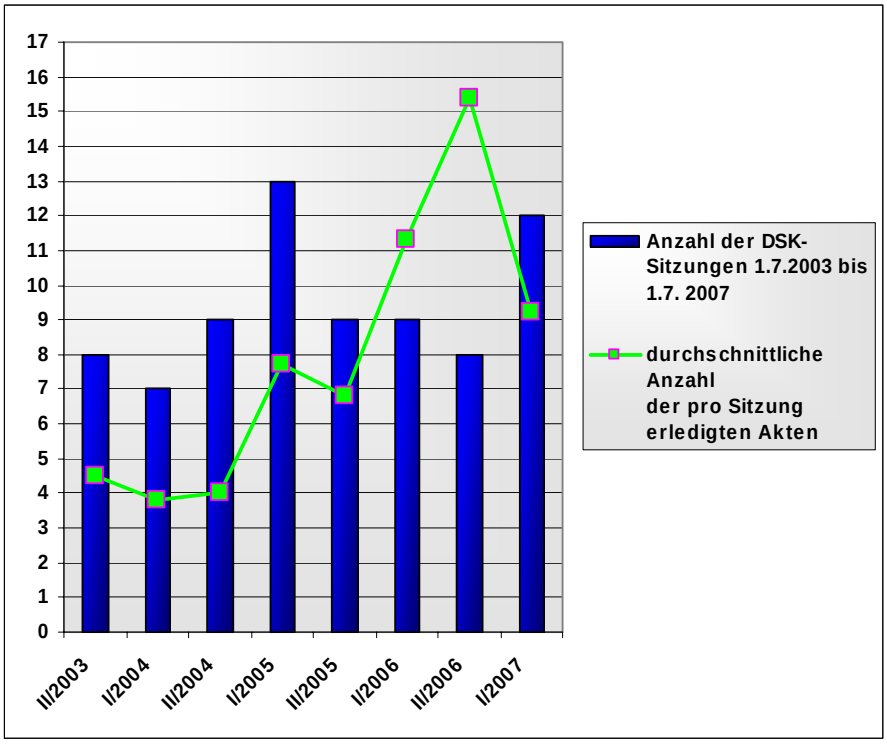
Im Berichtszeitraum wurde gegen 27 Bescheide der DSK Verwaltungsgerichtshofsbeschwerde erhoben, davon erfolgte in 6 Fällen eine Zurückweisung und in 6 Fällen wurde die Beschwerde abgewiesen; in den restlichen 15 Fällen steht die Entscheidung noch aus.

Weiters wurde im Berichtszeitraum vor dem Verwaltungsgerichtshof in 2 Fällen Säumnisbeschwerde erhoben.

4.3. Sitzungen der Datenschutzkommission

Die DSK ist nur bei Anwesenheit aller sechs Mitglieder, allenfalls vertreten durch das zugehörige Ersatzmitglied, beschlussfähig. Eine Ausnahme hievon durch Beschlussfassung im Umlaufweg ist bei Beschwerdeverfahren nach § 31 DSG 2000 nur dann möglich, wenn im Umlaufverfahren nur mehr die Ausformulierung der Bescheidbegründung behandelt wird.

Graphische Darstellung der Sitzungshäufigkeit und Effizienz:



5. Kritische Anmerkungen zur Personal- und Organisationssituation der Datenschutzkommission

5.1. Zu den Aufgaben der Datenschutzkommission und ihrer Personalausstattung

Im Abschnitt 3 befindet sich eine vergleichende Darstellung der Personalausstattung der Datenschutz-Kontrollstellen in Europa. Aus diesem Vergleich ergibt sich, dass die DSK nur rund halb so viel Personal besitzt wie die meisten Kontrollstellen vergleichbarer Staaten.

Die Frage, wie viel Personal die DSK objektiv braucht, hängt naturgemäß hauptsächlich davon ab, welche Kompetenzen ihr durch die österreichische Rechtsordnung übertragen wurden. Im Folgenden soll daher der Kompetenzumfang der DSK einer genaueren Analyse unterzogen werden.

Das Ergebnis dieser Analyse wird auch an den gemeinschaftsrechtlichen Vorgaben zu messen sein, ist die DSK doch die nationale österreichische Datenschutz-Kontrollbehörde im Sinne des Art. 28 der RL 95/46/EG. Hierbei ist zu berücksichtigen, dass der in den Jahren 1990 - 1995 ausgearbeitete Art. 28 der RL nur Mindest-Kompetenzen für eine Kontrollstelle festlegt und sich seither ein europäischer Standard für unabhängige Kontrollstellen herausgebildet hat, der z.B. mit Bezug auf den Europäischen Datenschutzbeauftragten aus den Art. 46 - 49 der Verordnung (EG) Nr. 45/2001 näherhin ablesbar ist.

5.1.1.Beschwerden von Bürgern

Mit dem derzeitigen Personalstand des Büros der DSK lassen sich, wie die statistischen Auswertungen im Abschnitt „Geschäftsgang“ gezeigt haben, die **Beschwerdeverfahren** und die **Beratung der Bürger** in Datenschutzangelegenheiten einigermaßen bewältigen; außerhalb von extremen Anfallsspitzen ist es bei entsprechend starker Anspannung möglich, jene Verfahren, für die die gesetzliche Entscheidungspflicht des § 73 AVG gilt, innerhalb von 6 Monaten durchzuführen. Auch bei den Ombudsmannverfahren ist es im Berichtszeitraum gelungen, weitestgehend eine Erledigungsdauer von weniger als 6 Monaten zu erreichen. Dies geht allerdings Hand in Hand mit einem beachtlichen Druck auf alle Mitarbeiter, was wieder dazu führt, dass es nicht ganz leicht ist, Mitarbeiter auf Dauer zu halten.

5.1.2. Zusammenarbeit auf EU-Ebene

Weiters ist es durch besondere Anstrengungen gerade noch möglich, einigermaßen (- wenn auch oft nur sehr oberflächlich -) an den wichtigsten Aktivitäten der **Art. 29 Gruppe**[7] und einiger ihrer Unterarbeitsgruppen sowie an den Sitzungen der **Gemeinsamen Kontrollinstanzen**[8] **der Dritten Säule** (vgl. dazu Abschnitt 7) teilzunehmen.

Wie wichtig intensive Mitarbeit in diesem Bereich wäre, ergibt sich daraus, dass die wesentlichen datenschutzrechtlichen Herausforderungen heute regelmäßig nicht mehr auf die nationale Ebene beschränkt sind, sondern globale Dimension haben; es ergibt sich daher zwangsläufig, dass die Antworten auf diese Herausforderungen auf Ebene der Europäischen Union gesucht werden. Typische Beispiele hiefür sind etwa die zwingende Übermittlung von Flugpassagierdaten an Flugdestinationsländer („PNR“), der Zugriff auf europäische Zahlungsverkehrsdaten im Zuge der Terrorismusbekämpfung („SWIFT“) oder die Verwendung von personenbezogenen Daten in internationalen Konzernen („BCRs) (nähere Ausführungen dazu im Abschnitt 7).

Die Art. 29 Gruppe wird – ebenso wie die Police Working Party[9] der Europäischen Unabhängigen

[7] Vgl. Pkt. 7.1
[8] Vgl. Pkt. 7.2
[9] Vgl. Pkt. 7.3

Datenschutz-Kontrollstellen in der Dritten Säule – zur Mitarbeit bei der Erarbeitung dieser europäischen Antworten regelmäßig herangezogen, weil auch auf EU-Ebene ein besonderes Bedürfnis nach unabhängigem Expertenrat in Datenschutzsachen besteht. Keine ausreichenden Personalressourcen für eine intensive Mitarbeit der DSK in diesen Gremien zu haben, widerspricht den nationalen Interessen Österreichs: Insbesondere in der Art. 29 Gruppe werden immer wieder Interpretationen und Verfahrensweisen entwickelt, die – zumindest faktisch bindende – unmittelbare Rückwirkungen auf den Datenschutz in Österreich haben.

Für diesen Tätigkeitsbereich gibt es keinen Referenten in der Geschäftsstelle der DSK, seitdem diese Planstelle mit 1. Juli 2006 verloren gegangen ist. Die gebotene systematische Betreuung dieses sehr umfangreichen, sehr dynamischen und sehr wichtigen Bereichs ist daher nicht möglich.

5.1.3. Prüfung von Datenanwendungen

Was beim gegebenen Personalstand weiters nicht ausreichend wahrgenommen werden kann, ist die **Prüfung von Datenanwendungen vor Ort** (vgl. § 30 Abs. 2 und 3 DSG 2000).

Das DSG 2000 normiert die *Kompetenz der DSK* zur Prüfung von Datenanwendungen vor Ort, und zwar bei nicht-vorabkontrollpflichtigen Datenanwendungen „im Falle eines begründeten Verdachtes“ (§ 30 Abs. 2), bei vorabkontrollpflichtigen Anwendungen „auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung“ (§ 30 Abs. 3). Auch wenn die Ausübung dieser Kompetenz gesetzlich nicht detailliert geregelt ist, muss doch die faktische Nicht-Ausübung dieser **Kontroll-Kompetenz** an sich schon als mangelnde Aufgabenerfüllung angesehen werden. Für die DSK ist der bestehende Zustand deshalb besonders schwerwiegend, weil er sie dem Vorwurf aussetzt, dass sie ihre Pflichten vernachlässigt und Mängel, die bei Ausübung ihrer Prüfkompetenz festgestellt hätten werden können, nicht rechtzeitig abgestellt hat.

Tatsache ist auch, dass nach dem bei den Datenschutzkontrollstellen iSd Art. 28 der RL 95/46/EG im Europäischen Wirtschaftsraum (EWR) vorherrschenden Standard die Kontrolltätigkeit in Form der Vorort-Prüfung von Datenanwendungen (- vgl. auch Art. 28 Abs. 3, erster Anstrich -) einen ganz besonders hohen Stellenwert einnimmt. So hat etwa die Art. 29 Gruppe eine eigene Unterarbeitsgruppe „Enforcement“ eingerichtet, die sich mit der koordinierten europaweiten datenschutzrechtlichen Überprüfung z.B. einer gesamten Branche durch die nationalen Kontrollstellen beschäftigt.

Es ist dringend geboten, die DSK durch Zurverfügungstellung der nötigen Ressourcen in die Lage zu versetzen, ihre Prüfkompetenz in ausreichendem Maße wahrzunehmen.

5.1.4. Öffentlichkeitsarbeit

a) Zur Einbeziehung der DSK in das Begutachtungsverfahren für Gesetzentwürfe:

Eine Teilnahme der DSK am Gesetzesbegutachtungsverfahren ist durch das DSG 2000 nicht ausdrücklich vorgeschrieben. Allerdings können die meisten Institutionen, die regelmäßig am Gesetzesbegutachtungsverfahren teilnehmen – insbesondere auch die Bundesministerien – keine ausdrückliche Rechtsgrundlage für diese Tätigkeit vorweisen. Maßgeblich ist auf Grund der Praxis – die hier offenbar von entscheidender Bedeutung ist – nur, dass eine Institution zu dem Sachgebiet des Gesetzesentwurfes aufgrund ihrer Tätigkeit voraussichtlich zweckdienliche Äußerungen erstatten könnte. Aus diesem Grund wird sogar zahlreichen privaten Institutionen regelmäßig im Begutachtungsverfahren Gelegenheit zur Stellungnahme gegeben, wie etwa der ARGE Daten. Die DSK ist hingegen bisher vom Gesetzesbegutachtungsverfahren weitestgehend ausgeschlossen geblieben[10].

Nun erwirbt die DSK aber aufgrund ihrer Tätigkeit als einzige nationale datenschutzrechtliche Beschwerdeinstanz sowie im Zusammenhang mit ihrer Mitarbeit im supra- und internationalen Bereich praktische und theoretische Erfahrungen und Erkenntnissen, bei welchen es sicher vorteilhaft wäre, wenn sie in den nationalen Gesetzgebungsprozess Eingang fänden. Diese Erfahrungen und Erkenntnisse können auch durch die Befassung des Daten-

[10] So etwa kürzlich bei der Begutachtung jener Novelle zum TKG 2003, mit der die Vorratsdatenspeicherung eingeführt und in der die DSK speziell mit der Vollziehung bestimmter Aufgaben betraut werden sollte. Angesichts der besonderen Wichtigkeit dieses Gesetzentwurfs sah sich die DSK allerdings veranlasst, dennoch von sich aus eine Stellungnahme gegenüber dem BMVIT und BMJ und gegenüber dem Parlament abzugeben.

schutzrates nicht ersetzt werden, da sie ganz anderer Natur sind. Seitdem der Geschäftsapparat der DSK Mitte 2004 von der für Datenschutz zuständigen Abteilung im BKA getrennt wurde, finden die Erfahrungen der DSK auch nicht mehr automatisch Berücksichtigung in den Stellungnahmen des Verfassungsdienstes des Bundeskanzleramtes. Es scheint daher sachlich absolut geboten, die DSK in das Begutachtungsverfahren für alle Gesetzesentwürfe, die *wichtige* Datenschutzfragen betreffen, einzubeziehen.

Die Befassung und Anhörung der nationalen Datenschutz-Kontrollstelle bei datenschutzrechtlich bedeutsamen Gesetzesprojekten ist selbstverständlicher Standard in den Mitgliedstaaten der EU. Auch Art. 28 Abs 2 der RL 95/46/EG legt wohl – schon um eine umfassende Integration des gesamten datenschutzrechtlichen Erfahrungsmaterials zu gewährleisten – eine Befassung aller Kontrollstellen zugrunde.[11]

b) Zur Öffentlichkeitsarbeit

Die äußerst dynamische Entwicklung im europäischen Datenschutz seit dem Inkrafttreten der RL 95/46/EG am 25. Oktober 1998 hat in den letzten Jahren immer deutlicher werden lassen, welche Unterschiede zwischen den Aufgaben einer „unabhängigen Kontrollstelle“ im Sinne des Art. 28 der RL und jenen einer klassischen österreichischen „Art. 133 Z 4 Behörde“ bestehen - trotz einer eigenen verfassungsrechtlichen Grundlage in den §§ 37 f DSG 2000[12] wird die DSK ihrem Wesen nach ja vielfach noch immer hauptsächlich als Art. 133 Z 4 Behörde gesehen, d.h. als Kollegialbehörde mit richterlichem Einschlag, deren wesentlichste Aufgabe die Entscheidung über Beschwerdefälle ist. Diese Sichtweise entspricht nicht (mehr) dem europäischen Standard: Nach heutigem Verständnis muss eine Unabhängige Kontrollstelle nach Art. 28 der RL nicht nur Datenschutzbeschwerden der Bürger behandeln, sondern vor allem auch öffentlicher Promotor des Datenschutzgedankens sein: Sie muss bestrebt sein, dem durch vielfache gegenläufige Interessen gefährdeten (Grund)Recht auf Datenschutz die notwendige Geltung in den nationalen Ausprägungen der modernen Informationsgesellschaft zu sichern. Dies verlangt kontinuierliche, zielgerichtete und aktualitätsnahe Öffentlichkeitsarbeit (vgl. hiezu etwa die auf der Internationalen Konferenz der Unabhängigen Datenschutzbehörden von London am 3. November 2006 beschlossene Initiative „Datenschutz vermitteln und effektiver gestalten“).[13]

Hierbei ist vor allem auch zu bedenken, dass in der öffentlichen Meinung ein großes Bedürfnis nach Stellungnahme und Erklärung von *unabhängiger, nicht-regierungsnaher* Expertenseite bei aktuell auftretenden Problemen mit Datenschutzbezug besteht.

5.1.5. Zusammenfassung

In den nach Auffassung der DSK von ihr wahrzunehmenden Bereichen „Kontrollverfahren“ und „Zusammenarbeit auf EU-Ebene“ sowie „Öffentlichkeitsarbeit“ besteht dringender Handlungsbedarf hinsichtlich der Personalausstattung der Geschäftsstelle der DSK. Es darf auch darauf hingewiesen werden, dass der in den Erläuterungen zum DSG 2000 und zum E-Governmentgesetz (- für die Stammzahlenregisterbehörde -) angegebene zusätzliche Personalbedarf nur jeweils zur Hälfte tatsächlich zur Verfügung gestellt wurde.

Die DSK sollte in Begutachtungsverfahren für Gesetze mit *wesentlichem* Datenschutzbezug einbezogen werden.

5.2. Zur räumlichen Unterbringung des Geschäftsapparates der DSK

Das DVR ist in einem anderen Gebäude des Bundeskanzleramtes (Hohenstauffengasse) unterge-

[11] Die deutsche Fassung der RL lässt dies nicht so klar erkennen wie die französische Fassung, in der die RL ausgearbeitet wurde: Gegenstand der Befassung der Kontrollstelle sind demnach „élaborations des mésures reglementaires ou administratives“.

[12] Schon den Redaktoren des DSG (1978) war bewusst, dass die Datenschutzkommission mit dem Modell des Art. 133 Z 4 B-VG nicht das Auslangen werde finden können, da sie als „Kontrollstelle“ mit generellen Einschau- und Empfehlungsbefugnissen nicht nur „entscheiden“ sollte, wie dies Art. 133 Z 4 B-VG als einzige Kompetenz einer auf dieser Grundlage existenten Behörde vorsieht. Dem entsprechend wurde eine eigene verfassungsrechtliche Grundlage für eine unabhängige Datenschutzkommission in den §§ 39 und 40 DSG (1978) geschaffen, die in die §§ 37 und 38 des DSG 2000 übernommen wurde.

[13] http://ico.crl.uk.com/files/ComG.PDF

bracht als der Rest der Geschäftsstelle, der seine Diensträume in der Hofburg hat.

Dass dies die Ausnutzung von Synergieeffekten, insbesondere etwa im Sekretariatsbereich, aber auch die fachliche Kommunikation erschwert, steht außer Streit. Es wurde der DSK auch bereits mehrfach versprochen, einen gemeinsamen Standort für die Unterbringung zu beschaffen. Bedauerlicherweise konnte diese Absicht auch in der vorliegenden Berichtsperiode nicht verwirklicht werden.

5.3. Zur organisatorischen Stellung der Datenschutzkommission und ihres Geschäftsapparates

5.3.1. Geschäftsführung

Die Organisation der Geschäftsführung der DSK hinsichtlich der laufenden Geschäfte entspricht nicht mehr den heutigen Erfordernissen: Das geltende Organisationsmodell entstammt den späten 70er Jahren des vorigen Jahrhunderts und geht davon aus, dass eine nebenberufliche Geschäftsführung für die DSK ausreichend sei – nach den Vergütungssätzen der Vergütungsverordnung, BGBl II 145/2006, offenbar im Ausmaß von etwa 20 Stunden im Monat, wobei die Sitzungsvorbereitung und -teilnahme in diesen Zeitaufwand aber bereits mit einzurechnen wäre. Die tägliche Arbeit der DSK ist seit 1980 so angewachsen und so vielfältig geworden, dass der Einsatz eines „Nebenerwerbs-Geschäftsführers“ den Anforderungen einer effizienten Geschäftsführung nicht mehr genügen kann: Auch wenn dem „Nebenerwerbs-Geschäftsführer“ ein vollbeschäftigter Geschäftsstellenleiter zur Seite steht, kann auf diese Weise das Auslangen nicht gefunden werden, da letzterer die zahllosen notwendigen eigenverantwortlichen Entscheidungen nicht selbst treffen kann, sondern immer bei den entscheidungsbefugten Organen der DSK rückfragen muss, was z.B. die Befassung des GfM mit Aufgaben der DSK weit über den für eine Nebentätigkeit üblichen Rahmen hinaus zur Folge hat. Auch auf europäischer Ebene kann mit dem Auftreten eines Geschäftsstellenleiters nicht das Auslangen gefunden werden – in der Art. 29 Gruppe sind Kommissionsmitglieder als Vertreter der nationalen Datenschutz-Kontrollstellen gefragt. Diese Tätigkeit kann z.B. keinesfalls auch noch innerhalb der vorgegebenen 20 Monatsstunden erbracht werden.

Gerade die Befassung mit Aufgaben im Rahmen der Art 29 Gruppe hat im Rahmen der Festlegung der dienstrechtlichen Rahmenbedingungen keine ausreichend klare Berücksichtigung gefunden. Den sich aus den spezifischen Wirkungen der Richtlinie ergebenden Unklarheiten sollte durch eine deutlichere gesetzliche Umsetzung abgeholfen werden.

5.3.2. Datenschutzkommission und Staatsreform

5.3.2.1. Die derzeit erkennbaren Konsequenzen des Reform-Modells für die Rechtsschutzzuständigkeiten in Datenschutzangelegenheiten

Der vor Kurzem zur Begutachtung versendete Entwurf der Expertengruppe Staats- und Verwaltungsreform im Bundeskanzleramt (Stand 23. Juli 2007), mit dem der erste Teil der so genannten „Staatsreform“ in Form einer Novelle zum B-VG (B-VG (neu)) umgesetzt werden soll[14], hat unter anderem die Entlastung des Verwaltungsgerichtshofs und die Ablösung der bisherigen Berufungsbehörden (2. Instanz) durch die neu zu schaffenden Verwaltungsgerichte zum Gegenstand. In diesem Zusammenhang sieht der Entwurf auch verschiedene, die DSK betreffende Änderungen der gegenwärtigen Rechtslage vor:

- Die **Auflösung der Datenschutzkommission:** Gemäß Art. 151 Abs. 37 Z 4 B-VG (neu) werden mit Inkrafttreten der in Art. 151 Abs. 37 Z 3 angeführten Bestimmungen die in der Anlage 1 bezeichneten Institutionen aufgelöst; die Datenschutzkommission ist in der Anlage 1 unter Z 23 angeführt;
- die **Übertragung der Aufgaben** der aufgelösten Behörden **auf die neuen Verwaltungsgerichte** (Art. 151 Abs. 37 Z 4 B-VG (neu)) – welche wird nicht näher festgelegt;
- ein **neuer Art. 20 B-VG** enthält in seinem 2. Absatz eine Regelung, wonach durch Gesetz Organe geschaffen werden können, die von der

[14] http://www.parlinkom.gv.at/portal/page?_pageid=908,6614640&SUCHE=J&_dad=portal&_schema=PORTAL#

„Bindung an Weisungen der ihnen vorgesetzten Organe freigestellt“ sind.

Die Kompetenz der Verwaltungsgerichte soll sich auf die **Rechtmäßigkeitsprüfung von Bescheiden** und von **unmittelbarer behördlicher Befehls- und Zwangsgewalt** erstrecken (Art. 130 Abs. 1 Z 1 und 2 B-VG (neu)). Darüber hinaus können einfache (Bundes- oder Landes)Gesetze weitere Zuständigkeiten der Verwaltungsgerichte zur Entscheidung über Beschwerden wegen Rechtswidrigkeit vorsehen.

Die DSK entscheidet **NICHT** über Beschwerden betreffend die Rechtswidrigkeit von Bescheiden oder unmittelbarer behördlicher Befehls- und Zwangsgewalt. Die Tätigkeiten der DSK sind daher von Art 130 Abs 1 Z 1 und 2 B-VG (neu) nicht erfasst, sie haben vielmehr Folgendes zu Gegenstand:

– die Entscheidung über die zwischen „Parteien“ strittige Verwendung von personenbezogenen Daten („Streitverfahren“), die **nicht** durch Bescheid oder die Anwendung behördlicher Befehls- und Zwangsgewalt erfolgte: Erfolgt sie nämlich durch Bescheid, dann ist das im Instanzenzug übergeordnete Organ anzurufen; erfolgt sie durch die Ausübung unmittelbarer Befehls- und Zwangsgewalt, sind derzeit die Unabhängigen Verwaltungssenate zuständig. Zu den Streitverfahren sind auch die Verfahren über behauptete Verletzungen des Auskunfts-, Berichtigungs- oder Löschungsrechts zu zählen;

– bestimmte „amtswegige“ Ombudsmannverfahren, Registrierungs- und Genehmigungsverfahren, amtswegige Prüfverfahren („Präventivverfahren“) und sonstige verfahrensfreie Aufgaben.

Daraus folgt, dass die Verwaltungsgerichte keine verfassungsrechtlich abgesicherten Zuständigkeiten besitzen, nach welchen Aufgaben der DSK besorgt werden könnten. Dennoch sieht Art. 151 Abs. 37 Z 4 B-VG (neu) vor, dass die DSK mit Inkrafttreten des Art. 130 aufgelöst wird und ihre Zuständigkeiten auf die Verwaltungsgerichte übergehen.

Aus den Art. 130 und 151 allein ist nicht gesichert – wovon aber offenbar implizit ausgegangen wird –, dass der einfache Gesetzgeber die derzeitigen Zuständigkeiten der DSK nach Art. 130 Abs. 1 **zweiter Satz** B-VG (neu) auf die Verwaltungsgerichte als zusätzliche Kompetenzen übertragen wird. Dies ist auch kompetenzrechtlich nicht so unproblematisch, dass mit einer rechtzeitig geänderten Rechtslage auf einfachgesetzlicher Stufe sicher gerechnet werden kann; dies aber lässt die vorgeschlagene Regelung auch aus gemeinschaftsrechtlicher Perspektive bedenklich erscheinen, weil hier ein Vakuum hinsichtlich der Umsetzung des Art. 28 der RL 95/46/EG entstehen könnte (siehe dazu Näheres im folgenden Punkt 5.3.2.2.).

Hinzu kommt, dass die Grenze der auf die Verwaltungsgerichte durch einfaches Gesetz zusätzlich übertragbaren Kompetenzen so gezogen ist, dass es sich immer um „Beschwerden wegen Rechtswidrigkeit“ handeln muss. Gemessen am Kompetenzumfang der DSK kämen daher überhaupt nur die Beschwerdeverfahren nach § 31 DSG 2000 für eine Übertragung durch einfaches Gesetz in Frage, wobei sich ein besonderes Problem jedoch hinsichtlich der Beschwerden über Verletzungen des Auskunftsrechts durch private Auftraggeber ergibt: Von den „Beschwerden wegen Rechtswidrigkeit“, die vor einem Verwaltungsgericht abzuhandeln wären, kann ja wohl nur rechtswidriges Verhalten von Verwaltungsbehörden erfasst sein, d.h. dass behauptetes rechtswidriges Verhalten von privaten Auftraggebern nur dann (mittelbarer!) Gegenstand eines Verfahrens vor einem Verwaltungsgericht sein könnte, wenn darüber bereits ein Bescheid ergangen wäre, der nun vor dem Verwaltungsgericht angefochten wird. Da dies bei den Auskunftsbeschwerden im privaten Bereich nicht der Fall ist, müssten diese daher auf die ordentlichen Gerichte übertragen werden. Dies könnte wiederum nur durch Änderung der Verfassungsbestimmung des § 1 Abs. 2 DSG 2000 geschehen, wofür im Entwurf allerdings keine Vorkehrung getroffen ist.[15] Auch das Schicksal der anderen Kompetenzen der DSK bleibt nach ihrer Auflösung ungewiss. Aus den Erläuterungen geht hervor, dass Zuständigkeiten der aufgelösten Behörden, die sich nicht auf Entscheidungen über Beschwerden beziehen, entweder in die bestehenden Verwaltungsstrukturen eingegliedert oder auf „Sonderbehörden“ übertragen werden sollen (S 22 der

[15] Die Zuständigkeit der DSK – und nicht der ordentlichen Gerichte – für Auskunftsbeschwerden im privaten Bereich war ein erklärtes Ziel des DSG 2000: „Um auch bei Aufrechterhaltung des geteilten Rechtsschutzsystems eine Vereinfachung des Zugangs zum Rechtsschutz für die Betroffenen zu bewirken, soll jedoch das Recht auf Auskunft – unabhängig davon, ob der belangte Auftraggeber dem öffentlichen oder dem privaten Bereich zuzurechnen ist – in Hinkunft vor der Datenschutzkommission durchsetzbar sein. Dies scheint deshalb so wichtig, weil der Inhalt der Auskunft in den meisten Fällen entscheidend ist für die Frage, ob der Betroffene sinnvollerweise ein Verfahren wegen Löschung, Berichtigung oder Unterlassung der Verwendung anstrengen soll“ (1613 BeilNR XX GP).

Erläuterungen). Die DSK ist in diesem Zusammenhang ausdrücklich erwähnt. Da die Übertragung der Restaufgaben der DSK (- die im Übrigen den überwiegenden Teil ihrer Tätigkeit darstellen -) auf die Verwaltungsbehörden unterster Instanz schon ihres Kontrollcharakters wegen nicht ernsthaft in Erwägung gezogen werden kann, muss geschlossen werden, dass den Redaktoren des Entwurfs offenbar die Einrichtung einer Nachfolgebehörde für die DSK nach dem Modell der Sonderbehörden nach Art. 20 Abs. 2 B-VG (neu) als Lösung vorschwebte. Dies bedarf einer eingehenden Diskussion.

5.3.2.2. Zu den gemeinschaftsrechtlich und verfassungsrechtlichen Vorgaben für die Ausgestaltung des Rechtsschutzes in Angelegenheiten des Datenschutzes

a) Nach Art. 28 Abs. 1 der RL 95/46/EG muss es in jedem Mitgliedsstaat der Europäischen Union „eine oder mehrere Behörden“[16] geben, die zur Überwachung der Einhaltung der nationalen Datenschutzgesetze berufen sind. Art. 28 enthält auch einen umfangreichen Katalog von Mindestkompetenzen dieser nationalen Kontrollstelle(n). Alle Mitgliedstaaten haben diese Bestimmung so umgesetzt, dass sie **eine** eigens für diese Aufgabe zuständige nationale Behörde geschaffen haben.[17] Diese gleichartige Umsetzung in den Mitgliedstaaten der Union zeigt deutlich, dass nur von einer eigens auf die Aufgabe der Datenschutz-Kontrolle konzentrierten Behörde die notwendige Durchschlagskraft, gegründet auch auf besonderen Sachverstand, erwartet werden darf. Die Betrauung der Verwaltungsgerichte mit den Beschwerdeverfahren in Angelegenheiten des Datenschutzes würde eine erhebliche Schwächung der Durchschlagskraft der österreichischen Datenschutz-Kontrollstelle bedeuten.

b) Gemeinschaftsrechtliche Vorbedingung für die Tätigkeit der nationalen Datenschutz-Kontrollstelle ist, dass sie ihre Tätigkeit „in völliger Unabhängigkeit“ ausübt. Dies setzt neben der funktionalen Unabhängigkeit, die in Österreich derzeit zweifelsfrei gegeben ist, auch eine entsprechende **organisatorisch/institutionelle** Komponente voraus, für die die organisatorische Trennung von anderen Behörden, dokumentiert etwa durch die Existenz eines eigenen Budgets, maßgeblich wäre.

Art. 20 B-VG (neu) enthält nun in seinem 2. Absatz eine Regelung, wonach durch (einfaches) Gesetz Organe geschaffen werden können, die von der „Bindung an Weisungen der ihnen vorgesetzten Organe freigestellt“ sind. Die Aufzählung der Aufgaben, für die eine solche Freistellung erfolgen darf, enthält u.a. auch den Fall, dass „dies nach Maßgabe des Rechts der Europäischen Union geboten ist“, was offenbar auch den Fall des Art. 28 der RL betreffen soll. Falls eine solche Freistellung von der Weisungsbindbarkeit erfolgt, gilt Folgendes: „Durch Gesetz ist ein angemessenes Aufsichtsrecht der obersten Organe über die weisungsfreien Organe vorzusehen, insbesondere das Recht, sich über alle Gegenstände der Geschäftsführung der weisungsfreien Organe zu unterrichten, und das Recht, weisungsfreie Organe aus wichtigen Gründen abzuberufen“.

Würde diese Rechtsgrundlage für die Schaffung einer neuen Datenschutz-Kontrollstelle herangezogen, wäre Folgendes, vergleichend zur jetzigen Situation, festzustellen:

Derzeit sind die Organe der DSK nicht weisungsbindbar. Eine „Aufsicht“ des Bundeskanzlers über die Organe der DSK gibt es nicht[18], vielmehr hat die DSK mindestens alle 2 Jahre einen Bericht über ihre Tätigkeit zu veröffentlichen, in dem darzulegen ist, wie die DSK ihre Aufgaben erfüllt. Eine Abberufung der Mitglieder der DSK durch den Bundeskanzler (oder die Bundesregierung) gibt es ebenfalls nicht – vorzeitiger Amtsverlust tritt nur durch Feststellung der DSK selbst nach § 36 Abs. 6 DSG 2000 ein. **Gemessen an der derzeitigen Rechtslage, würde die neue Rechtslage somit einen echten Rückschritt für die Unabhängigkeit der DSK bedeuten.**

c) Wollte man das Konzept des Art. 20 Abs. 2 B-VG (neu) auf eine neu zu schaffende Datenschutz-Kontrollstelle nach Art. 28 der RL anwenden, stellt sich daher vor allem auch die Frage, wie eine Institution, die auch die Obersten Organe kontrollieren muss, „in völliger Unabhängigkeit“ agieren kann, wenn sie der Aufsicht der zu kontrollierenden Organe unterstellt ist und von diesen sogar abberufen werden kann. Das Konzept des Art. 20 Abs. 2 B-VG

[16] „Die Richtlinie nimmt damit Rücksicht auf die föderalistische Struktur mancher Mitgliedstaaten“, wie Dammann/Simitis, Kommentar zur EG-Datenschutzrichtlinie, S. 306, RZ 4, ausführen.

[17] In manchen Ländern, z.B. in Deutschland und Spanien, gibt es darüber hinaus derartige Behörden zusätzlich auch auf Landes/Regionsebene.

[18] Nur die Mitarbeiter der Geschäftsstelle unterliegen der Dienstaufsicht durch den Bundeskanzler (vgl. e contrario § 37 Abs. 2 DSG 2000).

(neu) ist sichtbar inadäquat für eine neue Datenschutz-Kontrollstelle. Ähnlich gelagerte Probleme haben schon 1993 zum Erkenntnis des VfGH Zl. 139/93,G140/93,G141/93 geführt, wodurch § 14 DSG (1978) mit der Begründung aufgehoben wurde, dass eine einfachgesetzliche Bestimmung der DSK nicht die Aufgabe der Überprüfung von Handlungen der obersten Organe zuweisen könne[19]. Es besteht daher Grund zur Annahme, dass auch die vorliegende Textfassung des Art. 20 Abs. 2 B-VG (neu) als Grundlage für die Übertragung der Kontrolltätigkeiten der DSK über die obersten Organe durch einfaches Gesetz untauglich ist.

5.3.2.3. Zweckmäßigkeitserwägungen

Die Auswirkungen des gegenständlichen Entwurfs einer B-VG-Novelle auf die DSK sind jedoch nicht nur aus gemeinschaftsrechtlichen und verfassungsrechtlichen Gründen abzulehnen, sondern auch aus Zweckmäßigkeitserwägungen:

- Wie oben dargelegt, könnten an die Verwaltungsgerichte maximal die Beschwerdeverfahren nach § 31 DSG 2000 abgetreten werden, wobei die Auskunftsbeschwerden über private Auftraggeber allerdings den ordentlichen Gerichten übertragen werden müssten. Für alle anderen Aufgaben der DSK müsste entsprechend den Vorgaben des Art. 28 der RL 95/46/EG jedenfalls nach wie vor eine Datenschutz-Kontrollstelle eingerichtet werden. Ein durch die Auflösung der DSK erzielbarer nennenswerter Einsparungseffekt ist daher nicht erkennbar. Eine derartige Zersplitterung der fachkundigen Ressourcen – die schon jetzt schwer in zufriedenstellendem Ausmaß aufbringbar sind – scheint untunlich.
- Die neuen Verwaltungsgerichte sollen überprüfende Funktion hinsichtlich der staatlichen Verwaltung haben. Da die DSK jedoch **erste** Instanz ist, würde bei der Übertragung ihrer Kompetenzen auf die Verwaltungsgerichte diesen nunmehr erstinstanzliche Tätigkeit zufallen, was der Konzeption der Verwaltungsgerichtsbarkeit neuen Typs widerspricht und wofür daher wohl auch die Aufbau- und Ablauforganisation der Verwaltungsgerichte nicht ideal geeignet sein wird.
- Weiter ist zu bedenken, dass der Rechtsschutz in Angelegenheiten des Datenschutzes derzeit von der DSK in erster und einziger Instanz gewährt wird; gegen ihre Entscheidungen kann unmittelbar der Verfassungs- und der Verwaltungsgerichtshof angerufen werden. Dies ist ein Rechtszug, der an Kürze nicht überboten werden kann. Auch hier ist durch Übertragung der Zuständigkeit an die Verwaltungsgerichte nichts zu gewinnen. Soweit die Kompetenzen der DSK an die ordentlichen Gerichte übertragen werden müssten, würde sich im Gegenteil sogar ein grundsätzlich dreistufiger Instanzenzug ergeben.

Der Ersatz der DSK durch die Verwaltungsgerichte – und teilweise zusätzlich durch die ordentlichen Gerichte in Auskunftssachen – erscheint demgegenüber sogar als Nachteil, und zwar im Hinblick auf den mit dem Verlust einheitlicher Spruchpraxis einhergehenden Verlust an Rechtssicherheit, der auch zu einer vermehrten Anrufung des Verwaltungsgerichtshofs – und des Obersten Gerichtshofs (!) – führen wird, was wiederum einem erklärten Ziel der Staatsreform, den Verwaltungsgerichtshof zu entlasten, widerspricht.

Die Verminderung der Rechtssicherheit durch **Aufsplittung** der Zuständigkeiten in Angelegenheiten des Datenschutzes wird sich auch als zusätzlicher Kostenfaktor für die österreichische Wirtschaft erweisen, da sie mit vermehrter Rechtsmittelergreifung und dadurch längerer Verfahrensdauer und höheren Verfahrenskosten Hand in Hand geht. Höhere Verfahrenskosten haben im Übrigen auch alle Bürger, die Beschwerde erheben wollen, zu befürchten, da davon ausgegangen werden kann, dass Verfahren vor den Verwaltungsgerichten schon infolge größerer Förmlichkeit regelmäßig eine anwaltliche Vertretung erfordern werden, während die – relativ informellen – Verfahren vor der DSK gebühren- und kostenfrei sind. Dies gilt noch viel mehr für Auskunftsbeschwerden im privaten Bereich, die ja gerade zwecks Vermeidung von Verfahrenskosten durch das DSG 2000 nicht den ordentlichen Gerichten, sondern der DSK überantwortet wurden – dies müsste bei Inkrafttreten der vorgeschlagenen B-VG-Novelle rückgängig gemacht werden. Die Aufsplittung der derzeitigen Kompetenzen der DSK auf die Verwaltungsgerichte, die ordentlichen Gerichte und neue Sonderbehörden bedeutet auch eine Abkehr von den Prinzipien der modernen Verwaltungsstrukturen, die doch für den Bürger möglichst eine ein-

[19] Leitsatz: „Aufhebung der - untrennbaren - Bestimmungen des DSG über die Möglichkeit der Einbringung einer Beschwerde an die Datenschutzkommission infolge Verfassungswidrigkeit der Betrauung eines Verwaltungsorgans mit der nachprüfenden Kontrolle der Rechtmäßigkeit des Verhaltens (auch) eines obersten Organs der Vollziehung."

heitliche „Anlaufstelle („one-stop-shop"-Prinzip) bringen sollten.

Der Übergang der Zuständigkeit für die Durchführung rechtsförmlicher (Beschwerde-)Verfahren von der DSK auf die Verwaltungsgerichte und – in Auskunftssachen im privaten Bereich – an die ordentlichen Gerichte würde somit eine deutliche Verschlechterung der Situation der Verfahrensparteien mit sich bringen.

5.3.2.4. Zusammenfassung

Die DSK hält das Organisationsmodell des Art. 20 Abs. 2 B-VG (neu) aus den dargestellten Gründen als verfassungsrechtliche Basis für die Einrichtung einer neuen Datenschutz-Kontrollstelle iSd Art. 28 der RL 95/46/EG für ungeeignet; dies insbesondere deshalb, weil eine Kontrollfunktion unter der Aufsicht des zu Kontrollierenden nahe liegender Weise nicht „unabhängig" ausgeübt werden kann. Auch in der Übertragung der rechtsprechenden Funktionen der DSK auf Verwaltungsgerichte und ordentliche Gerichte kann angesichts der zu erwartenden Judikaturzersplitterung und den daraus resultierenden längeren Rechtsschutzwegen kein Vorteil erkannt werden. Insgesamt würde die neue Lösung nur zu einem erheblichen Effizienzverlust und zu Kostensteigerungen für die Gebietskörperschaften und die Verfahrensparteien führen. Hinsichtlich der für die Durchsetzung von Datenschutzrechten so wichtigen Auskunftsbeschwerden würde sogar eine erhebliche Erschwerung des Zugangs zum Recht bewirkt.

Die DSK erachtet daher im Kontext des Expertenentwurfs die Streichung der DSK aus der Anlage 1 und die Einrichtung einer Datenschutz-Kontrollstelle durch eigene Bestimmung im B-VG geboten, wobei die funktionale wie auch die organisatorische Unabhängigkeit der Kontrollstelle garantiert sein muss.

6. Zum Inhalt der im Berichtszeitraum durchgeführten Verfahren[20]

6.1. Beschwerdeverfahren nach § 1 Abs. 5 bzw. § 31 DSG 2000

Gemäß § 1 Abs. 5 DSG 2000 ist die DSK zur förmlichen Rechtsdurchsetzung - d.h. zur Entscheidung über Datenschutz-Beschwerden in **Bescheid**form - berufen, soweit der öffentliche Bereich betroffen ist; im privaten Bereich sind grundsätzlich die ordentlichen Gerichte in Datenschutzsachen zuständig.

Nur hinsichtlich des Rechts auf Auskunft (§§ 1 Abs. 3 Z 1 und 26 DSG 2000) erstreckt sich die Zuständigkeit der DSK zur förmlichen Rechtsdurchsetzung auch auf den privaten Bereich.

6.1.1. Recht auf Auskunft

Als Folge der umfassenden Zuständigkeit der DSK zur förmlichen Durchsetzung des Auskunftsrechts machen Verfahren wegen Verletzung dieses Rechts den weitaus größten Teil der Beschwerdefälle aus.

In diesem Bereich verdienen die folgenden, im Berichtszeitraum durchgeführten Verfahren besondere Erwähnung:

[20] Sämtliche Entscheidungen sind abrufbar im Rechtsinformationssystem des Bundes (RIS) unter http://www.ris.bka.gv.at/dsk/

6.1.1.1. „Massenverfahren“ gegen mehr als 50 Inkassounternehmen (K121.151 und K121.160 bis K121.216)

Im April 2005 brachte ein Beschwerdeführer in einem einzigen Anbringen Beschwerden gegen mehr als 50 Inkassounternehmen ein und zwar mit der Begründung, dass diese allesamt auf seine Auskunftsbegehren nicht reagiert hätten. Abgesehen von einzelnen Fällen, in denen sich herausstellte, dass der Beschwerdeführer gar kein Auskunftsbegehren gestellt hatte, konnte in einem Großteil der Fälle eine Reaktion der Inkassounternehmen zumindest im Nachhinein erreicht werden. Offenbar ist die Pflicht, Auskunftsersuchen binnen 8 Wochen zu beantworten, noch immer nicht allgemein bekannt.

Vollständigkeit und Richtigkeit der Auskunft sind in einem Verfahren, das das Unterbleiben jeglicher Reaktion des Auftraggebers zum Gegenstand hat, nicht zu prüfen. Diese Fragen können nur in einem neuen, nach Auskunftserteilung eingebrachten Beschwerdeantrag an die DSK aufgeworfen werden.

In einigen Fällen erfolgte jedoch auch im Laufe des Beschwerdeverfahrens keine Reaktion, oder es wurde bloß der DSK gegenüber Stellung genommen. Letzteres kann nach der jahrelangen Rechtsprechung der DSK eine Auskunft an den Auskunftswerber aber nicht ersetzen, da nur dieser selbst beurteilen kann, ob ihn eine erteilte Auskunft zufrieden stellt.

Insgesamt ist zu dieser Fallgruppe zu bemerken, dass bei den in die Verfahren involvierten Inkassounternehmen erhebliche Defizite beim korrekten Umgang mit datenschutzrechtlichen Auskunftsbegehren verzeichnet werden mussten.

6.1.1.2. Identitätsnachweis des Auskunftswerbers (K121.225)

In diesem Verfahren wegen Verletzung im Recht auf Auskunft hatte sich die DSK im Besonderen mit dem nach § 26 Abs. 1 DSG 2000 geforderten Identitätsnachweis auseinander zu setzen. Im konkreten Fall war dem Auskunftsbegehren des Beschwerdeführers per E-Mail ein solcher nicht beigelegt, weshalb das Heerespersonalamt als Auftraggeber den Beschwerdeführer mit Schreiben aufforderte, seine Identität durch beglaubigte Unterschrift bzw. beglaubigte Kopie eines Lichtbildausweises oder durch persönliches Erscheinen mit Lichtbildausweis nachzuweisen. Die Vorlage einer gescannten Reisepass-

kopie konnte die Bedenken des Auskunftspflichtigen nicht ausräumen, da statt dem Auskunftswerber sein Bruder (ohne Vollmacht) als Absender und „Verfasser“ des Auskunftsschreibens aufschien.

Die DSK stellte fest, dass Auskunftsbegehren auch per E-Mail gestellt werden können – gerade im Hinblick auf die im gegenständlichen Fall verwendete E-Mail-Adresse ist der Auftraggeber seiner pflichtgemäßen Sorgfalt, zum Identitätsnachweis aufzufordern, nachgekommen. Der von § 26 Abs. 1 DSG 2000 geforderte „Identitätsnachweis“ umfasst aber nicht nur eine so exakte Beschreibung einer Person („Identitätsbeschreibung“), dass sie ohne Verwechslungsgefahr in den Datenanwendungen des Auftraggebers gesucht werden kann, sondern auch den „Echtheitsanschein“ des Auskunftsbegehrens, d.h. dass das Auskunftsbegehren auch tatsächlich von der als Auskunftswerber genannten Person stammt. Der Nachweis ist wohl eine conditio sine qua non eines Auskunftsbegehrens, auf sein Fehlen muss der Antragsteller nach dem Gebot der Datenverarbeitung nach Treu und Glauben (§ 6 Abs. 1 Z 1 DSG 2000) aufmerksam gemacht werden und es muss ihm Gelegenheit zur Verbesserung gegeben werden. Erfolgt keine Verbesserung, liegt nicht einmal ein Auskunftsbegehren im Sinne des § 26 Abs. 1 DSG 2000 vor. Für die Frage, wie ein „Identitätsnachweis iSd § 26 Abs. 1 DSG 2000“ zu erbringen ist, ist darauf abzustellen, was geeignet ist darzutun, dass das Auskunftsbegehrens von der als Auskunftswerber bezeichneten und in ihrer Identität amtlich bestätigten Person herstammt. Dies kann eine Kopie eines Ausweises mit Unterschrift zum Vergleich mit jener auf dem Begehren sein oder jede andere Art sein, welche die Echtheit im obigen Sinne außer Zweifel stellt. Die Beschwerde wurde abgewiesen.

6.1.1.3. Auftraggeber- bzw. Dienstleistungsbegriff (K121.217 und K121.220)

Daten über von einer Sozialversicherungsanstalt eingeleitete Exekutionsverfahren werden von einer Kreditauskunftei (A) als negative Bonitätsdaten der Schuldner in einer öffentlich zugänglichen Kreditinformationsdatenbank gespeichert. Als Quelle dieser Informationen wurde von der Auskunftei A eine andere Kreditauskunftei B benannt.

Gegenüber der Sozialversicherungsanstalt hatte A die Auskunftserteilung hinsichtlich der von B stammenden Datenbestände abgelehnt, weil dafür B Auftraggeber sei. Dagegen erhob die Sozialversicherungsanstalt Beschwerde an die DSK (K121.217).

Das Ermittlungsverfahren ergab, dass zwischen A und B ein Vertrag bestand, wonach B seine Bonitätsdaten A zur Vermarktung über das Onlineportal von A überlasse. Dafür zahlt A an B einen monatlichen Geldbetrag. Für den Inhalt der Daten (einschließlich eine allfällige Löschung) war jedoch ausschließlich B verantwortlich. Die Daten aus der Datenbank von B erscheinen im Onlineportal abgegrenzt von den eigenen Daten von A.

Die DSK qualifizierte das Verhältnis zwischen A und B als Dienstleistungsverhältnis im Sinn des DSG 2000, weil es datenschutzrechtlich für die Zuordnung zu einer dieser Rollen zunächst auf die faktische Verfügungsgewalt ankommt, die eben bei B liege, was auch aus der abgegrenzten Darstellung im Onlineportal erhelle. Aus diesem Grund war nach dem erhobenen Sachstand die gegen A gerichtete Beschwerde abzuweisen.

6.1.1.4. Auftraggeberstellung von Inkassounternehmen (K121.155)

Im Herbst 2006 hatte die DSK über einen Fall zu entscheiden, in dem ein Inkassounternehmen die Erteilung einer Auskunft mit der Begründung abgelehnt hatte, es sei lediglich Dienstleister der Bank, welche den Inkassoauftrag erteilt habe. Im Zuge einer Einschau ergab sich jedoch, dass das Unternehmen - unter Berufung auf abgabenrechtliche Buchführungspflichten – die Daten des einzelnen Inkassofalles über den Abschluss hinaus mehrere Jahre lang aufbewahrte. Darin sah die DSK einen über die bloße Auftragserfüllung hinausgehenden Zweck der Datenverwendung durch das Inkassounternehmen und leitete daraus dessen Auftraggeberstellung ab, sodass der Beschwerde über die Nicht-Erteilung der Auskunft Folge zu geben war.

Im Auskunftsverfahren wird nicht über die Rechtmäßigkeit der Datenverwendung entschieden, sondern nur über die Frage, ob und inwieweit von dem um Auskunft Ersuchten Auskunft zu erteilen ist.

6.1.1.5. Kein Anspruch auf Bekanntgabe konkreter Mitarbeiter des Auftraggebers oder eines Dritten im Zuge einer Auskunft (K121.038)

Der Auftraggeber hatte dem Beschwerdeführer zwar Auskunft zu den in seiner Datenbank verarbeiteten Daten sowie zu deren Herkunft erteilt, nicht jedoch die konkreten MitarbeiterInnen benannt, die die Daten eingegeben hatten. Ebenso waren in der Auskunft die Namen jener Personen nicht enthalten, die bei der Herkunftsquelle die Daten an den Auftraggeber übermittelt hatten. Dadurch erachtete sich der Beschwerdeführer in seinem Recht auf Auskunft verletzt.

Die DSK vermochte in dem geschilderten Sachverhalt jedoch keine Rechtsverletzung zu erkennen: Auch wenn die Namen der MitarbeiterInnen gemäß § 14 Abs. 2 Z 7 DSG 2000 protokolliert wurden, handelt es sich dabei weder um „zur Person des Beschwerdeführers (beim Auftraggeber) verarbeitete Daten“ noch um „verfügbare Informationen über ihre Herkunft“ im Sinn des § 26 Abs. 1 DSG 2000. Auch die Funktion des Auskunftsrechts als „Begleitgrundrecht“ spricht gegen eine Benennung einzelner MitarbeiterInnen, weil im Hinblick auf die Rechtsverfolgung für den Auskunftswerber aus ihrer Kenntnis kein Vorteil zu gewinnen ist. Sofern der Auskunftswerber nicht ein besonderes Interesse an einer Benennung der konkreten Personen dartun kann (-etwa weil der Verdacht einer völlig zweckfremden nur im Interesse des Mitarbeiters gelegenen Datenverwendung zur Diskussion steht-), besteht somit kein Auskunftsrecht über die Identität von Mitarbeitern des um Auskunft ersuchten Auftraggebers.

Ebenso genügt es, ein bestimmtes Unternehmen als Datenquelle zu benennen, auch wenn Einzelheiten zu einem konkreten Mitarbeiter dieses Unternehmens als Bearbeiter gespeichert sind: Die nach § 26 Abs. 2 DSG 2000 vorzunehmende Interessenabwägung führte auch hier zu dem Ergebnis, dass dieses Datum für den Beschwerdeführer zur Verfolgung seiner Rechte auf Geheimhaltung bzw. Löschung ohne Bedeutung war und daher das Geheimhaltungsinteresse des betroffenen Mitarbeiters das Interesse des Beschwerdeführers an seiner Benennung überwog.

6.1.1.6. Daten im Zusammenhang mit Internet- und E-mail-Verwendung am Arbeitsplatz; Zutrittskontrollsystem (K121.259)

Der Beschwerdeführer arbeitet in einem öffentlich-rechtlichen Dienstverhältnis für eine Dienststelle des Bundesministeriums für Finanzen (BMF). Er richtete ein umfangreiches Auskunftsbegehren an das BMF als datenschutzrechtlichen Auftraggeber. Ihm wurde teilweise schriftliche Auskunft erteilt, teilweise Einsichtnahme gewährt und Ausdrucke (Screenshots) übergeben. Die Beschwerde rügte die Auskünfte als inhaltlich mangelhaft, insbesondere unvollständig.

Die DSK wies zunächst jenen Teil der Beschwerdeanträge, der auf Leistungsaufträge bzw. faktisches Tätigwerden der DSK sowie auf die Feststellung bereits beseitigter Rechtsverletzungen gerichtet war, als unzulässig zurück. Dies zum einen im Hinblick auf die auf § 40 Abs. 4 DSG 2000 gestützte Rechtsprechung des Verwaltungsgerichtshofes (Erkenntnis vom 27. Juni 2006, Zl. 2005/06/0366), wonach gegenüber Auftraggebern des öffentlichen Bereichs Rechtsverletzungen bloß festzustellen sind (da diese Auftraggeber durch § 40 Abs. 4 DSG 2000 gesetzlich zur unmittelbaren Umsetzung der Rechtsansicht der DSK verpflichtet sind) und zum andern im Hinblick darauf, dass an der Feststellung einer bereits behobenen Rechtswidrigkeit von Datenverwendungsvorgängen ein Rechtsschutzinteresse des Beschwerdeführers fehlt.

Die DSK stellte weiters fest, dass Log-Files von Internet-Verbindungen (Webzugang) dann personenbezogene Daten sind, wenn der Auftraggeber parallel zur Aufzeichnung der Internet-Verkehrsdaten pro Endgerät (Log-Files) auch Aufzeichnungen führte, welches Gerät wann von welchem User benutzt wurde (Log-in-Files). Den Einwand des Beschwerdegegners, es handle sich hier um sequenziell gespeicherte Protokolldaten gemäß § 14 DSG 2000, die (Hinweis auf die Gesetzesmaterialien zum DSG 2000) nicht dem Auskunftsrecht unterlägen, verwarf die DSK. Zum einen handle es sich hier nicht um Protokolldaten mit dem Zweck, unberechtigte Zugriffe auf Datenanwendungen des Beschwerdegegners zu vermeiden, da im Beschwerdefall Zugriffe auf nicht dem Auftraggeber zuzurechnende Datenanwendungen (Zugriffe des Beschwerdeführers auf Websites) protokolliert würden. Zum anderen wäre ein kategorischer Ausschluss des Auskunftsrechts bei Protokolldaten grundrechtswidrig. Der Gesetzgeber habe mit der Bezugnahme auf sequenziell gespeicherte Protokolldaten nur zum

Ausdruck bringen wollen, dass in diesen Fällen regelmäßig unverhältnismäßiger Suchaufwand vorliege, der beim Auftraggeber zu einer Ablehnung der Auskunftserteilung gemäß § 26 Abs. 2 DSG 2000 führen werde. Der Beschwerdegegner müsse daher – vorbehaltlich von Ausschlussgründen nach § 26 Abs. 2 DSG 2000 – in derselben Weise und unter Nutzung derselben (technischen) Suchinstrumente über Protokolldaten Auskunft erteilen, mit welchen er selbst eine Suche zu den von ihm angestrebten Zwecken (z.B. Überprüfung auf strafrechtswidrige Internetnutzung) durchführen würde. Dies gelte neben dem Internetzugang auch für das beim Beschwerdegegner betriebene Zutrittskontrollsystem.

Hinsichtlich jenes Teils des Auskunftsbegehrens, das auf Auskunft über den eigenen E-Mail-Account auf EDV-Anlagen des Dienstgebers (gespeicherte E-Mails, gesendete wie empfangene) abzielte, befand die DSK, dass, unter Berücksichtigung des Rechtsschutzinteresses des Betroffenen, eine Auskunft über Inhalte, die der Betroffene (dem hier überdies eine auftraggeberähnliche Stellung zu komme) selbst einsehen könne, den Auftraggeber unverhältnismäßig beansprucht und durch § 26 Abs. 2 DSG 2000 beschränkt ist. Dies gelte aber nicht für Fragen danach, wer auf Daten des (dienstlichen) E-Mail-Accounts zugegriffen hat; die Verweigerung dieser Auskunft habe das Auskunftsrecht des Beschwerdeführers verletzt. Hinsichtlich der Daten einer organisationsinternen Terminverwaltung war von Einsehbarkeit für den Betroffenen und dienstlicher „Quasi-Öffentlichkeit“ der Daten auszugehen, bei der Mitarbeiter und Vorgesetzte nicht als „Übermittlungsempfänger“ gelten können. Eine Auskunft über die Terminverwaltungsdaten wurde daher vom BMF zu Recht abgelehnt.

6.1.1.7. Bonitätsdaten einer Kreditauskunftei (K121.049, s. auch bereits K120.981)

Im Zusammenhang mit einem Auskunftsbegehren über eine Bonitätsbewertung (Rating), welche nach einem vom Beschwerdegegner entwickelten System aus verschiedenen Daten der Betroffenen erstellt wird, hat die DSK festgestellt, dass auch die Herkunft der Daten konkret, d.h. mit Bezeichnung und Anschrift der Quelle zu beauskunften seien. Das Auskunftsrecht steht zwar unter einem doppelten Gesetzesvorbehalt, insofern es seine Grenzen auch in den überwiegenden berechtigten Interessen des Auftraggebers oder eines Dritten hat, (§ 1 Abs. 3 und 4 iVm Abs. 2 DSG 2000; § 26 Abs. 3 DSG 2000); der Beschwerdegegner hat sich aber zu Unrecht auf das Betriebsgeheimnis einer Kreditauskunftei berufen (also auf überwiegende berechtigte Interessen des Auftraggebers bzw. Dritter), wenn es um die Angabe der konkreten Quelle einer Bonitätsinformation geht; vielmehr ist ein überwiegendes berechtigtes Interesse des Beurteilten an der konkreten Benennung der Herkunft dieser Daten gegeben, da er nur dadurch die Möglichkeit zu einer Richtigstellung seiner Daten erlangt.

Eine Beschwerde beim Verwaltungsgerichtshof gegen diesen Bescheid wurde mit Erkenntnis vom 23. Jänner 2007, Zl. 2006/06/0039, als unbegründet abgewiesen. Da die DSK den Beschwerdeführer (nur) verpflichtet habe, die Identität der Bank(en) und Lieferanten anzugeben, welche Quelle gespeicherter Bonitätsdaten waren, aber nicht aufgetragen habe, den Inhalt der jeweils übermittelten Daten bekannt zu geben, ist ein überwiegendes Interesse der Kreditauskunftei oder ihrer Informanten an einer Geheimhaltung dieser Angaben nicht zu erkennen.

6.1.1.8. Verarbeitung geschätzter Altersangaben durch einen Adressverlag (K121.241)

Die Beschwerdeführerin fühlte sich dadurch verletzt, dass ihr die Beschwerdegegnerin, ein Direktmarketingunternehmen nach § 151 GewO, die Herkunft ihres überdies unrichtigen Geburtsdatums nicht mitgeteilt habe. Die Beschwerdegegnerin habe eine Alterszuordnung aufgrund eines technischen Annäherungsverfahrens ermittelt, das auf der Häufigkeit bestimmter Vornamen in bestimmten Jahrgängen basiert. Tatsächlich hat eine Einschau in die Datenanwendungen der Beschwerdegegnerin ergeben, dass das Geburtsdatum der Beschwerdeführerin nicht gespeichert ist, diese aber einer „Altersgruppe 3 (46-60 Jahre)“ zugeordnet worden war. Die Beschwerdeführerin vermutete, dass ein konkretes (falsches) Geburtsdatum Selektionskriterium für Aussendungen der Beschwerdegegnerin gewesen sei.

Die DSK stellte fest, dass eine bloße Vermutung nicht geeignet ist, das Ergebnis der Einschau zu entkräften. Auch war in den Werbezusendungen (Gesundheitsprodukte) nie von einem konkreten Geburtsdatum die Rede. Berechnungsverfahren wie das im konkreten Fall angewandte zur Bestimmung der Altersgruppe sind auch durch die Verhaltensregeln gemäß § 6 Abs. 4 DSG 2000 für die Ausübung des Gewerbes gemäß § 151 Gewerbeordnung (Ad-

ressverlage und Direktmarketingunternehmen) gedeckt. Nach Abs. 4 Z 7 der Verhaltensregeln kann die zu bewerbende Zielgruppe anhand von für Marketingzwecke erhobenen Marketinginformationen oder -klassifikationen (wie hier eben die Altersgruppe), die namentlich bestimmten Personen aufgrund von Marketinganalyseverfahren zugeschrieben werden (sachbezogene Vermutungen und Typologien), definiert werden. Da diese Zuordnung beauskunftet worden war, was die Auskunftsverpflichtung erfüllt, weshalb die Beschwerde abzuweisen war.

6.1.2. Recht auf Geheimhaltung

6.1.2.1. Kriminalpolizeiliche Ermittlungen (K121.052, K121.053, K121.064, K121.065, K121.104 bis K121.106, K121.108)

In dieser Berichtsperiode setzte sich eine Serie von Beschwerdeverfahren ein und desselben Beschwerdeführers fort, bei der die ersten Entscheidungen bereits im Mai/Juni 2005 ergangen waren. Dieser Beschwerdeführer war Beamter im BMI, gegen den durch das Büro für Interne Angelegenheiten (BIA) des BMI Ermittlungen durchgeführt wurden.

Den Beschwerden wurde hinsichtlich der Ermittlungstätigkeit des BIA, sofern diese vor Einleitung der Voruntersuchung erfolgt war, weitestgehend Folge gegeben und eine Verletzung im Recht auf Geheimhaltung durch das BMI festgestellt. Tragender Grund dafür war das Fehlen der Zuständigkeit des BMI zur Durchführung strafprozessualer Ermittlungen in der Phase der Vorerhebungen, wenn nicht ein nach § 88 StPO erforderlicher Auftrag der Staatsanwaltschaft vorliegt. Bloßer „konsensualer Kontakt“ – dessen dauerndes Bestehen als Rechtfertigung vorgebracht wurde – kann nicht als solcher Auftrag angesehen werden. § 24 StPO erachtete die DSK im vorliegenden Fall nicht als geeignete Rechtsgrundlage für Ermittlungen, weil dessen Anwendungsvoraussetzungen nicht gegeben waren. Nicht Folge gegeben wurde hingegen Beschwerden, die die strafprozessuale Ermittlungstätigkeit nach Einleitung der Voruntersuchung betrafen, weil sie jedenfalls durch den – sehr weiten („alle zweckdienlichen Erhebungen“), jedoch für die DSK bindenden – richterlichen Auftrag gedeckt bzw. – im Fall von Hausdurchsuchungen – sogar überhaupt der Gerichtsbarkeit zuzurechnen und damit von der Zuständigkeit der DSK ausgenommen waren.

6.1.2.2. grenzüberschreitende Amtshilfe in Verkehrssachen zwischen Behörden in Vorarlberg, in der Schweiz, in Deutschland und Liechtenstein (K121.031, K121.047, K121.124)

In mehreren Verfahren stellte sich die Frage, in wie weit österreichische Kfz-Zulassungsbehörden an ausländischen (Verwaltungs-) Strafbehörden auf deren Ersuchen Daten des Zulassungsbesitzers aus der Zulassungsevidenz zwecks Ausforschung des Lenkers nach Verkehrsübertretungen mit österreichischen Kraftfahrzeugen im Ausland übermitteln dürfen.

Die DSK befand dies hinsichtlich der Schweiz und Deutschlands für zulässig und stützte sich dabei abschließend auf § 86 Abs. 3 KFG, hinsichtlich Deutschlands auch auf die Privilegierung deutscher Behörden durch den österreichisch-deutschen Amts- und Rechtshilfevertrag in Verwaltungssachen, BGBl Nr. 526/1990.

Gegen diese zwei Bescheide sind – nach Ablehnung entsprechender Beschwerden durch den VfGH – noch Beschwerden beim VwGH anhängig. Sie wurden auch mehrfach im verkehrsrechtlichen Schrifttum (ZVR 2007/10 ZVR 2006/115 ZVR 2006/38) veröffentlicht und auch glossiert.

Hinsichtlich Liechtensteins wurde einer Beschwerde stattgegeben, da die Anwendbarkeit von § 86 Abs. 3 KFG u.a. wegen der unklaren Rechtslage (unsichere innerstaatliche Kundmachung des Beitritts Liechtensteins zum so genannten „Pariser Übereinkommen“ über den Verkehr von Kraftfahrzeugen aus dem Jahr 1930) nicht möglich erschien.

Mit BGBl. III Nr. 52/2007 erfolgte nunmehr eine Kundmachung des Bundeskanzlers über den Geltungsbereich besagten Staatsvertrags (u.a. noch geltend zwischen Österreich und Liechtenstein), womit nunmehr auch die Anwendbarkeit von § 86 Abs. 3 KFG im Amtshilfeverkehr mit Liechtensteinischen Behörden gegeben erscheint.

6.1.2.3. Veröffentlichung einer parlamentarischen Anfrage mit Personenbezug auf der Homepage des Parlaments (K121.159, K121.224)

Eine parlamentarische Anfrage im Nationalrat, in der der Beschwerdeführer namentlich genannt war, war (wie grundsätzlich alle Verhandlungsgegenstände von National- und Bundesrat) auf der Homepage

des Parlaments veröffentlicht worden, wodurch sich der Beschwerdeführer verletzt erachtete.

Die DSK wies die dagegen erhobene Beschwerde wegen mangelnder Zuständigkeit gemäß § 1 Abs. 5 DSG 2000 zurück, weil die Stellung einer parlamentarischen Anfrage zur Mitwirkung des Nationalrates an der Vollziehung (Art. 50 ff B-VG) zählt und ihre Veröffentlichung durch den Präsidenten des Nationalrates bzw. die Parlamentsdirektion als parlamentarischer Hilfsdienst zu werten und damit der Staatsfunktion Gesetzgebung zuzurechnen ist.

Aus demselben Grunde war auch eine Beschwerde gegen die Ablehnung der Löschung der (mittlerweile von der Parlamentsdirektion anonymisierten) Anfrage von der Homepage zurückzuweisen.

6.1.2.4. Beschlagnahme eines PCs durch Sicherheitsorgane

Eine Betroffene erhob wegen Verletzung ihres Geheimhaltungsrechts Beschwerde gegen eine Sicherheitsbehörde (Bezirkshauptmannschaft) wegen einer vorläufigen Sicherstellung eines PC durch Polizeibeamte im Rahmen von Vorerhebung im Dienste der Strafjustiz (Verdacht der Untreue, Suche nach Buchhaltungsdaten eines Vereins). Die DSK sah ihre Zuständigkeit auf den Zeitraum zwischen der polizeilichen Sicherstellung des PCs und dem Wirksamwerden einer (später erfolgten) gerichtlichen Beschlagnahme sowie auf Fragen der Datenverwendung (möglicher Eingriff in das Recht auf Geheimhaltung durch Ermittlung personenbezogener Daten) beschränkt. Für den Zeitraum der DSK-Zuständigkeit war aber keine Datenermittlung durch die Sicherheitsbehörde nachweisbar. Die bloße Verwahrung des sichergestellten Geräts samt Datenträgern durch eine Polizeidienststelle bis zur Entscheidung des Gerichts über eine Auswertung ist keine Datenermittlung (diese erfolgte durch eine kriminaltechnische Untersuchungsstelle nachweislich erst nach Vorliegen des Beschlusses des Untersuchungsrichters, mit dem der PC beschlagnahmt wurde).

6.1.2.5. Zuständigkeitsabgenzung DSK-UVS bei der Ermittlung erkennungsdienstlicher Daten (insb. DNA-Proben; VwGH-Erkenntnisse vom 19. September 2006, Zl. 2005/06/0018, betreffend das DSK-Verfahren K120.922 –mittlerweile neu auf dieser Rechtslage entschieden, vom 23. Jänner 2007, Zl. 2005/06/0254, betreffend das DSK-Verfahren K120.925 und vom 21. Februar 2007, Zl. 2005/06/0275, betreffend das DSK-Verfahren K121.056)

Die angeführten Beschwerdefälle (die Beschwerden selbst stammen allesamt aus der vorigen Berichtsperiode) befassten sich im Zusammenhang mit möglichen Eingriffen in das Geheimhaltungsrecht mit der Frage der Abgrenzung der Zuständigkeit zwischen DSK und UVS bei der polizeilichen Ermittlung erkennungsdienstlicher Daten (Auslegung von § 90 SPG in der Fassung BGBl. I Nr. 104/2002). Eine typische erkennungsdienstliche Behandlung besteht aus der Abnahme der Fingerabdrücke, Abnahme eines Mundhöhlenabstrichs (DNA-Probe) und Anfertigen von Fotografien. Die Daten werden im Rahmen des EKIS verwendet (zu DNA-Daten vgl. die Sonderbestimmung des § 67 Abs. 2 SPG).

Die DSK hatte dabei zunächst die Auffassung vertreten, dass während einer behördlichen Anhaltung (Untersuchungs- oder Verwahrungshaft auf richterlichen Befehl, Verwahrungshaft nach Festnahme durch eine Sicherheitsbehörde aus eigener Macht) jede erkennungsdienstliche Behandlung die Vornahme einer Datenermittlung zumindest durch Befehlsgewalt der Sicherheitsbehörde sei, da dem Betroffenen in diesem Fall kein Widerstandsrecht zukomme. Die erkennungsdienstliche Behandlung darf – dies ist unstreitig – bei Weigerung auch durch Zwang vollzogen werden. Daraus folge die Zuständigkeit des UVS.

Diese Auslegung des Gesetzes wurde vom VwGH im Erkenntnis vom 19. September 2006, Zl. 2005/06/0018, verworfen. Eine Ausübung von Befehls- und Zwangsgewalt liegt laut verbindlicher Ansicht des Höchstgerichts erst ab dem Moment vor, in welchem dem Betroffenen für den Fall der Nicht-Kooperation die Ausübung von Zwang angedroht wird. Die Zuständigkeit der DSK reicht demnach weiter als bisher angenommen, mehrere Verfahren sind neu zu entscheiden.

6.1.2.6. Datenermittlung im Zuge von Verfahren – „Denkmöglichkeitsjudikatur“ (Ausgangsfall K121.005, vgl. weiters K121.046, K121.050, K121.229, K121.239, K121.277)

Im Ausgangsfall ging es um die Verwendung von Daten der Beschwerdeführerin (zB Versicherungs-

daten, Lohnzettel, KFZ-Zentralregistereintragungen) in einem Umsatzsteuerverfahren gegen Dritte – Beschwerdegegner war dementsprechend ein Finanzamt (§ 52 BAO sowie § 58 iVm. § 61 BAO bzw. iVm. § 58 Abs. 1 lit. f FinStrG), das hier die beim Bundesministerium für Finanzen eingerichtete Großbetriebsprüfung Wien zur Ermittlung herangezogen hatte.

In solchen Fallkonstellationen (Verwendung von Daten in anderen Verfahren) vertritt die DSK in ständiger Entscheidungspraxis (vgl. dazu schon die Bescheide vom 28. Februar 2003, GZ K120.806/002-DSK/2003, und vom 20. Mai 2005, GZ K120.956/0003-DSK/2005), die Rechtsauffassung, dass datenschutzrechtliche Beschwerden nicht geeignet sind, in der Sache vor andere Behörden gehörende Rechtsfragen (wie die Frage der Umsatzsteuerverpflichtung eines Rechtssubjekts oder dessen Verwicklung in einen allenfalls verwirklichten Betrugstatbestand) prüfen zu lassen. Diese Prüfung würde bewirken, dass die DSK – zumindest teilweise – an die Stelle der sachlich zuständigen Behörde tritt und im Umwege über den Abspruch über die Zulässigkeit von Sachverhaltsermittlungen eine sachliche Allzuständigkeit arrogiert. Dies ließe sich weder mit dem Grundsatz der festen Zuständigkeitsverteilung zwischen staatlichen Organen noch mit dem Grundrecht auf ein Verfahren vor dem gesetzlichen Richter vereinbaren.

Maßstab für eine Beurteilung der Zulässigkeit der Datenermittlung in Verwaltungs(straf)verfahren ist das Übermaßverbot als Ausdruck des Verhältnismäßigkeitsgrundsatzes (§ 1 Abs. 2 und § 7 Abs. 3 DSG 2000): Wenn es denkmöglich ist, dass die von einer in der Sache zuständigen Behörde ermittelten Daten nach Art und Inhalt für die Feststellung des relevanten Sachverhalts geeignet sind, ist die Zulässigkeit der (auf Bestimmungen im entsprechenden Verfahrensgesetz, zB § 57 FinStrG, beruhenden) Ermittlung aus datenschutzrechtlicher Sicht gegeben.

Auch kann die DSK über die Richtigkeit der Daten im Sinne der Rechtmäßigkeit der möglichen Bestrafung nicht entscheiden. Nur eindeutig überschießende, weil für den Zweck des durchgeführten Verfahrens (hier: Verwicklung in einen allenfalls verwirklichten Betrugstatbestand) denkunmöglicherweise wesentliche Daten dürfen nicht ermittelt bzw. der sachlich zuständigen Behörde nicht übermittelt (§ 7 Abs. 2 DSG 2000) werden, da dies in das Grundrecht auf Geheimhaltung eingreifen würde.

Im konkreten Fall konnte eine mögliche Verstrickung der Beschwerdeführerin in die geprüften dritten Unternehmen nicht ausgeschlossen werden, weshalb die Beschwerde als unbegründet abzuweisen war.

Gegen den Bescheid wurde sowohl beim Verfassungs- als auch beim Verwaltungsgerichtshof Beschwerde erhoben. Der Verfassungsgerichtshof hat mit Beschluss vom 25. September 2006 die Behandlung der Beschwerde abgelehnt, teils weil die Klärung einer verfassungsrechtlichen Frage nicht zu erwarten war, teils weil die Verletzung so wenig wahrscheinlich war, dass die Beschwerde keine hinreichende Aussicht auf Erfolg hat. Die Beschwerde beim Verwaltungsgerichtshof ist anhängig.

Diese „Denkmöglichkeitsjudikatur“ wurde im Berichtszeitraum mehrfach angewendet und auch auf andere Fälle der Datenverwendung im Rahmen von amtswegigen Verfahren ausgedehnt (zB Begründung der Ablehnung eines sozialversicherungsrechtlichen Anspruches und Ermittlungen im Zuge der Leistung von Amtshilfe).

6.1.3. Recht auf Löschung und Richtigstellung

6.1.3.1. Verwendung der Sozialversicherungsnummer in Schülerevidenzen (K121.021, K121.022, K121.025, K121.026)

Auch diese Serie von Beschwerden nahm ihren Anfang bereits vor Beginn der Berichtsperiode. Die Beschwerdeführer – Schüler vertreten durch ihre Eltern – hatten bei ihren Schulen Anträge auf Löschung der im BildDokG bzw. in der BildDokV zur Verarbeitung vorgesehenen Daten, insbesondere der Sozialversicherungsnummer, eingebracht. Begründet wurde dies ebenso wie die nach Ablehnung der Löschung bzw. Ablauf der achtwöchigen Reaktionsfrist eingebrachten Beschwerden mit Verfassungs- bzw. Europarechtswidrigkeit des BildDokG.

Drei der vier in diese Berichtsperiode fallenden Beschwerden wurden abgewiesen, weil das BildDokG und die BildDokV die Verarbeitung der darin genannten Datenarten durch die Schulen vorschreiben. Eine allfällige Verfassungswidrigkeit des BildDokG kann die DSK als Verwaltungsbehörde nicht aufgreifen. Einen Verstoß des BildDokG gegen die Datenschutzrichtlinie vermochte die DSK deshalb

nicht zu erkennen, weil das BildDokG - anders als von den Beschwerdeführern behauptet - in seinem § 3 Abs. 1 den Zweck der Verarbeitung eindeutig festlegt und somit dem Grundsatz der Zweckbegrenzung nach Art. 6 (1) b DS-RL entspricht.

In einem Fall (betreffend eine Wiener Privatschule) war der Beschwerde allerdings Folge zu geben, weil die Schule auf das Löschungsbegehren überhaupt nicht reagiert hatte.

6.1.3.2. Daten von Polizeidienststellen über Ermittlungen im Zusammenhang mit dem früheren § 209 StGB (ua. K120.828, K120.841, K121.043, K121.127, K121.145)

Zahlreiche Beschwerden – viele Fälle davon gehen jedenfalls in Teilen auch in den letzten Berichtszeitraum zurück - wurden von Personen angestrengt, gegen die wegen der Straftat nach dem früheren § 209 StGB (gleichgeschlechtliche Unzucht mit Personen unter achtzehn Jahren, aufgehoben durch BGBl I Nr. 134/2002, siehe auch VfGH-Erkenntnis vom 21. Juni 2002, VfSlg 16.565) polizeilich ermittelt wurde. Das Begehren lautete stets auf Löschung sämtlicher Daten im Zusammenhang mit den Ermittlungen. Dies betraf neben den (auf Grund eines Erlasses des Bundesministers für Inneres stets bereits gelöschten) EKIS-Daten insbesondere Daten in den automationsunterstützten oder manuellen Dateien, die von den Polizeidienststellen für Zwecke der Aktenverwaltung und Verfahrensdokumentation (AMKO [alt] und PAD [neu, s.o. 1.4.] sowie Indexkarteikarten und Protokollbucheinträge) geführt werden und darüber hinaus den so genannten „Kopienakt“, d.i. der bei der ermittelnden Polizeidienststelle (früher) jeweils geführte Papierakt. (Ein Versuch, über das Verfahren nach § 8 Strafregistergesetz die Löschung von – aufrechten – Verurteilungen wegen § 209 StGB durch Verfügung des Innenministers im Strafregister zu erreichen, scheiterte vor dem VfGH, Erkenntnis vom 4. Oktober 2006, Zl. B 742/06).

In dieser Berichtsperiode sind nunmehr zahlreiche Erkenntnisse von VfGH und VwGH zur Spruchpraxis der DSK in Fragen des Löschungsrechts ergangen. Generell kann gesagt werden, dass die Spruchpraxis der DSK in einigen Punkten für zu behördenfreundlich befunden wurde, wobei aber – bis heute nicht restlos geklärte – Judikaturdivergenzen zwischen beiden Gerichtshöfen entstanden sind:

Der VwGH bestätigte (für die Rechtslage vor der SPG-Novelle BGBl Nr. 151/2004 gegründete) die Ansicht der DSK, dass die Verarbeitung von Personendaten für Zwecke der Aktenverwaltung und der Verfahrensdokumentation zum inneren Dienst der Exekutive gehört und der in Frage kommende datenschutzrechtliche Auftraggeber daher nach den Bestimmungen der §§ 10 und 13 SPG zu bestimmen ist. Der VfGH wertet die gleiche Gesetzesauslegung durch die DSK hingegen als groben Rechtsirrtum und hob einschlägige Bescheide wegen gleichheitswidriger Willkür auf.

Begünstig wurde diese Divergenzen in der höchstgerichtlichen Rechtsprechung auch durch die Verfahrenstaktik der Beschwerdeführer, die von ihrem Recht Gebrauch machten, beide Gerichtshöfe des öffentlichen Rechts parallel anzurufen (statt zuerst den VfGH und erst subsidiär den VwGH damit zu befassen).

Eine Zusammenschau ergibt nunmehr folgende Rechtslage:

Traditionelle Papierakten sind, da sie keine besondere innere Strukturierung aufweisen keine (manuellen) Dateien; für diese Akten kann daher keine „Löschung“ bzw. Vernichtung, gestützt auf das Grundrecht auf Datenschutz durchgesetzt werden. Im Erkenntnis vom 7. März 2007, B 1708/06, hat der VfGH klargestellt, dass ein solches Recht weder aus § 1 DSG 2000 noch unmittelbar aus Art 8 EMRK abgeleitet werden kann.

In manuellen Dateien ist hingegen jeder Bezug auf § 209 StGB zu löschen. (Solche manuellen Dateien existieren bei den Polizeidienststellen noch in Form von archivierten Karteikarten und Protokollbüchern zu Aktenverwaltungs- und Dokumentationszwecken.) Das Interesse der Betroffenen an der Löschung von Eintragungen betr. § 209 StGB, die ja sensible Daten darstellen, überwiegt in diesem Fall jedenfalls auch den – grundsätzlich anerkannten - Dokumentationszweck.

Für die nunmehr automationsunterstützt geführten polizeilichen Aktenverwaltungs- Datenanwendungen (insbesondere „PAD“) ist der Dokumentationszweck in § 13 Abs. 2 SPG (idF BGBl. I Nr. 151/2004) festgelegt, allerdings anders als im Wortlaut von § 27 Abs. 3 DSG 2000 vorgesehen. Dieser Dokumentationszweck in elektronischen polizeilichen Aktenverwaltungssystemen ist im „§-209-Fall“ nicht vorrangig vor dem Löschungsrecht des Betroffenen. Die Notwendigkeit der Verarbei-

tung von Daten in derartigen Datenanwendungen für den angestrebten (Gesamt-)Zweck ist vom Auftraggeber darzulegen, von der DSK zu überprüfen und gegen schutzwürdige Interessen des Betroffenen abzuwägen.

6.1.3.3. Löschung von Daten in einer Krankengeschichte (K121.246)

Diese Entscheidung betraf ebenfalls die Frage, ob der Dokumentationszweck einer Datenanwendung, hier: einer ärztlichen Behandlungsdokumentation, die Löschung von Daten auf Antrag des Betroffenen ausschließt.

Der Beschwerdeführer verlangte die Löschung bzw. Richtigstellung einer Eintragung in einem Ambulanzprotokoll, u.a. mit der Begründung, die Aufzeichnungen enthielten unrichtige Daten, die unbewiesen und von keinem für diese Frage sachkundigen Arzt – der Verfasser der Eintragung sei Zahnmediziner und kein Psychiater – erhoben worden seien (nach Ansicht des Beschwerdeführers sollte die Eintragung nur dazu dienen, die Verweigerung einer bestimmten Behandlung, auf die er Anspruch zu haben glaubte, zu rechtfertigen). Der öffentlich-rechtliche Rechtsträger der Krankenanstalt lehnte als datenschutzrechtlicher Auftraggeber die Löschung ab.

Die DSK wies die dagegen erhobene Löschungsbeschwerde aufgrund folgender Erwägungen ab: Eine Löschung oder Richtigstellung der Daten kommt im Hinblick auf den Dokumentationszweck des Ambulanzprotokolls (§ 27 Abs. 3 DSG 2000) nicht in Frage. In der Frage, ob richtig stellende Anmerkungen gemäß § 27 Abs. 3 2. Satz DSG 2000 vorzunehmen seien, vertrat die DSK die Auffassung, dass das Gebot der Datenrichtigkeit mit dem Verwendungszweck der Daten verknüpft ist, das heißt der Maßstab für die Datenrichtigkeit ist der Zweck der Datenanwendung. Liegt dieser alleine in der Dokumentation von Meinungen bzw. Beurteilungen – dazu zählten auch Befunde und Gutachten von Personen mit bestimmtem Sachverstand, z.B. Ärzten – , so sind die Daten aus datenschutzrechtlicher Sicht richtig, wenn sie diese Meinung oder Beurteilung korrekt wiedergeben.

6.1.3.4. Elektronischer Akt eines Bundesministeriums (K121.131)

Eine weitere Frage des Dokumentationszwecks - nämlich u.a. Fragen der elektronischen Aktenführung - betraf eine Beschwerde, in der unter Berufung auf das Recht auf Löschung das Recht eines Bundesministeriums bestritten wurde, bestimmte Unterlagen in einem (elektronischen) Akt zu dokumentieren, die für ein vom Beschwerdeführer angestrengtes Amtshaftungsverfahren und die Beantwortung einer Beschwerde des Beschwerdeführers bei der Volksanwaltschaft relevant waren.

Die DSK wies die Beschwerde ab. Jeder von der Ergreifung derartiger Rechtsbehelfe betroffenen Behörde muss es zugestanden werden, das damit im Zusammenhang stehende Geschehen auch zu dokumentieren, insbesondere im Hinblick auf die Gebarungskontrolle nach dem 5. Hauptstück des B-VG, die der Verwaltungsgerichtshof in seinem Erkenntnis vom 29. November 2005, Zl. 2004/06/0169, ausdrücklich als einen solchen Zweck begründend anerkannt hat. Hierfür ist es auch zulässig, Daten (hier: in Form von Beweisunterlagen) bei nachgeordneten Behörden zu ermitteln und zu verarbeiten. Ein Anspruch auf richtig stellende Anmerkungen sei ebenfalls im Hinblick auf den Dokumentationszweck nicht gegeben, da aus den Unterlagen klar hervorgehe, dass es sich um Äußerungen in einem kontradiktorischen Verfahren gehandelt hat.

6.2. Kontrollverfahren nach § 30 DSG 2000

Zusätzlich zur unter I. dargestellten förmlichen Rechtsdurchsetzung kann sich nach § 30 Abs. 1 DSG 2000 jedermann wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten nach dem DSG 2000 mit einer Eingabe an die DSK wenden. Dies führt in der Regel zur Durchführung eines so genannten Kontrollverfahrens (auch als „Ombudsmannverfahren“ bezeichnet).

Bei vorabkontrollpflichtigen Datenanwendungen kann ein solches auch ohne Vorliegen einer Eingabe oder auch nur eines konkreten Verdachts durchgeführt werden. Die Durchführung eines solchen Verfahrens ist (anders als beim Beschwerdeverfahren)

unabhängig vom geltend gemachten Recht (Pflicht) bzw. dem angesprochenen Auftraggeber zulässig, und zwar auch dann, wenn die DSK alternativ auch zur förmlichen Rechtsdurchsetzung zuständig wäre.

Ziel ist nach § 30 Abs. 6 DSG 2000 die Herbeiführung eines rechtmäßigen Zustands. Dazu können nötigenfalls auch – nicht unmittelbar verbindliche – Empfehlungen ausgesprochen werden. Häufig kann aber auch ohne den Einsatz dieses Mittels im Zuge solcher Verfahren eine datenschutzrechtlich befriedigende Situation hergestellt werden, wenn sich die Eingabe nicht schon von vornherein als unbegründet erweist.

Im Berichtszeitraum scheinen aus diesem Bereich die folgenden Fälle bzw. Fallgruppen besonders erwähnenswert:

6.2.1. Gegen das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) gerichtete Eingaben wegen Anwendung von § 26 Abs. 2 und 5 DSG 2000 (K210.534, K210.552, K210.559, K210.561)

Hier wandte sich im Mai 2006 zunächst ein in der „Tierschutzszene“ aktiver Einschreiter an die DSK, dem das BVT in einem Auskunftsschreiben mitgeteilt hatte, dass darüber hinaus keine der Auskunftspflicht unterliegende Daten vorliegen würden. Der Einschreiter vermutete, dass unrechtmäßigerweise Daten nicht beauskunftet worden seien.

Als Ergebnis des Auskunftsüberprüfungsverfahrens vermochte die DSK keinen rechtswidrigen Zustand zu erkennen. In ihrer abschließenden Mitteilung an den Einschreiter hielt sie fest, dass einem Auftraggeber, der mit in § 26 Abs. 2 Z 5 DSG 2000 genannten Aufgaben betraut ist, stets zugestanden werden muss, einer Auskunft den Zusatz gemäß § 26 Abs. 5 DSG 2000 anzuschließen („Im Übrigen werden keine der Auskunftspflicht unterliegenden Daten verarbeitet.“); dies unabhängig davon, ob tatsächlich (weitere) Daten vorhanden sind. Andernfalls könnte aus unterschiedlichen Auskünften auf den tatsächlichen Inhalt der Datenanwendungen geschlossen werden, was aber deren geschützte Zwecke vereiteln könnte.

Der DSK sind in solchen Verfahren die zur Person eines Einschreiters verarbeiteten Daten zur Gänze offen zu legen. Sie hat jedoch im Sinne des § 31 Abs. 4 DSG 2000 die geschützten Geheimhaltungsinteressen in ihrem gesamten Verfahren zu wahren. Eine vollständige inhaltliche Auskunft wird daher nur dann angeordnet bzw. selbst vorgenommen, wenn die DSK die Verweigerung der (vollständigen) Auskunft für unrechtmäßig erachtet.

6.2.2. Verwendung von Bonitätsdaten

Zahlreiche Eingaben betrafen die Verwendung von Bonitätsdaten, oft im Zusammenhang mit Kreditauskunfteien (§ 152 GewO), wobei der Großteil der Fälle sich auf drei bestimmte Kreditauskunfteiunternehmen beschränkte.

Häufig endeten die Fälle mit einer Löschung der Betroffenen aus einer Bonitätsdatenbank, wodurch jedenfalls ein rechtmäßiger Zustand hergestellt war. Sofern es sich nicht überhaupt um Verwechslungen oder Irrtümer handelte, vermochten die Einschreiter häufig Gründe anzugeben, die die Aussagekraft der Daten im Hinblick auf ihre Bonitätslage fragwürdig erscheinen ließen; es musste festgestellt werden, dass etwa die begründeten Bestreitung von als unbezahlt vorgemerkten Forderungen oder sogar eine gerichtliche Entscheidung, aus der sich das Nichtbestehen der Forderung ergab, in dem Kreditinformationssystem nicht entsprechend sichtbar gemacht wurde.

In einigen Fällen erachtete die DSK die Bonitätsdatenspeicherung auch als rechtmäßig. Sowohl Kreditauskunfteien als auch deren Datenlieferanten wurden aber daran erinnert, beim Umgang mit derartigen Daten besondere Sorgfalt walten zu lassen und auf die Datenrichtigkeit zu achten.

Derzeit sind bezüglich des Kreditinformationssektors noch mehrere Verfahren über Eingaben (§ 30 Abs. 1 DSG 2000) sowie auch ein amtswegig eingeleitetes Kotrollverfahren (§ 30 Abs. 3 DSG 2000) anhängig, in denen zum Teil auch die Durchführung einer Einschau vor Ort (§ 30 Abs. 2 DSG 2000) durchgeführt wurde.

Besonders erwähnenswert erscheinen die folgenden zwei Fälle, in denen die DSK nach § 30 Abs. 6 DSG 2000 Empfehlungen ausgesprochen hat:

6.2.2.1. Öffentlich zugängliche Bonitätsdatenbank (K211.593)

Der Einschreiter hatte einer Kreditauskunftei die Weitergabe seiner Daten an Dritte untersagt. Die Daten waren in einer Datenbank gespeichert, die für jedermann gegen Zahlung einer Gebühr von EUR 25,-- pro Abfrage zugänglich war. Die Auskunftei behauptete dem Wunsch des Einschreiters dadurch nachgekommen zu sein, dass ersatzweise unter dem Namen des Einschreiters eine Anmerkung angebracht wurde, dass der Einschreiter die Erteilung von Auskünften über ihn nicht wünsche. Daraus könne nicht unmittelbar auf eine verschlechterte Bonitätslage geschlossen werden.

Die DSK hielt zunächst fest, dass das bloße Bestehen einer Kostenpflicht für den Zugang zu einer derartigen Bonitätsdatenbank nichts daran ändert, dass diese als öffentlich zugängliche Datei zu qualifizieren ist, und damit § 28 Abs. 2 DSG 2000 unterliegt.

Die vom Einschreiter begehrte „Auskunftssperre" stellt rechtlich ein Minus zum gesetzlich eingeräumten Löschungsanspruch dar und steht ihm daher ebenso zu. Die „ersatzweise" Verarbeitung und Übermittlung des Hinweises auf den Widerspruch („Wunsch") des Betroffenen ist gesetzlich nicht vorgesehen und stellt eine Aushöhlung des auf volle Löschung (oder entsprechend dem Antrag des Betroffenen auf eine Sperrung) gerichteten Widerspruchsrechts dar. Sie ist daher rechtswidrig, weshalb die DSK die Entfernung des Hinweises empfohlen hat.

6.2.2.2. Datenweitergabe von einem Inkassobüro an eine Kreditauskunftei (K211.773)

Eine Buchhandlung, bei der der Einschreiter ein bestelltes Buch nicht bezahlt hat, hatte mit der Einbringung der Kaufpreisforderung in Höhe von EUR 41,80 ein Inkassobüro beauftragt. Nachdem der Einschreiter von diesem zur Zahlung aufgefordert worden war, bot er eine Zahlung des Betrages samt Spesen in zwei Monatsraten an und leistete auch sogleich eine Zahlung in Höhe von EUR 36,36. Kurz darauf musste er feststellen, dass das Inkassobüro dennoch die Forderung mit EUR 41,80 an eine Kreditauskunftei als offen gemeldet hatte. Daraufhin bezahlte er sogleich (früher als vereinbart) den noch offenen Restbetrag an das Inkassobüro.

Die DSK erachtete diese Vorgangsweise in mehrfacher Hinsicht als rechtswidrig: Wenngleich durch die gesetzliche Anerkennung des Kreditauskunfteigewerbes in § 152 GewO davon auszugehen ist, dass der Gesetzgeber in bestimmten Fallkategorien ein das Betroffeneninteresse überwiegendes berechtigtes Interesse an der Ermittlung, weiteren Verarbeitung und Übermittlung von Bonitätsdaten als gegeben erachtete, muss im Hinblick auf die besondere Eingriffstiefe der Bonitätsdatenverarbeitung, welche im Übrigen auch in § 18 Abs. 2 Z 3 DSG 2000 zum Ausdruck gebracht wird, vor der Weitergabe von Inkassodaten an eine Kreditauskunftei geprüft werden, ob Daten, die auf den ersten Blick bonitätsrelevant scheinen, in Wahrheit keine oder nur sehr beschränkte/unzuverlässige Aussagekraft über die Bonität des Betroffenen besitzen. In diesem Zusammenhang ist auch der sachlichen Datenrichtigkeit (§ 6 Abs. 1 Z 4 DSG 2000) besonderes Augenmerk zu schenken: Diese muss im Hinblick auf den Verwendungszweck einer Bonitätsauskunft gegeben sein. Liegt sie nicht (mehr) vor, ist ein überwiegendes berechtigtes Interesse an der Übermittlung dieser Daten an eine Kreditauskunftei nicht gegeben. Damit der Betroffene seine Rechte verfolgen kann, müssen die Informationspflichten nach § 24 Abs. 2 DSG 2000 in besonderem Maße erfüllt werden: Diesbezüglich muss eine Kreditauskunftei auch selbst aktiv werden.

Ein Zahlungsangebot in lediglich zwei Monatsraten, dem der Einschreiter überdies durch Leistung der ersten Rate bereits nachgekommen war, ist ein Umstand, der die Aussagekraft der ursprünglich offenen Forderung für Bonitätszwecke als nicht gegeben erscheinen lässt.

Werden daher dem Inkassobüro keine nennenswerten Zahlungsschwierigkeiten bekannt – das ist bei einer Zahlung in lediglich zwei Monatsraten anzunehmen – ist die bloße Übergabe ins Inkasso im Hinblick auf die dargelegte beschränkte Aussagekraft ein Datum, für dessen Weitergabe an eine Kreditauskunftei keinesfalls ein überwiegendes berechtigtes Interesse angenommen werden kann. Auf Mahnungen durch den Gläubiger kommt es dabei nicht an. Die Datenweitergabe an die Auskunftei war somit unzulässig und hat den Einschreiter in seinem Recht auf Geheimhaltung nach § 1 Abs. 1 DSG 2000 verletzt. Die DSK empfahl daher, Datenweitergaben künftig zu unterlassen, wenn eine Forderung sogleich bezahlt werde oder eine Ratenzahlung angeboten wird, die einer sofortigen Zahlung nahe kommt.

Die DSK erachtete es darüber hinaus aber auch als Rechtsverletzung, dass das Inkassobüro die Forderung in voller Höhe als offen weitergegeben hatte, obwohl bereits eine erhebliche Teilzahlung geleistet worden war. Sie empfahl daher, unbezahlte Forderungen nur in jener Höhe an eine Kreditauskunftei weiterzugeben, die im Zeitpunkt der Weitergabe tatsächlich offen war.

Festgestellt wurden weiters fehlende Informationen über die Voraussetzungen einer Datenübermittlung an Auskunfteien, die im Hinblick auf die Eingriffstiefe nach § 24 Abs. 2 DSG 2000 erforderlich gewesen wären. Es war insbesondere auch unzulässig, dem Einschreiter gegenüber zu behaupten, eine Forderung sei „dem Inkassobüro abgetreten worden“, weil dies durch § 118 Abs. 2 GewO ausdrücklich verboten ist.

6.2.3. Verwendung der Sozialversicherungsnummer für Zwecke der Anmeldung für Lehrerfortbildungsveranstaltungen an Pädagogischen Instituten (K210.523, K211.623, K121.153)

An die DSK wandten sich (Bundes- und Landes-) Lehrer, die es als unzulässig ansahen, dass sie für Zwecke der elektronischen Anmeldung zu Fortbildungsveranstaltungen der Pädagogischen Institute (PIs) ihre Sozialversicherungsnummer angeben mussten. Die DSK erachtete die Eingaben (bzw. auch eine Beschwerde nach § 31 Abs. 2 DSG 2000) allesamt als berechtigt. Auch wenn die jeweiligen Landesschulräte, denen die PIs mangels selbständiger Organqualität zuzurechnen sind, bereits über die Sozialversicherungsnummer verfügen, dürfen sie diese nur für den durch § 31 Abs. 4 ASVG bzw. § 159b B-KUVG gesetzlich vorgegebenen Zweck (Verwaltung personenbezogener Daten für Zwecke der Sozialversicherung bzw. des Arbeitsmarktservice) verwenden. Eine (als Übermittlung zu qualifizierende) Weiterverwendung bzw. neuerliche Ermittlung für den Zweck der Lehrerfortbildung geht darüber hinaus und ist daher unzulässig. Entsprechende Empfehlungen an die Landesschulräte wurden ausgesprochen, im Beschwerdefall wurde eine Verletzung im Recht auf Geheimhaltung festgestellt.

6.2.4. Gesetzwidrige Zustimmungserklärungen in Antragsformularen für Versicherungen (K211.634)

Der Einschreiter befürchtete eine Verletzung im Recht auf Geheimhaltung durch Erklärungen, die in einem Antragsformular für den Abschluss einer Reiseversicherung verlangt wurden. Die DSK teilte diese Bedenken teilweise:

Eine allgemein gehaltene Zustimmungserklärung zur Datenermittlung bei Ärzten, Krankenanstalten, sonstigen Einrichtungen der Krankenversorgung oder Gesundheitsvorsorge sowie von Sozialversicherungsträgern war unter einer irreführenden Überschrift mit Informationen und anderen Willenserklärungen vermischt. Die Erklärungen widersprachen darüber hinaus der datenschutzrechtlichen Spezialbestimmung in § 11a Abs. 2 VersVG. Im Rahmen von Versicherungsverträgen sind Zustimmungen nur wirksam, wenn sie den in Z 3 oder Z 4 dieser Regelung bestimmten Inhalt aufweisen. Die allgemein gehaltene Formulierung der Zustimmungserklärung im beschwerdegegenständlichen Formular genügte dem nicht. Insbesondere erlaubt die Z 3 des § 11a Abs. 2 VersVG nur eine Zustimmung zur Datenermittlung im Einzelfall (der damit bei Abgabe der Erklärung bekannt sein muss) und die Z 4 nur eine Zustimmung zur Beurteilung von Ansprüchen aus einem konkreten Versicherungsfall. Außerdem fand sich in dem Formular ein Feld für ein „ärztliches Kurzattest“, bei dem nicht klar war, von wem dieses einzuholen war. Die DSK empfahl eine Neugestaltung des Formulars unter Berücksichtigung dieser Bedenken. In diesem Zusammenhang gibt es noch ein weiteres wesentliches Problem: In den Krankenanstaltengesetzen der meisten Bundesländer (vgl. zB § 35 Abs. 1 Sbg KAG 2000) finden sich Regelungen, welche eine über § 11a VersVG hinausgehende Weitergabe von Daten aus Krankengeschichten im Zusammenhang mit der Abrechnung mit privaten Krankenversicherungen vorsehen. Über Anregung des (damaligen) Bundesministeriums für Gesundheit und Frauen hat die DSK diesen Widerspruch zwischen Bundes- und Landesrecht aufgegriffen, die zuständigen Bundesministerien, die Länder (im Wege der Verbindungsstelle) sowie den Datenschutzrat darauf aufmerksam gemacht und diese um Herbeiführung einer rechtseinheitlichen Regelung ersucht. Die zwischenzeitlich stattgefundenen Gespräche zwischen Bundes- und Ländervertretern lassen auf eine Lösung hoffen.

6.2.5. Verständigung des Arbeitgebers von einer vorläufigen Führerscheinabnahme (K210.544)

Dem Einschreiter, einem Berufskraftfahrer (Lkw), wurde bei einer nächtlichen Fahrzeugkontrolle (Fahrt mit dem privaten Pkw) nach einem Alkomattest wegen Alkohol am Steuer der Führerschein gemäß § 39 Abs 1 FSG vorläufig abgenommen. Am nächsten Tag rief ein Beamter der betreffenden Polizeidienststelle am Arbeitsplatz des Einschreiters an und gab einen „Wink", das mit dem Führerschein des Einschreiters etwas nicht in Ordnung sei. Der Dienstvorgesetzte des Einschreiters rief daraufhin bei der Polizeidienststelle an und erfuhr von der erfolgten Führerscheinabnahme (der Einschreiter selbst hatte sich an diesem Tag krank gemeldet), worauf die Entlassung des Einschreiters ausgesprochen wurde.

Die DSK erachtete diese Form der Datenübermittlung für unzulässig und gab eine entsprechende Empfehlung gegenüber dem zuständigen Landespolizeikommando ab. Verantwortlicher datenschutzrechtlicher Auftraggeber ist das Landespolizeikommando, da die entsprechenden Daten für Zwecke einer Anzeige an die zuständige Verwaltungsstraf- und Führerscheinbehörde ermittelt wurden (Datenverwendung gemäß § 35 Abs. 3 Z 2 FSG iVm § 13 Abs. 2 SPG). Da der Dienstgeber eines Berufskraftfahrers gemäß § 29 Abs. 2 Z 2 FSG ausdrücklich nur von einer vollstreckbaren, das heißt bescheidmäßig ausgesprochenen Entziehung der Lenkberechtigung zu verständigen ist, kommt im Umkehrschluss eine Verständigung von der vorläufigen Führerscheinabnahme nicht in Betracht (keine sinngemäße Anwendung der Bestimmung). Die DSK fügte ihren Ausführungen aber hinzu, dass dies kein Recht für Berufslenker bedeute, eine Führerscheinabnahme vor dem Dienstgeber geheim zu halten, da (neben führscheinrechtlichen Verpflichtungen) insbesondere arbeitsrechtliche Pflichten anderes besagen.

6.2.6. Verwendung der Indexkartei einer Polizeiinspektion für Zwecke einer führerscheinrechtlichen Verlässlichkeitsprüfung (K210.513)

Die als Ergebnis dieses Verfahrens ausgesprochene Empfehlung der DSK behandelte die Frage, ob Dateien für Zwecke der Aktenverwaltung und Verfahrensdokumentation für Zwecke führerscheinrechtlicher Verlässlichkeitsprüfungen verwendet werden dürfen. Die DSK wertete eine solche Verwendung als unzulässig und empfahl, Überprüfungen in dieser Form in Zukunft nicht mehr durchzuführen. Es handelte sich um Daten einer Datei für die in § 13 Abs. 2 SPG festgelegten Zwecke (Aktenverwaltung und Verfahrensdokumentation). Die Durchsuchung eines Kanzleiindex nur nach dem Namen eines Betroffenen ist in § 13 Abs. 2 SPG ausdrücklich untersagt. Dies ist dahin zu verstehen, dass der Gesetzgeber eine Durchsuchung, die allein anhand von Identifikationsmerkmalen des Betroffenen erfolgt, nicht zulassen wollte (vgl. dazu auch EB zur RV 643 NR 22. GP, 9). Schon auf Grund dieses Verbots konnte die Vorgangsweise, die „Zuverlässigkeit" eines Betroffenen in der Weise zu überprüfen, dass die für den Wohnort des Betroffenen zuständige Dienststelle der Sicherheitsexekutive – wenn auch meist nur implizit – ersucht wird, einen Blick in ihre Indexkartei zu machen und über „einschlägige Vormerkungen" zu berichten, nicht als rechtskonform angesehen werden.

Für die Feststellung erwiesener Tatsachen, die gemäß § 7 Abs. 1 FSG die führerscheinrechtliche Zuverlässigkeit eines Menschen in Frage stellen, dürfen aber Daten aus anderen „Evidenzen" herangezogen werden (siehe z.B. das Vormerksystem für bestimmte straßenpolizeiliche und kraftfahrrechtliche Übertretungen gemäß §§ 16ff und 30a FSG idF BGBl. I Nr. 152/2005, das Strafregister nach § 9 Abs. 1 Z 1 des Strafregistergesetzes 1968, BGBl Nr. 277 idF BGBl I Nr. 151/2004, oder diverse Verwaltungsstrafevidenzen).

6.2.7. Datenabfrage von Sozialversicherungsdaten eines Unternehmers durch einen Vertreter des Arbeitsnehmers, der ihm von der Kammer für Arbeiter und Angestellte beigestellt wurde (K210.485)

Die Zulässigkeit einer derartigen Datenabfrage wurde von der DSK im Berichtszeitraum erneut (vgl. schon den Bescheid vom 4. Juni 2002, GZ: K120.673/003-DSK/2002) überprüft. Die Daten wurden als Beweismittel vor Gericht in einem arbeitsrechtlichen Prozess verwendet, in dem ein Vertreter der Arbeiterkammer für den klagenden Arbeitnehmer einschritt. In der von der DSK ausgesprochenen Empfehlung wurde diese Vorgehenswei-

se als unzulässig gewertet, da es sich um keine rechtmäßig ermittelten Daten handelt.

Die Arbeiterkammer hatte u.a. zu ihrer Rechtfertigung geltend gemacht, die Gewährung von Rechtsschutz für Kammermitglieder gehöre zu den gesetzlichen Aufgaben der Kammer, das Gericht gehe von einer Verfügbarkeit solcher Daten für die Arbeiterkammer aus und könnte deren Nichtvorlage gemäß durch § 178 Abs. 2 ZPO als Verstoß gegen die so genannte „allgemeine Prozessförderungspflicht" werten. Die DSK hielt dies nicht für überzeugend und betonte, dass Kammermitglieder vor dem Arbeitsgericht nicht durch die Arbeiterkammer, sondern durch eine von der Kammer damit beauftragte Person (Kammerangestellten oder –funktionär) vertreten werden. Die Kammer für Arbeiter und Angestellte wird dabei nicht im eigenen Namen und Interesse tätig, sondern für ihr Mitglied und dessen Zwecke. Für solche Zwecke kann sich die Kammer daher nicht auf die Ermächtigung gemäß § 93 Abs. 1 AKG stützen.

6.2.8. Pensionistenausweise auf Kontoauszügen (K211.680)

Eine Pensionistin hatte die DSK angerufen, weil auf ihren Bankauszügen bei der Buchung ihrer Pension zahlreiche personenbezogene Daten angeführt waren, die sie für die Auszahlung der Pension für nicht erforderlich hielt. Sie hat als Beweis einen Bankauszug übersendet, auf dem neben den Daten zur Pension selbst auch die Sätze „Befreit von der Rezeptgebühr" und „Gilt als Pensionistenausweis" angeführt waren. Die Sozialversicherungsanstalt, die die Pension ausbezahlte, hat erklärt, dass sie gesetzlich verpflichtet sei, Lohnzettel für Pensionisten auszustellen.

Es steht außer Zweifel, dass Sozialversicherungsanstalten gemäß § 47 Abs. 3 und § 78 Abs. 5 Einkommensteuergesetz 1988 verpflichtet sind, Lohnzettel für Pensionisten auszustellen. Dennoch wurde der betreffenden Sozialversicherungsanstalt in einer Empfehlung nahegelegt, innerhalb von sechs Monaten die Praxis der Übermittlung von Daten der Lohnzettel für Pensionisten so zu ändern, dass keine Angaben mehr an die Banken übermittelt werden, die über die Angaben zur Pensionsauszahlung hinausgehen. Dies mit der Begründung, dass die Angaben „Befreit von der Rezeptgebühr" und „Gilt als Pensionistenausweis" auf den Lohnzetteln der Pensionisten keinesfalls von den Bestimmungen des Einkommensteuergesetzes 1988 gedeckt sind. Weiters kam die DSK zu dem Schluss, dass Lohnzettel im Einzelfall eine Reihe von Informationen enthalten, an denen nach allgemeiner Lebenserfahrung ein erhebliches Geheimhaltungsinteresse des Betroffenen anzunehmen ist (siehe dazu schon die Empfehlung der DSK GZ: K211.413/006-DSK/2002 vom 3. September 2002). Es kann daher nicht erwartet werden, dass Pensionisten einen Lohnzettel mit vertraulichen Daten z.B. am Fahrkartenschalter vorzeigen. Weiters sind Lohnzettel nicht wirklich als Nachweis für die Pensionisteneigenschaft geeignet, weil die Echtheit eines Lohnzettels (auch in Form eines Bankauszuges) nicht leicht und rasch nachgeprüft werden kann. Die betreffende Sozialversicherungsanstalt hat in der Folge erklärt, dass die Praxis geändert werde und ab 1. Jänner 2008 die genannten Zusätze nicht mehr auf den Lohnzetteln der Pensionisten aufscheinen werden.

6.2.9. Speicherung von Verkehrsdaten über Internetverbindungen (K213.000)

In mehreren Fällen wurde von einer Musikverwertungsgesellschaft die IP-Adresse von Benutzern einer Filesharingplattform ermittelt. Es handelt sich dabei um ein Netzwerk, in dem Dateien aller Art heruntergeladen werden können, die von anderen Benutzern öffentlich zur Verfügung gestellt wurden. Um Dateien aus einem solchen Netzwerk zu beziehen, ist es erforderlich, auch selbst Dateien zur Verfügung zu stellen, was im konkreten Fall zu einer Urheberrechtsverletzung geführt hat. Aufgrund dieses von der Leistungsverwertungsgesellschaft (LVG als Privatanklägerin) wahrgenommenen Vergehens wurde ein strafgerichtlicher Beschluss auf Bekanntgabe der Stammdaten jenes Nutzers erwirkt, der die von der LVG ermittelte IP-Adresse zum Zeitpunkt der Urheberrechtsverletzung verwendet hat. Diese IP-Adresse war keinem einzelnen bestimmten Benutzer zugeteilt worden, sondern wurde nacheinander verschiedenen Kunden des Internetaccessanbieters zugewiesen (so genannte „dynamische IP Adresse").

Um gemäß dem Gerichtsbeschluss zu ermitteln, wem diese IP-Adresse zu diesem bestimmten Zeitpunkt zugeteilt war, musste der Internetaccessanbieter Verkehrsdaten, nämlich Protokolle über den Verbindungsaufbau in das Internet, auswerten. Als Rechtfertigung für die Speicherung hat der Interne-

taccessanbieter gegenüber der DSK angegeben, er brauche diese Daten für Zwecke der Verrechnung, obwohl die Betroffenen sogenannte „flat rate"-Verträge abgeschlossen hatten. Dies erachtete die DSK nicht als geeignete Grundlage für die Speicherung der Verkehrsdaten. Vielmehr hätte nach § 99 TKG 2003 der Internetaccessanbieter nach Abschluss des jeweiligen Internetbesuchs die Verkehrsdaten seiner Kunden löschen müssen bzw. gar nicht speichern dürfen. Die Speicherung von dynamisch vergebenen IP-Adressen für Zwecke der Überprüfung einer Fair Use Policy ist für Verrechnungszwecke nicht erforderlich und kann daher hinsichtlich der Zulässigkeit nicht auf § 99 Abs. 2 TKG 2003 gestützt werden. Daher hat die Datenschutzkommission am 29. September 2006 eine Empfehlung ausgesprochen, die u.a. Folgendes aussagt:

„§ 99 TKG 2003 verpflichtet die Betreiber öffentlicher Kommunikationsnetze, Verkehrsdaten, außer in den gesetzlich besonders geregelten Fällen, nach Abschluss der technischen und organisatorischen Abwicklung einer Verbindung im Netz zu löschen oder zu anonymisieren. IP-Adressen sind Zugangsdaten im Sinne des § 92 Abs. 3 Z 4a TKG 2003 und somit Verkehrsdaten im Sinne des TKG 2003. Nur statische IP-Adressen können gleichzeitig auch Stammdaten sein, wenn sie in einem Verzeichnis mit den Identitätsdaten des Teilnehmers verbunden sind. Die Speicherung von dynamisch vergebenen IP-Adressen für Zwecke der Überprüfung einer Fair Use Policy ist für Verrechnungszwecke nicht erforderlich und kann daher hinsichtlich der Zulässigkeit nicht auf § 99 Abs. 2 TKG 2003 gestützt werden." (Empfehlung K213.000/0005-DSK/2006)."

6.3. Gesetzlicher Handlungsbedarf

6.3.1. Zuständigkeitsfragen

6.3.1.1. Rechtsschutz gegenüber behaupteten Datenschutzverletzung durch Organe der Gesetzgebung

Im Berichtszeitraum wurden mehrfach Beschwerden eingebracht, die sich auf Sachverhalte bezogen, die der Staatsgewalt „Gesetzgebung" zuzurechnen sind.[21]

Diese waren angesichts der auf den Bereich der Verwaltung beschränkten Zuständigkeiten der DSK zurückzuweisen.

Während für Datenschutzbeschwerden im gerichtlichen Bereich, in dem die DSK mangels Zuständigkeit ebenfalls keine Schutzfunktion ausüben kann, in den letzten Jahren in §§ 83 ff. GOG idF der Nov. BGBl I 2004/ 128 ein eigenes, justizinternes Rechtsschutzverfahren geschaffen wurde, fehlt ein solches derzeit noch für die Staatsgewalt „Gesetzgebung". Diese Lücke sollte geschlossen werden.

6.3.1.2. Rechtsschutz gegenüber Sicherheitsbehörden im strafprozessualen Vorverfahren

Eine ganze Reihe von Beschwerden gegen Handlungen von Sicherheitsbehörden im sog. „kriminalpolizeilichen Bereich", haben die Frage nach der Zuständigkeit für den datenschutzrechtlichen Rechtsschutz aufgeworfen. Dass derzeit klare rechtliche Regelungen fehlen, ist allseits bekannte Tatsache. Dass jedoch auch die mit 1. Jänner 2008 in Kraft tretende neue Strafprozessordnung diesbezüglich keine völlige Klarheit schaffen wird, sei rechtzeitig angemerkt. Welche Konsequenzen daraus zu ziehen wären, muss den für Gesetzesinitiativen zuständigen Stellen überlassen bleiben.

6.3.2. Inhaltliche Fragen

6.3.2.1. Bonitätsinformation

Eine auffallende Häufung von Beschwerdefällen hat sich im Berichtszeitraum auf Fragen der zulässigen Ermittlung und weiteren Verwendung von Kredit- und Bonitätsinformationen bezogen.
Die DSK ist bei der Behandlung dieser Fälle zur Auffassung gelangt, dass in diesem Bereich, in dem nicht ordnungsgemäße Datenverwendung für die Betroffenen auch sehr wichtige wirtschaftliche Implikationen hat, gesetzlicher Handlungsbedarf besteht, soweit die anstehenden Probleme nicht durch Verhaltensregeln gemäß § 6 Abs. 4 DSG 2000 gelöst

[21] Z.B. Verwendung personenbezogener Daten in parlamentarischen Anfragen oder Veröffentlichung von Daten über namentlich angeführte Bürger auf der Homepage des Parlaments

werden können: Es müssten die §§ 152 der GewO 1994 betr. „Auskunfteien über Kreditverhältnisse“ und 118 über „Inkassoinstitute“ – ähnlich wie dies bei § 151 GewO hinsichtlich der Adressverlage und Direktmarketingunternehmen geschehen ist – mit genaueren Regelungen über die Zulässigkeit der Ermittlung von Bonitätsdaten, insbesondere über die zulässigen Quellen, über die Pflichten der Auftraggeber zur Qualitätssicherung bei gespeicherten Bonitätsdaten, über die zulässige Speicherdauer und über die effiziente Durchsetzung der Betroffenenrechte, insbesondere Löschungsansprüche, angereichert werden. Der gegenwärtige Zustand ist jedenfalls von größter Rechtsunsicherheit geprägt, was zu den oben erwähnten zahlreichen Beschwerden an die DSK über die Datenverwendung in diesem Bereich geführt hat. Die DSK ist gerne bereit, ihr aus der Behandlung der Beschwerden erworbenes, spezielles Erfahrungswissen den für die Genehmigung von Verhaltensregeln bzw. für die Legistik zuständigen Ressorts zur Verfügung zu stellen.

6.3.2.2. Videoüberwachung

Ein ähnlich dringendes Bedürfnis nach näherer gesetzlicher Regelung besteht nach den Erfahrungen der DSK mit den Meldungen an das Datenverarbeitungsregister hinsichtlich der Zulässigkeit der Durchführung von Videoüberwachung für nichtbehördliche („private“) Zwecke. Während für die Vornahme von Videoüberwachung für behördliche Zwecke aufgrund des Gesetzesvorbehaltes des § 1 Abs. 2 DSG 2000 klar ist, dass diese jeweils nur bei Vorliegen eines speziellen Gesetzes zulässig ist, ist dies in allen anderen Fällen – mangels Geltung eines strengen Gesetzesvorbehalts – weit weniger eindeutig. Im Spannungsverhältnis zwischen der Privatautonomie, die den Schutz der eigenen Sicherheit z.B. vor Einbruch oder Sachbeschädigung durch Videoüberwachung, als selbstverständlich zulässig postuliert, und den Datenschutzinteressen von gefilmten Personen muss ein Gleichgewicht geschaffen werden. Dabei ist angesichts der Allgemeinheit der zugrunde liegenden geltenden Regelungen ein so großer Interpretationsspielraum gegeben, dass die Vollziehung mangels ausdrücklicher gesetzlicher Regelungen überfordert erscheint. Die DSK hofft daher, dass das im Regierungsprogramm in Aussicht gestellte Gesetz über die Videoüberwachung bald vorliegen wird. Die Erfahrungen der DSK aus den Registrierungsverfahren sind im Anhang zu diesem Bericht näher dargestellt.

6.3.2.3. Telekom-Verkehrsdatenspeicherung („Vorratsdatenspeicherung“)

Die im Berichtszeitraum behandelten Beschwerden betrafen dieses Problem in erster Linie im Hinblick darauf, ob der Zugriff auf Verkehrsdaten, die beim Internet-Betreiber (noch) gespeichert sind, auch für Zwecke der Ahndung von Urheberrechtsverletzungen zulässig ist.

Angesichts der unmittelbar bevorstehenden Fortsetzung des Begutachtungsverfahrens über gesetzliche Bestimmungen zur Umsetzung der RL 2006/24/EG über die Vorratsspeicherung von Daten soll im gegenwärtigen Zeitpunkt nur so viel festgehalten werden: Aus datenschutzrechtlicher Sicht wird es von entscheidender Bedeutung sein, ob es gelingt, die zulässigen Zwecke klar und nicht überschießend festzuschreiben und auch die formalen Voraussetzungen der Weiterverwendung so festzulegen, dass keine wesentlichen Interpretationsdifferenzen entstehen können.

6.2.3.4. Zustimmungserklärungen zur Verwendung von Gesundheitsdaten in Versicherungsverträgen

Aus Anlass mehrerer Anbringen von Versicherungsnehmern aber auch ärztlichen Mitarbeitern von Krankenanstalten an die DSK ist hervorgekommen, dass in den einzelnen Bundesländern erhebliche rechtliche Unterschiede bei der Weitergabe von Daten über Behandlungen in Krankenanstalten an private Krankenversicherer bestehen und die Regelungen in einzelnen Landeskrankenanstaltengesetzen auch in direktem Widerspruch zu den bundesrechtlichen Regelungen des § 11a Versicherungsvertragsgesetzes stehen.

Die DSK hat die zuständigen Bundesministerien und die Länder auf diese Problematik aufmerksam gemacht. Das BM für Justiz hat es übernommen, alle Beteiligten koordinierend mit einer allfälligen Neuordnung der Gesetzeslage zu befassen.

6.2.3.5. Verwendung der Sozialversicherungsnummer zur Identifikation von Personen außerhalb des Gesundheitsbereichs

Dieses Problem ist im Berichtszeitraum hauptsächlich im Zusammenhang mit Bildungseinrichtungen

aufgetreten. Abgesehen von der durch das Bildungsdokumentationsgesetz vorgeschriebenen Verwendung der Sozialversicherungsnummer als Identifikator im Bereich der Evidenzen der Schüler und der Studierenden wird die Verwendung dieser Nummer z.B. auch für die Anmeldung zu Lehrerfortbildungsveranstaltungen gefordert.

Dies ist nicht mehr zeitgemäß: Nachdem im Rahmen des E-Governmentgesetzes, BGBl I Nr. 10/2004, Indentifikationsroutinen geschaffen wurden, die von hoher Qualität, datenschutzrechtskonform und für die Schulverwaltung allgemein verfügbar sind, sollte anstelle der Sozialversicherungsnummer von diesen Gebrauch gemacht werden. Es ist zu hoffen, dass sich die gegenwärtigen Bestrebungen zur Novellierung des Bildungsdokumentationsgesetzes diesem Ziel annähern. Für den Bereich der Lehrerfortbildung wäre eine gesonderte Lösung zu suchen.

7. Internationale Zusammenarbeit mit anderen unabhängigen Datenschutz-Kontrollstellen

7.1. Zusammenarbeit im Rahmen der Art. 29-Gruppe

Die Datenschutz-RL 95/46/EG hat in ihrem Art. 29 eine „Datenschutzgruppe“ geschaffen, die aus den Vertretern der in jedem Mitgliedstaat bestehenden Datenschutz-Kontrollstellen (iSd Art. 28 der RL) zusammengesetzt ist und als unabhängiges Organ die EU-Kommission in Datenschutzfragen berät.

Die zwischenzeitige Entwicklung bringt es mit sich, dass die Art. 29-Gruppe oft auch vom Europäischen Parlament bei besonders wichtigen Datenschutzfragen befasst wird und dass diese Befassung des Öfteren auch über den eigentlichen Geltungsbereich der RL hinausgeht: Einige der wichtigsten Datenschutzprobleme der letzten Jahre sind solche der sog. „dritten Säule“, d.h. der Zusammenarbeit der Mitgliedstaaten im Bereich Inneres und Justiz zum Zweck der Bekämpfung des Terrors und des organisierten Verbrechens. Dass es bislang nicht gelungen ist, in diesem Bereich ein generell geltendes Datenschutzregime auf europäischer Ebene einzurichten, muss als gravierender Mangel empfunden werden, der durch die Verzögerungen bei der Annahme einer EU-Verfassung, die die Säulenteilung beseitigen wollte, immer dringender spürbar wird. Ebenso wesentlich wäre das Inkrafttreten des EU-Grundrechtskatalogs, da darin ein Grundrecht auf Datenschutz ausdrücklich anerkannt werden soll.

Die Art. 29 Gruppe hat sich im Berichtszeitraum immer wieder zu den wesentlichsten Bedrohungen des Rechtes auf Datenschutz geäußert und versucht, entstandene Bedenken den Entscheidungsträgern in der Europäischen Union nahe zu bringen. Diese Bedenken betrafen sowohl innereuropäische Entwicklungen wie etwa die Annahme eines generellen „Verfügbarkeitsprinzips“ von Daten aus nationalen Datenbanken für die Zusammenarbeit der Polizei- und Justizbehörden der EU-Mitgliedstaaten, als auch Entwicklungen in den transatlantischen Beziehungen, insbes. zu den USA. Hier hat sich in den letzten beiden Jahren die Schaffung US-amerikanischer Rechtsvorschriften mit unmittelbarer Auswirkung auf EU-Bürger und -Unternehmen als besonderes Problem erwiesen, wobei die Zahl der hiefür zitierbaren Beispiele zunimmt. War es zunächst vor allem die Verpflichtung von Fluggesellschaften, Passagierdaten an die US-Einwanderungsbehörden zu übermitteln, so sind in der Zwischenzeit Verpflichtungen zur Datenübermittlung z.B. im Bereich der Kontrolle des von SWIFT abgewickelten Zahlungsverkehrs an das US-Finanzministerium oder compliance-Verpflichtungen von weltweit agierenden US Unternehmen mit US-Rechtsvorschriften (z.B. über „whistle-blowing“ oder „pre trial discovery“) hinzugekommen, die Auswirkungen auf die europäischen Tochterunternehmen in Form von Übermittlungs- oder Offenlegungsverpflichtungen haben.

Zu einer speziellen Ausprägung dieser Entwicklung, nämlich der Verpflichtung europäischer Töchter von US-Konzernen, „whistle blowing hotlines“ einzurichten, hat die Art. 29 Gruppe eigens Stellung genommen (WP 117).[22]

Im Berichtszeitraum hat sich die Art. 29 Gruppe insbesondere mit folgenden Themen auseinander gesetzt:

7.1.1. Flugpassagierdaten

7.1.1.1. PNR (Passenger name record):

Seit 2002 verlangen die US-Einwanderungsbehörden von allen Fluglinien, die in den USA landen wollen, (- aber auch von solchen, die die USA nur überfliegen -), Daten über ihre Passagiere, die zum Zweck der Reiseabwicklung gespeichert werden. Diese sogenannten „PNR (Passenger name record) Daten“ werden von den Flug-

[22] Sämtliche veröffentlichte Expertisen der Art. 29 Gruppe („opinions“) sind auf der Homepage der EU-Kommission unter http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_de.htm einsehbar.

gesellschaften nicht immer im vollen Umfang ermittelt, sodass von den 34 möglichen Datenelementen oft auch nur 12 oder 15 Elemente vorhanden sind. Bislang haben sich die USA mit den jeweils tatsächlich vorhandenen PNR-Daten zufrieden gegeben.

Aus europäischer Sicht stellt das Verlangen der US-Einwanderungsbehörden die aus Europa in die USA fliegenden Fluglinien vor das Problem, dass sie nach US-Recht Datenübermittlungen vornehmen müssen, die nach EU-Recht einer Rechtsgrundlage entbehren und daher unzulässig sind. Zur Lösung dieses Konflikts wurde im Mai 2004 zwischen den USA und der Europäischen Union ein Abkommen über die Übermittlung von Flugpassagierdaten abgeschlossen. Infolge Ungültigerklärung dieses Abkommens durch den Europäischen Gerichtshof wegen falscher (-nämlich der 1. Säule entnommener -) Rechtsgrundlage war dieses Thema mit den USA neu zu verhandeln – Ergebnis ist das eben abgeschlossene neue Abkommen[23], das freilich aus datenschutzrechtlicher Sicht viele Nachteile aufweist, wie längere Speicherdauer, nur scheinbare Reduktion der Anzahl der zu übermittelnden Daten, keine Kontrolle der Einhaltung des Abkommens unter Einbeziehung europäischer Kontrollore usw. Freilich hat der Abschluss des Abkommens immerhin zur Folge, dass ein rechtlicher Rahmen für den durch den Flugverkehr von Europa in (oder über) die USA verursachten Datenverkehr vorhanden ist.

7.1.1.2. „No fly“ und „Selectee“ Listen

Welche Gefahr von immer stärker anwachsenden Datensammlungen ausgehen kann, illustriert der Fall des in Syrien geborenen kanadischen Staatsbürgers Maher Arar besonders anschaulich. Auf einem Flug von Zürich nach Montréal wurde der Techniker für drahtlose Netzwerke im Transitbereich des John F. Kennedy Flughafens festgehalten und aufgrund einer fehlerhaften Interpretation von PNR und Geheimdienstdaten 12 Tage später nach Syrien deportiert, wo er ein Jahr lang inhaftiert wurde.

Selbst nach der Entlastung von allen Anschuldigungen durch eine kanadische Untersuchungskommission und Zuerkennung einer hohen Entschädigungsleistung befindet sich Maher Arar noch immer auf der „No-fly“ Liste der Vereinigten Staaten von Amerika:

Neben der Auswertung der Reservierungsdaten (PNR-Daten) nutzen die US-Sicherheitsbehörden zur Überwachung der Passagiere weitere von den Geheimdiensten und Sicherheitsbehörden erstellte Unterlagen (Listen). Ausgewählte Sicherheitskräfte der Fluggesellschaften erhalten täglich eine aktualisierte „No-fly“-Liste und eine „Selectee“-Liste aus den USA. Auf der „No-fly“-Liste sind Personen vermerkt, die nicht in die USA einreisen dürfen. Auf der „Selectee“-Liste befinden sich Daten von Personen, die einer eingehenden Leibesvisitation und Gepäckkontrolle unterzogen werden müssen und erst nach Rücksprache mit einem Sky-Marshal, das ist ein Repräsentant von US-Sicherheitsbehörden auf einem europäischen Flughafen, in die USA einreisen dürfen. Auf beiden geheim gehaltenen Listen sind ca. 100.000 Personen verzeichnet.

Es ist weder ein Rechtsweg vorgesehen, der eine Einsicht in diese Listen ermöglichen würde, noch besteht die Möglichkeit, die Richtigkeit eines Eintrags zu bestreiten oder die Löschung zu verlangen.

Neben den USA erhält aktuell Kanada PNR-Daten von Flugreisenden aus den Reservierungssystemen der Fluggesellschaften. Der Datensatz, der den kanadischen Behörden zur Verfügung gestellt wird, ist allerdings deutlich kleiner als im Fall der USA. Er enthält keine sensiblen Daten und die gefilterten 25 Datenarten werden von den Fluglinien an die kanadische Einwanderungsbehörde im „push-Verfahren“ übermittelt.

Australien und Indien möchten ebenfalls von den Fluglinien Reservierungsdaten erhalten.

Auch innerhalb der europäischen Union besteht der Wunsch einiger Mitgliedsstaaten, Zugriff auf die PNR-Daten der Flugreisenden nach Europa zu erhalten. Ein solches Projekt wurde kürzlich vom zuständigen EU-Kommissar offiziell erwähnt.

Weitere Überlegungen ziehen bereits andere Mobilitätsdaten wie zB. Bahnkartendaten, Schiffskartendaten, Road-Pricing-Daten und Verkehrssteuerungsdaten mit ein.

Mobilitätsdaten von Einzelpersonen werden demnächst im Wege der Vorratsdatenspeicherung von Funkzellenstandortsdaten erfasst.

Die Auswertung von verschiedenen Mobilitätsdaten kann dazu führen, dass es kaum noch Bewegungen des Menschen gibt, die nicht elektronisch erfasst werden.

[23] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0016:01:DE:HTML

7.1.2. SWIFT

Durch Medienberichte wurde Mitte 2006 plötzlich bekannt, dass sämtliche europäischen Zahlungsverkehrsdaten in den USA gespeichert werden und dort regelmäßig aufgrund von Anordnungen des US-Finanzministeriums („administrative sub-poenas“) zwecks Analyse zur Terrorbekämpfung herausgegeben werden müssen.

Dies ist das Ergebnis des Umstandes, dass derzeit grundsätzlich alle Zahlungsströme über ein elektronisches Netzwerk abgewickelt werden, das von SWIFT[24] betrieben wird, einer Kooperative der Banken nach belgischem Recht. SWIFT hatte in den 80iger Jahren aus Gründen der Datensicherheit eine Spiegeldatenbank zu der in Europa gelegenen in den USA eingerichtet, wo die Zahlungsverkehrsdaten jeweils für 124 Tage gespeichert bleiben.

Weder der Datenexport noch die allfällige Übermittlung an das US-Finanzministerium waren den europäischen Banken und den zuständigen staatlichen Stellen bekannt. Der Datenexport aus Belgien in die USA war auch keinem Genehmigungsverfahren im Sinne der Art. 25 und 26 der RL 95/46/EG unterzogen worden.

Die Art. 29 Gruppe hatte in der Folge eine eingehende Analyse der datenschutzrechtlichen Implikationen dieses Vorgangs vorgenommen und in ihrer opinion **WP 128** veröffentlicht. Darin wird davon ausgegangen, dass die Verantwortung für die rechtswidrige Datenverwendung durch Transfer in die USA die europäischen Banken ebenso trifft wie SWIFT selbst: die Banken vor allem deshalb, weil sie ihre Überwachungspflicht als Auftraggeber der Zahlungsanweisungen nicht wahrgenommen haben und SWIFT, weil es diese Datentransfers vorgenommen hat, ohne ihre Kunden und deren Kunden entsprechend zu informieren und ohne sich um das Vorliegen der rechtlichen Voraussetzungen ausreichend zu kümmern.

Unter dem Druck der öffentlichen Meinung hat sich SWIFT in der Zwischenzeit bereit gefunden, eine Änderung der Systemarchitektur seines elektronischen Zahlungsverkehrssystems in Betracht zu ziehen, was zur Folge haben sollte, dass europäische Zahlungsverkehrsdaten nur mehr, soweit dies für die Durchführung von Zahlungen an Banken in USA notwendig ist, in die USA gelangen. Die Verwirklichung eines solchen Vorhabens wird allerdings nach Aussage von SWIFT mehrere Jahre in Anspruch nehmen. Bis dahin ist noch keine zufrieden stellende rechtliche Lösung in Aussicht – der Umstand, dass sich SWIFT mit seiner US-amerikanischen Niederlassung in den sog. „safe harbor“ begeben hat, kann das Problem nicht lösen, da die safe habor Regeln angemessenen Datenschutz nur im privaten Bereich zu erzeugen vermögen, nicht aber gegenüber und zwischen staatlichen Institutionen, worin im gegenständlichen Fall der Kern des Problems zu sehen ist.

[24] **S**ociety for **W**orldwide **I**nterbank **F**inancial **T**elecommunication

7.1.3. Elektronischer Gesundheitsakt (ELGA)

In ganz Europa sind Bestrebungen im Gange, die Kosten des öffentlichen Gesundheitswesens zu senken und die Qualität medizinischer Behandlungen möglichst zu optimieren. Als ein Mittel hiezu wird vieler Orten der „elektronische Gesundheitsakt“ angepriesen, d.i. eine (möglichst) vollständige Krankengeschichte, von der Wiege bis zur Bahre, die elektronisch zugänglich und daher grundsätzlich immer und überall verfügbar ist.

Dass ein solches Unterfangen eine Menge von datenschutzrechtlichen Risiken mit sich bringt, liegt auf der Hand. Ob dem entsprechende medizinische Vorteile gegenüber stehen, kann mangels Erfahrung noch nicht endgültig beurteilt werden. Jedenfalls darf ein solches Projekt nicht verwirklicht werden, ohne zuvor einen Rechtsrahmen zu schaffen, der die Risiken für die Betroffenen durch entsprechende Vorkehrungen minimiert und der auch der Dispositionsfreiheit des einzelnen entsprechenden Freiraum lässt. Die zwangsweise Einführung des ELGA für alle Bürger könnte jedenfalls im Hinblick auf die Verhältnismäßigkeit eines solchen Grundrechtseingriffs bedenklich sein.

Auf der Grundlage eines von der DSK erstellten Entwurfs hat die Art. 29 Gruppe in ihrer Opinion **WP 131** detailliert dargestellt, welche Fragen in dem notwendigen Rechtsrahmen (gesetzlich) geregelt werden müssten und hat auch Präferenzen für gewisse Lösungsmöglichkeiten geäußert. Die betroffenen Fachkreise werden in der Opinion ersucht, der Art. 29 Gruppe ihre Meinung zu dem Papier mitzuteilen, sodass nach dieser Konsultationsphase eine endgültige Wertung gewisser Lösungsansätze erfolgen kann.

7.1.4. Binding Corporate Rules (BCRs, Verbindliche Konzern-Richtlinien)

Die Art. 29 Gruppe beschäftigt sich schon seit mehreren Jahren mit der Ausarbeitung von Methoden, die den Datenfluss innerhalb von internationalen Konzernen datenschutzrechtlich bewältigbar machen sollen. Als ein Instrument auf diesem Weg wurde die Durchführung von „gemeinsamen Genehmigungsverfahren“ für den Datenexport aus unterschiedlichen Mitgliedstaaten der EU an ausländische Konzernunternehmen geschaffen.

Da sich diese Prozedur als einigermaßen komplex erwiesen hat, wurde nunmehr ein einheitliches Antragsformular **(WP 133**) für das gemeinsame Genehmigungsverfahren geschaffen, um den Antragstellern deutlicher zu machen, welche Unterlagen und welche Informationen an wen gegeben werden müssen, um dieses Verfahren möglichst reibungslos zu gestalten.

7.1.5. Interpretation des Begriffs der „personenbezogenen Daten“

Das Arbeitsprogramm der Art. 29 Gruppe ist naturgemäß auch der ureigensten Aufgabe dieser Institution verpflichtet, nämlich der harmonisierenden Interpretation der Bestimmungen der RL 95/46/EG. Zu diesem Zweck wird jeweils ein besonders wichtiger RL-Begriff einer genaueren Analyse unterzogen. Im Hinblick auf Fragen der Anwendbarkeit datenschutzrechtlicher Kategorien auf neue technologische Phänomene wie RFID wurde der Begriff der „personenbezogenen Daten“ zur Analyse ausgewählt. **WP 136** ist das Ergebnis dieser Arbeit, die von sehr grundsätzlicher Bedeutung für die künftige Interpretation des sachlichen Geltungsbereichs von Datenschutz sein wird.

7.1.6. Kontrollverfahren

Besonderer Erwähnung verdient eine weitere Initiative der Art. 29 Gruppe auf dem Gebiet der Durchsetzung von Datenschutz: Es wurde versucht, ein gemeinsames Kontrolluntersuchungsprojekt durchzuführen, indem alle nationalen Datenschutz-Kontrollbehörden einen bestimmten Bereich – im vorliegenden Fall waren es die privaten Krankenversicherungsunternehmen – unter Einsatz vorher vereinbarter Vorgangsweisen hinsichtlich der Datenverwendungsvorgänge untersuchen sollten. Die Ergebnisse dieses Projekts liegen in einem Bericht vor. Es wurde beschlossen, diesen Weg konzertierter, EU-weiter Prüf-Aktionen weiter zu verfolgen und zu perfektionieren.

7.1.7. Internet Task Force

Eine eigene Arbeitsgruppe der Art. 29 Gruppe ist damit beauftragt, die jeweils neuesten technologischen Entwicklungen auf ihre Datenschutzrelevanz hin zu untersuchen. Sie hat ihren Namen von einer ihrer ersten Aufgaben er- und beibehalten.

Diese Arbeitsgruppe setzt sich mit Problemen wie RFID, Geolocalisation oder Ubiquitous Computing, den Aktivitäten von ICANN und WHOIS, Projekten wie In-vehicles Telematics, einschließlich e-call (automatische Herbeirufung von Hilfe bei Unfällen) oder dem Screening von E-Mail Kommunikationen zu Werbezwecken durch Anbieter kostenloser E-Mail-Dienste auseinander. Die Ergebnisse dieser Arbeit können auf der oben genannten Homepage der EU-Kommission nachgelesen werden.

7.1.8. Weiterverwendung von Daten für den Zweck „Öffentliche Sicherheit“, insbesondere Terrorbekämpfung

Die Art. 29 Gruppe hatte immer wieder Anlass, sich mit Neuerungen auf dem Gebiet der Weiterverwendung von Daten für Zwecke der „Öffentlichen Sicherheit“ auseinander zu setzen. Da die Rechtsgrundlage der Art. 29 Gruppe ein Instrument der sog. „Ersten Säule“ ist, ergeben sich gelegentlich Zuständigkeitsfragen, die vor allem dann releviert werden, wenn die Expertise der Art. 29 Gruppe nicht willkommen ist. Da im nationalen Bereich die Datenschutzgesetze regelmäßig unbeschränkt gelten (also auch für die Bereiche der Polizei und der Justiz), ist die beschränkte Geltung der RL auf der EU-Ebene jeweils ein Anlass zu einer gewissen Irritation, die nur entweder durch die Verabschiedung eines Rahmenbeschlusses über Datenschutz in der Dritten Säule oder durch Abschaffung der Säulen innerhalb der EU beseitigt werden könnte.

Es wurde jedenfalls von den nationalen Datenschutz-Kontrollstellen kein wesentlicher Anlass ausgelassen, um zu datenschutzrechtlich bedenklichen Entwicklungen in der Dritten Säule Stellung zu nehmen, sei es in Gestalt der Art. 29 Gruppe, sei es in Gestalt der „Police Working Party", die von der Konferenz der Europäischen Unabhängigen Datenschutzbehörden gegründet wurde (vgl. hiezu die näheren Ausführungen unter Pkt. 7.3.).

7.2. Zusammenarbeit im Rahmen der Gemeinsamen Kontrollinstanzen der Dritten Säule

7.2.1. Europol

Europol ist das Europäische Polizeiamt, das EU-weit operiert und schwerwiegende Formen internationaler Kriminalität bekämpfen soll. Dazu werden große Mengen an personenbezogenen Daten verarbeitet, die auf Grund der Zielsetzung von Europol von besonderer datenschutzrechtlicher Bedeutung sind. Aus diesem Grund sind im Europol-Übereinkommen, mit dem auch Europol selbst gegründet wurde, besondere Rechte der Betroffenen vorgesehen (zB. Art 19 – Auskunftsanspruch; Art 20 – Berichtigung und Löschung von Daten).

Neben den nationalen Kontrollinstanzen (Art 23) wurde eine Gemeinsame Kontrollinstanz (GKI; „Europol Joint Supervisory Body")[25] eingesetzt (Art 24), deren Aufgabe darin besteht, die Tätigkeit von Europol nach Maßgabe der Europol-Konvention daraufhin zu überprüfen, ob durch die Verwendung der bei Europol vorhandenen personenbezogenen Daten die Datenschutzrechte von Personen verletzt werden. Die GKI ist auch zuständig für die Prüfung von Anwendungs- und Auslegungsfragen im Zusammenhang mit der Tätigkeit von Europol bei der Verwendung personenbezogener Daten. Weiters führt die GKI jährlich eine Inspektion bei Europol durch.

[25] Die GKI verfügt über eine eigene Website: http://europoljsb.consilium.europa.eu/ (ihre Mitglieder haben überdies Zugriff auf eine interne Website zur Vorbereitung auf die Sitzungen). Europol selbst ist unter http://www.europol.europa.eu/ zu finden.

Die österreichischen Mitglieder der GKI werden von der DSK entsandt. Überdies stellt die DSK ein Mitglied der Europol-Inspektionsgruppe, welche im März 2006 und im März 2007 Inspektionen bei Europol durchgeführt hat. Während im Jahr 2006 der Schwerpunkt der Kontrolle bei der Funktionsfähigkeit des Europol Informations Systems (EIS) (Art 7f) und der Rechtskonformität der verarbeiteten Daten in Analytical Work Files (AWF) – Arbeitsdateien (Art 10) lag, konzentrierte sich das Team 2007 auf die Datenverarbeitung in den einzelnen Abteilungen des Serious Crime Departments. Dieser Teil von Europol ist mit der – hauptsächlich nicht personenbezogenen – Analyse bestimmter schwerer Formen von Kriminalität mit internationalen Aspekten beschäftigt. Das Inspektionsteam erstellt einen Bericht, der – nachdem Europol die Möglichkeit zur Stellungnahme eingeräumt wurde und er in der GKI formell verabschiedet wurde – auch veröffentlicht wird.

Im Herbst 2006 hielt Europol überdies zum Thema Herausforderungen für den Datenschutz im Bereich der täglichen Arbeit bei Europol eine Konferenz in Brüssel ab. Neben der Vorstellung der GKI seitens ihres Vorsitzenden und den Erfahrungen mit Inspektionen seitens des Direktors von Europol stellte Franco Frattini die zukünftigen Entwicklungen von Europol und anderer im Rahmen der 3. Säule der EU betriebenen Informationssysteme näher vor. In einem runden Tisch wurde diskutiert, ob bei Europol ausreichender Datenschutz gewährleistet ist.

Derzeitige Schwerpunkte der Sitzungsarbeit in der GKI Europol sind der neue rechtliche Rahmen von Europol (Rahmenbeschluss des Rates statt Übereinkommen), der Europol zu einer vollständig dem EU-Budget unterstellten Institution erhebt, sowie das so genannte OASIS-Projekt, das der typisierten „Vorkontrolle" von Daten vor Eingliederung in die in Art 6 genannten automatisierten Informationssammlungen (EIS, AWFs und Indexsystem) dient. Außerdem möchte die GKI in einem eigenen Awareness Program ihre Bedeutung und Arbeit einem breiten Kreis der Bevölkerung näher bringen.

Im Beschwerdeausschuss Europol, der für die Behandlung der Beschwerden von Betroffenen betreffend die Datenverwendung durch Europol zuständig ist, wurden zwischen Juli 2005 und Juni 2007 zwei Beschwerdefälle erledigt, ein weiterer Beschwerdefall ist anhängig.

7.2.2. Schengen

Die DSK ist nationale Kontrollinstanz im Sinne des Art. 114 Schengener Durchführungsübereinkommen von 1990 (SDÜ) zur Überwachung des nationalen Teils des Schengener Informationssystems (SIS). Als solche entsendet sie auch die Vertreter in die Gemeinsame Kontrollinstanz von Schengen.[26] Diese überwacht die Übereinstimmung der Verwendung der Daten im Schengener (Informations-)System mit dem Schengener Durchführungsübereinkommen. Dazu kontrolliert sie die technische Unterstützungseinheit des SIS, prüft Anwendungs- und Auslegungsfragen im Zusammenhang mit dem Funktionieren des SIS sowie Fragen im Zusammenhang mit den von den nationalen Kontrollinstanzen unabhängig vorgenommenen Kontrollen oder mit der Ausübung des Auskunftsrecht und erarbeitet harmonisierte Vorschläge im Hinblick auf gemeinsame Lösungen für bestehende Fragen.

Das Bundesministerium für Inneres (BMI) ist für die Führung des nationalen Teils des Schengener Informationssystems (das N.SIS) zuständig. Als dessen Auftraggeber trifft das BMI auch die Pflicht zur Auskunftserteilung gemäß §§ 1 und 26 DSG 2000 an Betroffene. Fälschlicherweise an die DSK gerichtete Auskunftsbegehren werden daher an das BMI weitergeleitet. Außerdem lässt sich auf der Website der DSK schon seit Jahren ein Formular (mit englischer Übersetzung) für die Auskunft aus dem N.SIS abrufen (http://www.dsk.gv.at/schengd.htm). Österreich ist bisher das einzige Schengen-Land, das eine solche Leistung anbietet.

Die EU-Erweiterung sorgte für Änderungen in der Handhabung der Daten im SIS. Daten zu bestimmten Aufenthaltsverboten (z.B. wegen illegaler Beschäftigung oder wegen Mittellosigkeit) bezüglich Bürger der neuen EU-Staaten wurden aus dem Fremdeninformationssystem gelöscht und die entsprechenden Aufenthaltsverbote auch nicht mehr vollstreckt.

Schon seit 2003 wird über eine neue rechtliche Basis für das SIS diskutiert, da das bisherige System die durch den Beitritt neuer Mitgliedstaaten zu erwartenden Datenmengen nicht mehr aufnehmen kann. So wurden für das so genannte SIS der zweiten Generation - „SIS II“ - ein Vorschlag für einen Ratsbeschluss sowie eine Verordnung des EP und des Rates eingebracht, die auch in der GKI diskutiert und von ihr kommentiert wurden. Den ursprünglichen Zeitplan, das System mit Anfang 2008 in Vollbetrieb zu nehmen, hat man bald aufgegeben und als Übergangslösung auf ein SIS I+ gesetzt, welches auf dem bisherigen System aufbaut, aber auch die Daten der 2004 beigetretenen Mitgliedsländer aufnehmen kann. Letztstand der Entwicklungen: SIS I+ wird jedenfalls bis 2008 verwendet, dann soll die Implementierung von SIS II erfolgen. Die geänderten Kommissionsvorschläge wurden dem EP übermittelt, allerdings bedürfen sowohl die Verordnung als auch der Beschluss noch ihrer Annahme. Nach derzeitiger Planung soll das SIS II 2009 in Betrieb gehen.

Dass die Durchsetzung von Rechtsschutz trotz der Bestimmung des Art. 111 SDÜ, der die Anrufung der Datenschutz-Kontrollstelle in jedem (!) Mitgliedstaat nach Wahl des Betroffenen eröffnet, gegenüber dem SIS schwierig sein kann, hat sich in einem konkreten Beschwerdefall gezeigt, in dem die DSK wegen einer Eintragung im französischen nationalen Teil des SIS (und damit auch im zentralen SIS) befasst wurde: Die der Ausschreibung zur Einreiseverweigerung zugrunde liegende Entscheidung einer französischen Behörde war durch die nächsthöhere Instanz aufgehoben worden. Dem entsprechenden Löschungsantrag an die französische Datenschutzbehörde (in Frankreich gilt indirektes Löschungsrecht) wurde nicht entsprochen. Der Betroffene wandte sich daraufhin mit einer Beschwerde an die DSK, die nach Verschweigung der französischen Behörden im Ermittlungsverfahren auf Löschung der Eintragung erkannte. Derartige Entscheidungen sind gemäß Art 111 SDÜ für alle Vertragsstaaten bindend. In dem hier geschilderten Verfahren hat sich jedoch gezeigt, wie schwierig sich die Durchsetzung dieser Bindungswirkung gestalten kann. Die französische Seite hat nunmehr auf ein laufendes Rechtsmittelverfahren gegen die aufhebende Entscheidung der französischen Behörde vor dem Höchstgericht verwiesen, weshalb eine Löschung nicht durchgeführt werden dürfe. Österreich hat in dieser Situation die GKI befasst, die ihrerseits in einer Stellungnahme einerseits zum Ausdruck gebracht hat, dass bindenden Entscheidungen einer Datenschutzbehörde – wie hier der DSK – durch die anderen Datenschutzbehörden Rechnung getragen werden müsse (Art 111 SDÜ), andererseits eine Umfrage zu Art 111 auch unter allen anderen Schengen-Mitgliedern bzw. Beobachtern durchgeführt. Eine Lösung des Falles steht nach wie vor aus.

[26] Die Gemeinsame Kontrollinstanz von Schengen hat eine eigene Website: http://www.schengen-jsa.dataprotection.org/. Die Jahresberichte der GKI Schengen sind auf der Website der Datenschutzkommission http://www.dsk.gv.at/ veröffentlicht.

7.2.3. ZIS

Auf der Basis der Verordnung (EG) 515/97 des Rates über die gegenseitige Amtshilfe zwischen Verwaltungsbehörden der Mitgliedstaaten und die Zusammenarbeit dieser Behörden mit der Kommission im Hinblick auf die ordnungsgemäße Anwendung der Zoll- und Agrarregelung vom 13. März 1997 (ABl. L 82 vom 22. März 1997, S. 1) sowie des Übereinkommens aufgrund von Artikel K.3 des Vertrages über die Europäische Union über den Einsatz der Informationstechnologie im Zollbereich vom 26. Juli 1995 (ABl. C 316 vom 27. November 1995, S. 34) wurde ein gemeinsames Zollinformationssystem (ZIS) eingerichtet. Dieses erlaubt es, sowohl in einer Datenbank für den Bereich der gemeinschaftsrechtlichen Zuständigkeiten wie auch in einer Datenbank, die den nicht harmonisierten Bereiche betrifft, Daten über Waren oder Transportmittel sowie über natürliche und juristische Personen zu speichern, für die es tatsächliche Anhaltspunkte gibt, dass sie im Zusammenhang mit Handlungen stehen, die der Zoll- oder der Agrarregelung zuwiderlaufen.

Das ZIS ist als Ausschreibungsdatei im Rahmen der Betrugsbekämpfung konstruiert und ermöglicht es jenem Mitgliedstaat, der die Daten in das System eingegeben hat, einen ZIS-Partner in einem anderen Mitgliedstaat um die Durchführung u.a. gezielter Kontrollen zu ersuchen:

Um eine adäquate datenschutzrechtliche Kontrolle zu gewährleisten, wurde durch das vorstehend zitierte Übereinkommen vom 26. Juli 1995 eine gemeinsame Aufsichtsbehörde (Gemeinsame Kontrollinstanz für das ZIS) eingerichtet, für die jedes EU-Mitgliedsland 2 Vertreter namhaft macht, die von der jeweiligen nationalen unabhängigen Datenschutzbehörde nominiert werden. Österreich hat seit der Aufnahme der Aktivität der ZIS-GKI im Jahre 2002 aktiv an deren Arbeiten teilgenommen. Sitzungen fanden bisher im Rhythmus von etwa 4 - 6 Monaten statt.

Schwerpunkt des Berichtzeitraumes war eine Kontrolle bei der nationalen ZIS-Stelle (Bundesministerium für Finanzen). Dabei hat sich herausgestellt, dass das System zwar wenig genutzt wird, aber zufrieden stellend funktioniert.

7.3. Die „Police Working Party“

Die Police Working Party (PWP) hat sich als wichtigste Untergruppe der Frühjahrskonferenzen der Europäischen Datenschutzbehörden herauskristallisiert. Sie dient hauptsächlich der Behandlung der wichtigsten datenschutzrechtlichen Fragen in der 3. Säule der EU, der polizeilichen und justiziellen Zusammenarbeit – sie fungiert damit auch als Pendant und/oder Bindeglied zur Art. 29 Datenschutzgruppe.

Im Berichtszeitraum hatte sich die PWP mit dem Konzept der Verfügbarkeit personenbezogener Daten im Bereich der Strafverfolgung sowie mit einem Rahmenbeschluss über den Datenschutz in der 3. Säule (als „Gegenstück“ zur RL 95/46/EG) auseinander zu setzen. Außerdem arbeitet man an einem Rahmen für die Inspektion von Polizeidaten. Jüngst hat sich die PWP bei der Frühjahrskonferenz der Datenschutzbehörden 2007 auf Zypern als Working Party Police and Justice (WPPJ) neu konstituiert und arbeitet derzeit eine eigene Geschäftsordnung aus.

7.4. Eurodac

Das Dubliner Übereinkommen, das am 15. Juni 1990 von allen Mitgliedstaaten unterzeichnet wurde, ermöglicht die Bestimmung des Staates, der für die Prüfung eines in einem Mitgliedstaat gestellten Asylantrags zuständig ist. Deshalb wurde im Dezember 1991 die Einführung eines gemeinschaftsweiten Systems zur Abnahme der Fingerabdrücke von Asylwerbern („Eurodac"), das die Identifizierung dieser Personen ermöglicht, beschlossen. Im März 1996 wurden Verhandlungen über ein neues Übereinkommen auf der Grundlage von Artikel VI EU-Vertrag (dritter Pfeiler) aufgenommen. Im Jahre 1998 zeigte sich dann, dass der Anwendungsbereich des Systems auf die Behandlung der Fingerabdrücke bestimmter anderer Ausländer ausgeweitet werden musste, um die Erfüllung bestimmter Verpflichtungen aus dem Dubliner Übereinkommen zu erleichtern. Zu diesem Zweck wurde ein Entwurf eines Protokolls ausgearbeitet, durch den das Übereinkommen auf diesen Personenkreis ausgedehnt werden sollte. Aufgrund des bevorstehenden Inkrafttre-

tens des Vertrags von Amsterdam, durch den sich die Rechtsgrundlage und das Verfahren für die Asylpolitik änderte, beschloss der Rat im Dezember 1998, die beiden Entwürfe zu einem Rechtsinstrument der Gemeinschaft zu vereinen.

Nach Inkrafttreten des Amsterdamer Vertrags unterbreitete die Kommission deshalb einen Vorschlag für ein Rechtsinstrument der Gemeinschaft und entschied sich für eine Verordnung, die die beiden Vorschläge für das Übereinkommen und das Protokoll aufgreift und sich auf den neuen Titel IV des EG-Vertrags und insbesondere Artikel 63 Absatz 1 Buchstabe a EGV stützt. Es wurde der Rechtsetzungsform Verordnung (statt Richtlinie) der Vorzug gegeben, weil sie es ermöglicht, genaue Regeln für die Aufbewahrung, den Vergleich und die Löschung von Fingerabdruckdaten festzulegen, die in allen Mitgliedstaaten unmittelbar anwendbar sind. Das Dubliner Übereinkommen wurde daher am 18. Februar 2003 durch die Dublin-Verordnung ersetzt, die zunächst für alle Mitgliedstaaten außer Dänemark sowie für Island und Norwegen galt, seit dem 1. April 2006 aber auch auf Dänemark Anwendung findet.

Das „Eurodac"-System ermöglicht den Mitgliedstaaten, Asylbewerber sowie Personen zu identifizieren, die beim illegalen Überschreiten einer EU-Außengrenze aufgegriffen wurden. Anhand des Vergleichs der Fingerabdrücke kann ein Mitgliedstaat feststellen, ob ein Asylwerber oder ein Ausländer, der sich illegal in seinem Hoheitsgebiet aufhält, bereits in einem anderen Mitgliedstaat Asyl beantragt hat oder ob ein Asylbewerber illegal in die EU eingereist ist. „Eurodac" besteht aus einer von der Kommission verwalteten Zentraleinheit, einer computergestützten Datenbank für Fingerabdrücke und elektronischen Einrichtungen für die Datenübertragung zwischen den Mitgliedstaaten und der zentralen Datenbank. Neben den Fingerabdrücken umfassen die von den Mitgliedstaaten übermittelten Daten u. a. den Herkunftsmitgliedstaat, Ort und Zeitpunkt der Antragstellung, das Geschlecht sowie die Kennnummer (Namen werden in diesem System nicht gespeichert, es handelt sich daher um eine Sammlung von „indirekt personenbezogenen Daten“ im Sinne des öDSG). Die Fingerabdrücke werden allen Personen über 14 Jahren abgenommen und direkt von der Zentraleinheit in die Datenbank übertragen. Die Aufbewahrungsfrist bei Asylwerbern beträgt 10 Jahre, bei Erwerb der Staatsangehörigkeit eines Mitgliedstaates besteht Löschungsverpflichtung. Daten über Ausländer, die beim illegalen Überschreiten einer Außengrenze aufgegriffen worden sind, werden in der Regel zwei Jahre ab dem Zeitpunkt der Abnahme der Fingerabdrücke aufbewahrt. Bei Ausländern, die sich illegal im Hoheitsgebiet eines Mitgliedstaats aufhalten, erlaubt „Eurodac" lediglich den Vergleich ihrer Fingerabdrücke mit den in der zentralen Datenbanken gespeicherten Fingerabdrücken, um festzustellen, ob die betreffenden Personen in einem anderen Mitgliedstaat einen Asylantrag gestellt haben. Die zwecks Vergleich übermittelten Fingerabdrücke werden von „Eurodac" nicht gespeichert.

In Bezug auf den Schutz personenbezogener Daten sind die Herkunftsmitgliedstaaten verantwortlich für die Rechtmäßigkeit der Abnahme der Fingerabdrücke sowie für die Rechtmäßigkeit der Verwendung, Übermittlung, Aufbewahrung und Löschung der Daten. Neben den nationalen Kontrollinstanzen wurde eine unabhängige gemeinsame Kontrollinstanz eingerichtet, die sich aus höchstens zwei Vertretern der nationalen Kontrollinstanzen eines jeden Mitgliedstaats zusammensetzt. Sie hat die Aufgabe, die Tätigkeit der Zentraleinheit daraufhin zu kontrollieren, ob die Rechte der betroffenen Personen gewahrt bleiben und ist zuständig für die Prüfung von Anwendungsfragen im Zusammenhang mit dem Betrieb von „Eurodac".

Im Berichtszeitraum hat die DSK eine Kontrolle des Eurodac-Systems in den nationalen Stellen Bundesasylamt und Bundeskriminalamt vorgenommen. Ergebnis war, dass das System vom ersten Tag an ohne Probleme läuft – auch die DSK hat bis dato keine Beschwerde oder Anfrage zu Eurodac erhalten. Außerdem hat der Europäische Datenschutzbeauftragte die Zentraleinheit von Eurodac einer Prüfung unterzogen.

8. Das Datenverarbeitungsregister

Das „Datenverarbeitungsregister“ (DVR) dient der Transparenz der in Österreich durchgeführten Datenverarbeitungen. Es ist ein öffentliches, jedermann zugängliches, teilweise elektronisch geführtes Register, in das alle meldepflichtigen Datenanwendungen aufgrund einer Meldung des jeweiligen Auftraggebers eingetragen werden. An der Verfügbarkeit des Registers im Internet wird gearbeitet.

Gemäß § 2 Abs. 3 DVRV 2002 besteht die Datenanwendung „Datenverarbeitungs**register**“ aus:

- den registrierten Meldungen über Auftraggeber und Datenanwendungen
- einem gesonderten Verzeichnis der Informationsverbundsysteme und
- den Registrierungsakten.

Daneben ist das „Datenverarbeitungsregister“ auch jene Organisationseinheit (Referat DVR) innerhalb des Geschäftsapparats der DSK, in der die Registrierungsverfahren durchgeführt und auch die das Registrierungsverfahren betreffenden Bescheide der Kommissionsorgane vorbereitet werden.

8.1. Allgemeine Bemerkungen

In seiner derzeitigen Form als Teil der DSK wurde das DVR gemäß § 16 Abs. 1 DSG 2000 mit Wirksamkeit vom 1. Jänner 2000 eingerichtet. Davor war es im Österreichischen Statistischen Zentralamt angesiedelt. Aus diesem Umstand ergeben sich noch heute beachtliche Probleme der technischen Registerführung, da die unterschiedliche technische Infrastruktur noch nicht zur Gänze überwunden ist.

Das vom Statistischen Zentralamt für das DVR im Jahre 1986 geschaffene EDV-Programm („Applikation HOST“) stand für Abfragen aus dem Register hinsichtlich jener Eintragungen, die bis Ende 2001 vorgenommen wurden, bis Ende 2005 zur Verfügung. Mit dem Suchkriterium „DVR-Nummer“ oder „Bezeichnung des Auftraggebers“ konnten eingeschränkte Informationen über Meldungen, aber nicht der Meldungsinhalt selbst abgefragt werden. Der Inhalt dieser bis Ende 2001 registrierten Meldungen liegt nur in Papierform vor. Derzeit befinden sich im Register für ca. 70.000 Auftraggeber Meldungen nur in Papierform - insgesamt sind ca. 80.000 Auftraggeber[27] aufrecht registriert.

Meldungen, die zwischen Jänner 2002 und Dezember 2005 im DVR eingelangt sind, wurden sodann mittels des im Bundeskanzleramt eingeführten „EiB“ („Elektronischer Akt im Bund“)-Systems verwaltet, das für die elektronische Aktenverwaltung im Bund geschaffen wurde. Die damit gewonnene Erfahrung hat gezeigt, dass dieses System für die Führung eines großen Registers nicht ideal geeignet ist. Deshalb wurde Ende 2005 für den internen Bereich der Registerführung und -Verwaltung ein neues elektronisches System entwickelt und mit Dezember 2005 in den internen Echtbetrieb genommen. Davor erfolgte im November 2005 noch die Datenübernahme aus der alten Applikation HOST der Statistik. Die Datenübernahme aus dem ELAK System „EiB“ in das neue elektronische Verwaltungssystem ist noch nicht abgeschlossen.

Für die Ermöglichung des online-Zugangs zum DVR von außen – sowohl für Bürger, die Information suchen, als auch für meldepflichtige Auftraggeber – wird derzeit an der Erstellung eines neuen Systemteiles gearbeitet, für das ein Fertigstellungstermin im Herbst 2008 geplant ist. Dann wird es möglich sein, über Internet Einsicht in die im DVR registrierten Datenanwendungen zu nehmen, aber auch elektronisch Meldungen im online-Dialogverkehr zu erstatten.

[27] Der Umfang der bei den Auftraggebern registrierten Datenanwendungen ist unterschiedlich. Insbesondere im öffentlichen Bereich sind bei einzelnen Auftraggebern mehrere hunderte Datenanwendungen registriert.

8.2. Zum Geschäftsgang des Registers

8.2.1. Statistische Aufbereitung

Mit der bereits operationalen neuen internen Applikation ist es nunmehr auch besser möglich, statistische Auswertungen vorzunehmen. Die Zahlen in folgender Tabelle stammen zum Teil aus den Protokollzahlen des EiB, Auswertungen aus dem neuen internen System und anderen Aufzeichnungen.

	Halbjahres-Durchschnitt im letzten Berichtzeitraum	**1. Juli 2005 bis Juni 2007 Gesamtzahlen**	**1. Juli 2005 bis Juni 2007 Halbjahres-Durchschnitt**
Protokollzahlen für eingehende Meldungen im ELAK	4.929 (in diesem Zeitraum wurden im ELAK zu jeder eingehenden Meldung die bereits vorhandenen Registrierungen zum selben Auftraggeber miterfasst)	6.368 (in diesem Zeitraum wurden anlässlich neuer Meldungen keine Registrierungen mehr miterfasst)	1.592
Erst- und Folgemeldungen betreffend Auftraggeber (nicht Anzahl der Datenanwendungen)	1.054	5.940	1.485
Neue DVR-Nummern	571	3.377	844
Anzahl der gemeldeten Datenanwendungen	nicht auswertbar	7.277 davon registriert: 4.424	1.819 davon registriert 1.106
Erledigungen Insgesamt	1.928	8.497	2.124
Davon Verbesserungsaufträge	400	2.271	567
Versendete Registrierungsnachweise	628	2016	504
Büro- und Berichterstatterentwürfe für Auflagenbescheide	118 (betraf weitgehend gleichlautende Auflagenbescheide betreffend. Warnliste der Banken)	80	20
Einstellungen	170	250	62
Sonstige Erledigungen (E-Mail-Beantwortungen, Auskünfte aus dem Register, Fristverlängerungen u dgl.)	571	3.800	950

8.2.2. Richtigstellungen des Registers

Um das Register auf einem möglichst aktuellen Stand halten zu können, wäre gemäß § 22 DSG 2000 eine fortgesetzte Richtigstellung des DVR erforderlich – z.B. hinsichtlich von rechtlich nicht mehr existenten Auftraggebern. In diesem Berichtszeitraum mussten die Richtigstellungen mangels freier Ressourcen allerdings weitgehend vernachlässigt werden.

8.3. Meldungen an das Register

8.3.1. Ausnahmen von der Registrierungspflicht

8.3.1.1. Standardanwendungen

Durch die Einführung der nicht meldepflichtigen Standardanwendungen durch das DSG 2000 konnte zunächst eine gewisse Reduktion des Arbeitsanfalles im Register bewirkt werden, doch muss in Rechnung gestellt werden, dass die Prüfungstätigkeit, die der Registrierung vorausgeht, angesichts zunehmender Komplexität heutiger Datenanwendungen immer anspruchsvoller und zeitaufwändiger wird. Der Verwaltungsaufwand im Register wurde jedoch trotz nicht meldepflichtiger Standardanwendungen nicht reduziert, weil Auftraggeber oftmals nicht in der Lage sind, selbst zu beurteilen, ob die von ihnen durchgeführten Datenanwendungen den Standardanwendungen entsprechen, weshalb sie mit der Klärung dieser Fragen das DVR befassen. Weiters melden Auftraggeber des privaten Bereiches oftmals auch nicht-meldepflichtige Standardanwendungen zwecks Erlangung einer DVR-Nummer – der Besitz einer DVR-Nummer wird offenbar sowohl aus der Sicht der Auftraggeber als auch aus Sicht der Betroffenen als ein nach außen dokumentiertes „Qualitätssiegel“ betrachtet, weil das Führen einer DVR-Nummer den Eindruck erweckt, dass vom Auftraggeber die Pflichten, die ihm das DSG 2000 auferlegt, auch eingehalten werden. Vielfach wenden sich Betroffene an das Register und unterstellen einem möglichen Auftraggeber einer Standardanwendung Verletzungen von Auftraggeberpflichten, wenn dieser keine DVR-Nummer führt. Es bedarf in diesen Fällen einiger Aufklärungsarbeit über die geltende Rechtslage.

Viele Auftraggeber beurteilen die nicht meldepflichtigen Standardanwendungen aber äußerst positiv, da damit eine erhebliche Verringerung des Verwaltungsaufwandes auch bei den Auftraggebern erzielt wurde.

Die mit 1. August 2004 in Kraft getretene Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem DSG 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004) beschreibt nahezu 30 Standardanwendungen, mit welchen z.B. KMUs üblicherweise das Auslangen finden, sodass für sie eine Meldepflicht gar nicht erst entsteht.

8.3.1.2. Manuelle Dateien

Solche Dateien sind von der Meldepflicht ausgenommen, soweit es sich nicht um die Verarbeitungen handelt, die der Vorabkontrolle nach § 18 Abs. 2 DSG 2000 unterliegen (z.B. sensible Daten oder strafrelevante Daten). Beispiele für solche Datenanwendungen sind etwa Kundendateien von freiberuflich tätigen medizinisch technischen Diensten oder Aktenverwaltungsindices von Polizeibehörden. Durch die Umstellung der Aktenverwaltungssysteme bei den Sicherheitsbehörden auf elektronische Systeme im Jahr 2005 wird der Anwendungsbereich des § 58 DSG 2000 allerdings neuerlich verringert.

8.3.2. Hilfsmittel zur Erleichterung der Registrierungspflicht

8.3.2.1. Musteranwendungen

Bisher wurden nur 5 Musteranwendungen geschaffen – sie sind der Anlage 2 der StMV 2004 zu entnehmen.

8.3.2.2. Ausfüllmuster

Als Serviceleistung für meldepflichtige Auftraggeber, die gleichartige Datenanwendungen vornehmen (z.B. Behörden, freiberuflich tätige Angehörige der medizinisch technischen Dienste, Rechtsanwälte,

Notare, Unternehmensberater, Vermögensberater, Versicherungsvermittler, u.a.) wurden bereits in der Vergangenheit Ausfüllmuster ausgearbeitet und diesen auf Wunsch für die Meldungen gemäß DSG 2000 zur Verfügung gestellt. Diese Vorgangsweise wird seitens der Auftraggeber sehr begrüßt und erweist sich auch für die Mitarbeiter des DVR als vorteilhaft. Durch diese Serviceleistung werden bei den Auftraggebern beträchtliche Ressourcen eingespart. Der Aufwand für das Erstellen von Ausfüllmustern ist an sich dem Aufwand für die Ausarbeitung einer „Standardanwendung" vergleichbar. Im Gegensatz zu Standardanwendungen können Ausfüllmuster jedoch jederzeit dem aktuellen Stand und der aktuellen Rechtslage angepasst werden.

Derzeit informieren auch die beruflichen Interessensvertretungen ihre Mitglieder von der Meldepflicht und bieten entsprechende Ausfüllmuster entweder auf ihrer Homepage an oder stellen sie den Mitgliedern elektronisch für die Meldung zur Verfügung.

In Zukunft sollen in Zusammenarbeit mit den beruflichen Interessensvertretungen sowie den einzelnen Ressorts und Vertretern der Länder weitere Ausfüllmuster erstellt und den Auftraggebern in der neuen Datenbank als Serviceleistung angeboten werden. Die Ausfüllmuster werden im neuen System der jeweiligen Berufsgruppe, Behörde oder einem sonstigen Auftraggeber zugeordnet. Dem Online-User werden beispielsweise nach Auswahl seiner Berufsgruppe jene Ausfüllmuster vorgeschlagen, die für die Meldung gemäß DSG 2000 für seinen Bereich zutreffen können.

8.3.3. Anmerkungen zum Registrierungsverfahren

Datenanwendungen, die inhaltlich über die in der StMV 2004 taxativ umschriebenen Standardanwendungen hinausgehen, unterliegen nach wie vor der Meldepflicht.

Sämtliche innerhalb des Berichtszeitraumes im Register eingelangten Eingaben waren zu prüfen. Die häufigsten Ursachen für einen Verbesserungsauftrag sind folgende:

- Es wird nur das Formblatt „Angaben zum Auftraggeber" vorgelegt, ohne dass gleichzeitig Datenanwendungen zum Zweck der Registrierung im Datenverarbeitungsregister gemeldet werden;
- es wird mit einem formlosen Schreiben (E-Mail oder Fax) um Zuteilung einer DVR-Nummer ersucht;
- es werden in den Formblättern „Meldung einer Datenanwendung" die Bezeichnungen der nicht meldepflichtigen Standardanwendungen eingetragen;
- die Angaben zum Inhalt der Datenanwendung fehlen entweder zur Gänze oder sind unvollständig;
- es fehlen die Angaben der entsprechenden Rechtsgrundlagen für die Übermittlungen an die angeführten Empfängerkreise;
- es fehlt der Nachweis der Rechtsgrundlage für die Verwendung von Daten;
- der Inhalt der gemeldeten Datenanwendungen ist unstimmig;
- es fehlen die „Allgemeinen Angaben zu ergriffenen Datensicherheitsmaßnahmen";
- vielfach weisen verbesserte Meldungen wieder Mängel auf, sodass ein neuerlicher Verbesserungsauftrag notwendig ist.

Um den Verwaltungsaufwand in Grenzen zu halten, wurden die Auftraggeber im Falle gemeldeter „nicht meldepflichtiger Standardanwendungen" oder bei Fehlen des Nachweises der Rechtsgrundlage für die Verwendung von Daten – dies betrifft in der Regel neu gegründete Firmen, die noch nicht im Gewerberegister eingetragen sind – auf die Möglichkeit der Zurückziehung der Eingabe hingewiesen. In den überwiegenden Fällen wurde von dieser Möglichkeit Gebrauch gemacht, sodass das Registrierungsverfahren eingestellt werden konnte und keine bescheidmäßige Ablehnung erfolgen musste.

8.4. Die Einsichtnahme in das Datenverarbeitungsregister

Jedermann kann in das Register Einsicht nehmen und Folgendes in Erfahrung bringen:

- Wem gehört eine bestimmte DVR-Nummer?

- Ist ein bestimmter Auftraggeber registriert?
- Mit welchen Datenanwendungen ist dieser Auftraggeber registriert?
- Was ist der Inhalt der einzelnen registrierten Datenanwendungen?

Hierauf werden folgende Informationen gegeben:

- Name und Anschrift des Auftraggebers sowie eines vorhandenen Vertreters/Zustellbevollmächtigten;
- die einem Auftraggeber zugeteilte DVR-Nummer – sofern diese nicht bereits bekannt ist;
- die Bezeichnung der registrierten Datenanwendungen sowie, ob diese dem öffentlichen oder privaten Bereich zugerechnet wurden und welchen Inhalt diese Datenanwendungen aufweisen;
- im Falle des Vorliegens eines Informationsverbundsystems die genaue Bezeichnung desselben, die teilnehmenden Auftraggeber, Name und Anschrift des Betreibers, den Inhalt der Datenanwendung sowie der Spruch allfälliger Auflagen.

Darüber hinausgehende Informationen, wie Einsicht in den Registrierungsakt und darin allenfalls enthaltene Genehmigungsbescheide, erhalten Personen, die ihre Eigenschaft als Betroffener glaubhaft machen, soweit nicht überwiegende schutzwürdige Geheimhaltungsinteressen des Auftraggebers oder eines Dritten vorliegen.

Ziel der Registerführung ist es, jedermann die Einsichtnahme in das DVR und die Anfertigung von Abschriften aus diesem zu ermöglichen. In Hinkunft soll schrittweise die Möglichkeit der Einsichtnahme auch über das Internet verwirklicht werden.

8.5. Datenschutzrechtlich bedeutsame Trends betreffend den Inhalt von gemeldeten Datenanwendungen:

Im Berichtszeitraum lassen sich folgende Trends hinsichtlich neuartiger Datenanwendungen erkennen:

8.5.1. Videoüberwachung

Das DVR wurde in den letzten eineinhalb Jahren immer öfter mit der Frage befasst, ob und inwieweit Videoüberwachung zulässig ist und ob sie meldepflichtig ist. Derzeit liegen etwa 300 Meldungen vor, von welchen nur ein kleiner Teil bereits registriert ist.

Mangels einschlägiger detaillierter gesetzlicher Regelungen war es notwendig, Leitlinien für die Registrierung von Videoüberwachungsmeldungen zu entwickeln, um dem DVR Anhaltspunkte dafür zu geben, wann es registrieren darf und wann ein ablehnender Bescheid für die Beschlussfassung durch das Kollegium der DSK vorzubereiten ist.

Eine zusammenfassende Darstellung dieser Leitlinien ist aus der Anlage zum vorliegenden Abschnitt zu ersehen.

8.5.2. Systeme integrierter Gesundheitsversorgung

Im medizinischen Bereich ist ein eindeutiger Trend dahin zu verzeichnen, weit verbreitete Krankheiten auf mehrfachen Ebenen zu bekämpfen: Zum einen durch intensive Verbreitung des Vorsorgegedankens einschließlich der Einrichtung eigener Einladungssysteme für besonders gefährdete Bevölkerungsgruppen, zum anderen durch Qualitätskontrolle von Behandlungsmethoden zum Zweck der Optimierung von Behandlungsstandards, wobei der fugenlosen Betreuung durch die unterschiedlichen Arten von Gesundheitsdiensten besondere Beachtung geschenkt wird.

Aus datenschutzrechtlicher Sicht sind solche Systeme insofern besonders interessant, weil hier durch unterschiedliche Anwendung von Pseudonymisierung bzw. Anonymisierung spezieller Schutz bei der Verwendung der sensiblen Gesundheitsdaten erreicht werden kann. Die DSK hat hier ein modular strukturiertes Vorgehensmodell entwickelt, das den Anwendern eine datenschutzrechtlich optimale Auslegung ihres Systems erleichtern soll.

Als zentrales Problem hat sich in diesem Zusammenhang bisher das Fehlen einer von allgemeinem Vertrauen getragenen besonderen Pseudonymisierungsstelle erwiesen, die auch das technische know-how besitzt, um datenschutzfördernde Verschlüsselungsmethoden mit möglichst geringem Aufwand für die involvierten Auftraggeber in der Praxis umzusetzen. Die Schaffung einer solchen Stelle würde von der DSK in höchstem Maße begrüßt.

8.5.3. Neue Informationsverbundsysteme

Da umfassende Informationsverbundsysteme grundsätzlich besonderes datenschutzrechtliches Gefährdungspotential besitzen, soll auf neue derartige Datenanwendungen näher eingegangen werden.

8.5.3.1. Führerscheinregister

Zweck der Datenanwendung ist die Verarbeitung und Übermittlung von Daten zur Durchführung von Verfahren und Amtshandlungen nach dem Führerscheingesetz, weiters die Administration des Sachverständigenwesens, der zu leistenden Vergütungen für die Fahrprüfung sowie die Erfassung der Fahrschulen, sachverständigen Ärzte und verkehrspsychologischen Untersuchungsstellen Die Führerscheinbehörden sind die teilnehmenden Auftraggeber.

Fahrschulen und die im Kraftfahrbeirat vertretenen Vereine von Kraftfahrzeugbesitzern haben ein Leserecht für Führerscheindaten und ein Schreibrecht im Zusammenhang mit der Mehrphasenausbildung. Fahrschulen haben weiters ein Leserecht für Führerscheindaten und das Schreibrecht für Antragsdaten und Nachweise. Dies betrifft näherhin die Erfassung der Daten

- von Antragstellern auf Erteilung oder Ausdehnung einer Lenkerberechtigung;
- von Führerscheinbesitzern, die Perfektionsfahrten gem. §§ 4b und 4c FSG absolvierten sowie
- von Inhabern von Mopedausweisen

zur Speicherung und Verwendung dieser Daten im Informationsverbundsystem Führerscheinregister.

Übermittlungen von Daten des Führerscheinregisters sind vorgesehen an die Exekutive, an den Unabhängigen Verwaltungssenat, das Bundesministerium für Landesverteidigung und weitere Organe des Bundes, der Länder und Gemeinden, soweit diese sie für die Wahrnehmung der ihnen gesetzlich übertragenen Aufgaben benötigen. Schließlich finden Übermittlungen auch an zuständige Behörden anderer Staaten auf Grund völkerrechtlicher oder gemeinschaftsrechtlicher Verpflichtungen statt.

8.5.3.2. Österreichisches Zentrales Vertretungsverzeichnis (ÖZVV)

Das Institut der Vorsorgevollmacht ist gesetzlich geregelt in den §§ 284f ABGB. Dabei soll es zukünftig auch nächsten Angehörigen (§ 284c ABGB) möglich sein, im Bedarfsfall eine Vertretungsbefugnis zu erhalten, während dem Betroffenen demgegenüber das Recht zukommt, dieser Vertretungsbefugnis vorab oder auch im Eintrittsfall zu widersprechen (§ 284d ABGB). Das Institut der Sachwalterschaft bleibt daneben weiterhin bestehen.

Im Hinblick auf die Vielzahl der möglichen Vertretungsformen hat der Gesetzgeber die Österreichische Notariatskammer ermächtigt, das „Österreichische Zentrale Vertretungsverzeichnis (ÖZVV)“ einzurichten, zu führen und zu überwachen.

Das ÖZVV dient folgenden Zwecken:

- Registrierung der einem Notar oder Rechtsanwalt vorgelegten Vorsorgevollmachten;
- Registrierung der einem Notar oder Rechtsanwalt vorgelegten schriftlichen Sachwalterverfügungen;
- Registrierung der einem Notar oder Rechtsanwalt vorgelegten schriftlichen Widersprüche gegen die Vertretungsbefugnis nächster Angehöriger;
- Registrierung der Vertretungsbefugnis nächster Angehöriger und des Wirksamwerdens der einem Notar vorgelegten Vorsorgevollmacht und deren Widerrufs.

Durch die Vielzahl der Ansprechpartner (Notare, Rechtsanwälte) soll den Betroffenen eine einfache Registrierung ermöglicht werden. Durch die Verarbeitung der Daten in einem Informationsverbundsystem (§ 4 Z 13 DSG) soll schließlich gewährleistet werden, dass es zu keinen widersprüchlichen Registrierungen kommt.

8.5.3.3. Patientenverfügungsregister des österreichischen Notariats

Das Patientenverfügungsregister dient der Registrierung von errichteten Patientenverfügungen im Sinne des PatVG. Dies schließt die Aufzeichnung von Patientendaten und gegebenenfalls von Angaben über den Verwahrungsort der Patientenverfügung ein.

Daneben besteht die Möglichkeit, die Patientenverfügung im Urkundenarchiv des Österreichischen Notariats zu archivieren.

8.5.3.4. Neue Informationsverbundsysteme aufgrund landesgesetzlicher Regelungen

Solche neuen Systeme werden derzeit laufend in den Bereichen Jugendwohlfahrt, Sozialhilfewesen und Behindertenhilfe geschaffen. Teilnehmende Auftraggeber sind hier in erster Linie die Bezirksverwaltungsbehörden, daneben aber auch die Ämter der Landesregierungen.

ANHANG

Videoüberwachung

FAQs und Leitlinien für das Registrierungsverfahren im DVR

1. Was ist „Videoüberwachung“?

Unter **„**Video*überwachung*“ wird die **Beobachtung, d.h. die systematische und längerdauernde visuelle und allenfalls auch akustische Kontrolle einer Örtlichkeit mit Hilfe von Videokameras** verstanden. Sie liefert jedenfalls Bilddaten, allenfalls zusätzlich auch akustische Daten.

Daneben gibt es Anwendungen der Videokamera-Technik, die keinen Kontrollzweck verfolgen, sondern nur Bilder von Örtlichkeiten zur Verfügung stellen sollen, z.B. auch in Form der Veröffentlichung im Internet. Sie sollen in der Folge mit „**WebCam“- Anwendungen** bezeichnet werden.

Videoüberwachung kommt in der Praxis entweder als bloßes „*real time monitoring* (RTM)“ vor, wobei ein Aufsichtsorgan einen Ort durch Beobachtung eines oder mehrere Bildschirme kontrolliert, oder *mit Aufzeichnung* der von der Kamera erfassten Daten. Hiezu zählen auch Systeme, die nicht dauernd Bilder aufnehmen, sondern nur in bestimmten Zeitabständen (z.B. nur alle 10 Sekunden), oder nur aufgrund besonderen Befehls (z.B. Knopfdruck des überwachenden Organs oder eines Hilfe suchenden Passanten) oder nur wenn Bewegungsabläufe vom eingesetzten System als „abweichend“ vom Normalfall erkannt werden und deshalb aufgezeichnet werden (z.B. Objekte, die sich mit einer Geschwindigkeit von mehr als 80 km/h bewegen, oder stürzende Objekte etc.).

Als Zweck des Einsatzes von Videokameras wird in den Meldungen an das DVR am häufigsten Folgendes genannt:

- Schutz des Eigentums des Auftraggebers der Videoüberwachung (z.B. Hausfassaden, Inneneinrichtung gegen Vandalismus oder Diebstahl etc.)
- Schutz der Mitarbeiter des Auftraggebers (z.B. gegen Gefahren, die von Menschen oder auch von Sachen oder Umständen ausgehen)
- Schutz von anderen Personen (als Mitarbeitern) gegen strafrechtliches Verhalten oder sonstige Gefahren

Unter „Schutz“ wird dabei sowohl Generalprävention, also Verhinderung, als auch Spezialprävention, also Verfolgung, verstanden.

Gelegentlich werden Anfragen über die Zulässigkeit des Einsatzes von Videokameras an das DVR allerdings auch hinsichtlich völlig anderer Zwecke gestellt, wie z.B.

- Werbung für einen Veranstaltungsort durch Veröffentlichung der Aufnahmen im Internet („webcam“-Anwendungen)
- „Abfangen“ von digitalen Videoaufzeichnungen auf dem Weg von der Kamera zum Speichermedium („Baby phone“)

In jedem Fall wird der Zweck, zu dem die Videokameras eingesetzt werden, wesentlich für die Beurteilung der datenschutzrechtlichen Zulässigkeit sein, da diese immer an das Verhältnis des „Zwecks der Datenverwendung“ zum „Berechtigungsumfang des Auftraggebers“, d.h. an das Vorhandensein oder Nicht-Vorhandensein eines berechtigten Zwecks anknüpft.

2. Sind mit Videokamera aufgenommene Bilder „personenbezogene Daten“?

Bilddaten sind dann personenbezogene Daten, wenn die Kameraeinstellung es grundsätzlich erlaubt, die aufgenommenen Personen (insbesondere: deren Gesichtszüge) zu erkennen. (vgl. hiezu auch Beispiel Nr. 3 im Arbeitspapier WP 136 der Art. 29 Gruppe[28] über den Begriff der „personenbezogenen Daten“).

Für das Vorliegen einer „Verarbeitung personenbezogener Daten“ kommt es nicht darauf an, ob die aufgenommen Personen tatsächlich identifiziert werden; es genügt vielmehr, dass diese grundsätzlich **identifizierbar** sind (vgl. hiezu § 4 Z 1 DSG 2000 bzw. Art. 2 (a) der Datenschutz-RL 95/46/EG). „Identifizierbar“ sind Daten auch dann, wenn nicht der Aufnehmende, sondern nur ein Dritter (z.B. eine Sicherheitsbehörde) voraussichtlich in der Lage sein wird, eine Identifikation erfolgreich vorzunehmen. (so Erwägungsgrund 26 der RL 95/46/EG).

3. Kann Videoüberwachung (außerhalb des SPG) zulässig sein?

Die DSK ist in mehreren Bescheiden davon ausgegangen, dass für die Vornahme von Videoüberwachung Auflagen erteilt werden können, woraus zu schließen ist, dass sie Videoüberwachung im Rahmen der geltenden Rechtslage nicht als grundsätzlich unzulässig ansieht.[29]

Dieser Spruchpraxis folgend hat das DVR in den letzten Monaten Meldungen von Videoüberwachung mehrfach registriert.

Hinsichtlich der rechtlichen Grundlagen kann allgemein auf § 8 Abs. 4 DSG 2000, insbesondere dessen Z 3, verwiesen werden.

4. Ist Videoüberwachung meldepflichtig?

Nur „Datenanwendungen“ müssen dem DVR gemeldet werden (vgl. §§ 16 ff DSG 2000). Eine „Datenanwendung“ liegt vor, wenn die zur Erreichung des Zwecks der Datenanwendung vorgenommenen Verarbeitungsschritte „zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen“ (§ 4 Z 7 DSG 2000). Nur die Videoüberwachung mit Daten*aufzeichnung* ist demgemäß eine „Datenanwendung“.

Digitale Bildaufzeichnung stellt jedenfalls eine „Datenanwendung“ dar, analoge Datenaufzeichnung nur dann, wenn sie als „Datei“ iSd § 4 Z 6 DSG 2000 organisiert ist (vgl. hiezu § 58 DSG 2000).

Festzuhalten ist jedoch, dass auch dann, wenn ein konkreter Einsatz von Videokameras nicht als „Datenanwendung“ zu werten ist, dieser Sachverhalt zumindest den Regelungen des Grundrechts auf Datenschutz unterliegt.

Videoüberwachung, die zum Zweck der Verhinderung und Verfolgung von strafbarem Verhalten durchgeführt wird, kann voraussichtlich nicht als Datenverwendung für „rein private oder familiäre Tätigkeiten“ gelten, da hier die Verwendung der Bilddaten für einen nicht-privaten Zweck, nämlich den der Strafverfolgung, im Vordergrund der Datenermittlung steht. Videoüberwachung für diesen Zweck wird daher – sofern sie eine Datenanwendung darstellt – derzeit als meldepflichtig angesehen. (Erleichterungen könnten hier – sobald Klarheit über die rechtlichen Rahmenbedingungen besteht – durch die Schaffung von Standardanwendungen erreicht werden).

Videoüberwachung, die hingegen für rein private oder familiäre Datenanwendung betrieben wird (wie z.B. ein „baby-phone“), ist nicht meldepflichtig. Falls sich auf solchen Aufnahmen zufällig Daten über strafrelevante Sachverhalte finden, könnten diese voraussichtlich nach § 45 Abs. 2 DSG 2000 als Beweismaterial vor Polizei und Gericht herangezogen werden.

Festgehalten werden muss jedoch, dass detaillierte Erfahrungen zur Abgrenzung der „rein privaten oder familiären Datenanwendungen“ und damit zu den insoweit bestehenden Ausnahmen von der Meldepflicht noch fehlen.

[28] Fundstelle: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

[29] http://oe1.orf.at/inforadio/78611.html?filter=0: Webbericht (mit Link zu einer Audiodatei) über eine Kurzreportage im Ö1-Morgenjournal vom 19. Juli 2007 aus Anlass der Verlautbarung der ÖBB über die Inbetriebnahme von Videoüberwachungsanlagen in bestimmten Zügen. Bemerkenswert ist, dass die Spontanumfrage des Journalisten eine massiv überwiegende Zustimmung der Betroffenen zur Überwachung ergab.

5. Wann darf eine Videoüberwachungsanlage in Betrieb genommen werden?

Wenn der Zweck einer digitalen Videoüberwachung in der **Ermittlung von Bilddaten über strafbare Handlungen** („strafrechtlich relevante Daten“) oder in der Ermittlung von sensiblen Daten besteht, handelt es sich um eine der **Vorabkontrolle** iSd § 18 Abs. 2 DSG 2000 unterliegende Datenanwendung: Der Vollbetrieb einer solchen Datenanwendung darf daher nicht schon mit der Abgabe der Meldung, sondern grundsätzlich erst nach der Registrierung aufgenommen werden. (Bei vorhandener ausreichender Rechtsgrundlage kann gemäß § 20 Abs. 3 DSG 2000 die Aufnahme der Verarbeitung allerdings bereits früher erlaubt werden.)

6. Wonach bestimmt sich die Zulässigkeit der Datenermittlung mit Hilfe von Videokameras?

Jede Ermittlung personenbezogener Daten stellt einen Eingriff in das Grundrecht auf Datenschutz dar. Eingriffe sind nur unter den Voraussetzungen des § 1 Abs. 2 DSG 2000 erlaubt.

Auch die Ermittlung von Bilddaten mit Videokameras ist daher nur unter den Voraussetzungen des § 1 Abs. 2 DSG 2000 zulässig, d.h. wenn entweder die *Zustimmung* aller Betroffenen vorliegt oder die Ermittlung im *lebenswichtigen Interesse* der Betroffenen notwendig ist oder ein *überwiegendes berechtigtes Interesse* eines anderen – insbesondere des Auftraggebers – gegeben ist.

Im letzteren Fall ist zunächst das Vorliegen eines berechtigten Interesses an dem Einsatz von Videokameras zu prüfen. Dies setzt eine Definition des Zwecks der Datenermittlung voraus. Der Vergleich des definierten Zwecks mit dem Berechtigungsumfang dessen, der die Videokamera(s) einsetzen will, ergibt die Antwort auf die Frage, ob ein „berechtigtes Interesse“ an der Datenverwendung gegeben ist.

Angesichts des Verhältnismäßigkeitsgebots (§ 1 Abs. 2 letzter Satz DSG 2000) für jeden Grundrechtseingriff ist weiters der Nachweis erforderlich, dass ein festgestelltes berechtigtes Interesse an der Datenverwendung in einer bestimmten Konstellation das (ebenfalls berechtigte) Interesse des Betroffenen an der Geheimhaltung seiner Daten überwiegt. Nur bei Vorliegen eines „überwiegenden berechtigten Interesses“ ist die Verwendung personenbezogener Daten tatsächlich zulässig.

7. Welche berechtigten Interessen können hinsichtlich der Durchführung von Videoüberwachung (im Sinne von systematischer Kontrolle eines Raumes) geltend gemacht werden?

Videoüberwachung für *behördliche* Zwecke bedarf jeweils einer besonderen gesetzlichen Grundlage (vgl. den Gesetzesvorbehalt in § 1 Abs. 2 DSG 2000 und Art. 18 B-VG). Die Zulässigkeit von Videoüberwachung für sicherheitsbehördliche Zwecke ist im Sicherheitspolizeigesetz abschließend geregelt (vgl. § 54 Abs. 6 und 7 SPG).

Die Sicherheitsbehörden selbst dürfen Videoüberwachung nur an „öffentlichen Orten“ betreiben, d.h. an Orten, die von einem nicht von vornherein bestimmten Personenkreis betreten werden können (§ 27 Abs. 2 SPG).

Für die Videoüberwachung zu nicht-behördlichen Zwecken (und daher insbesondere auch für jede Datenermittlung mit Hilfe von Videokameras durch Private) gilt nicht der strenge Gesetzesvorbehalt des § 1 Abs. 2 DSG 2000 für Grundrechtseingriffe – mangels konkreter gesetzlicher Ermächtigungen kann sich die Berechtigung zu einem Grundrechtseingriff diesfalls auch aus einer Gesamtschau der Rechtsstellung des Auftraggebers in der Rechtsordnung ergeben.

Private können ein „berechtigtes Interesse“ an Videoüberwachung (im Sinne einer systematischen Kontrolle eines Raumes) allenfalls aus dem Bestehen eines „Hausrechts (im weitesten Sinn)“ ableiten, d.h. aus dem Recht, über das Betreten eines Ortes und Sich-Aufhalten an diesem Ort zu verfügen.

Private können daher überhaupt nur dort Videoüberwachung betreiben, wo das Bestehen bzw. der Schutz eines „Hausrechts im weiteren Sinn“ denkbar ist, also nicht im „öffentlichen Raum“.

Den „Privaten“ gleichzuhalten sind Auftraggeber des öffentlichen Bereichs bei der Besorgung von Aufgaben der Privatwirtschaft.

8. Die Einteilung des Raumes aus dem Blickwinkel der Verfügungsberechtigung über den Zutritt

Die Ermächtigung der Sicherheitsbehörden zur Videoüberwachung bezieht sich auf „öffentliche Orte“ im Sinne des § 27 Abs. 2 SPG, also auf Orte, bei welchen der Zutritt nicht auf von vornherein bestimmte Personenkreise beschränkt ist. Dieser Begriff umfasst somit sowohl Örtlichkeiten ohne jede Zutrittsbeschränkung als auch solche mit Zutrittsbeschränkung, wenngleich der Zutritt nicht von der Identität oder besonderen Eigenschaften des Betroffenen abhängig sein darf (z.B. Clubmitgliedschaft), sehr wohl aber z.B. an den Besitz einer Eintrittskarte (Fußballstadium, Museum) geknüpft sein kann.

Der Begriff der „öffentlichen Orte“ ist für die Beurteilung der Zulässigkeit von Videoüberwachung zu anderen als sicherheitspolizeilichen Zwecken zu undifferenziert. In der Folge werden daher die Begriffe **„öffentlicher Raum“** und **„beschränkt öffentlicher Raum“** als Unterbegriffe der „öffentlichen Orte“ verwendet:

- „öffentlicher Raum“ ist jener Bereich, in dem sich jedermann grundsätzlich unbeschränkt aufhalten darf und eine Zutrittkontrolle rechtlich nicht – oder nur aus besonderem Anlass – zulässig ist – dies betrifft etwa Straßen, Plätze, die freie Natur etc.
- „beschränkt öffentlicher Raum“ ist jener Bereich, in dem zwar ein privatrechtliches Verfügungsrecht über die Örtlichkeit besteht, die Berechtigung des Zutritts jedoch nicht auf von vornherein bestimmte Personen (z.B. „Schüler der Schule“, „Patienten“ etc.) beschränkt ist.

Demgegenüber stehen Räumlichkeiten, zu welchen der Zutritt nur bestimmten Personen gestattet ist, z.B. den Mitarbeitern eines Unternehmens. Dieser Bereich wird im Folgenden als **„nicht-öffentlicher Raum“** bezeichnet, wobei hier als besondere Kategorie noch der „private Raum“ unterschieden werden kann, der rein privaten, insbesondere Wohnzwecken vorbehalten ist. Diese Unterscheidung scheint hinsichtlich des Ausmaßes der Verfügungsgewalt über den Zutritt sinnvoll.

9. Schema betr. das berechtigte Interesse Privater an der Vornahme von Videoüberwachung

Das Vorliegen eines „berechtigten Interesses“ Privater an einer Videoüberwachung ergibt sich aus dem Zweck, zu dem die Videoüberwachung betrieben werden soll, und dem Ausmaß der Verfügungsberechtigung über den Ort, der überwacht werden soll.

Die Matrix auf dieser Seite verdeutlicht, in welchen Konstellationen ein berechtigtes Interesse eines Privaten an einer Videoüberwachung *denkmöglicherweise* bestehen kann (ob die Videoüberwachung im Einzelfall tatsächlich zulässig ist, hängt davon ab, ob das berechtigte Interesse im konkreten Fall als „überwiegend“ zu werten ist, siehe dazu Pkt. 10).

Auch dort, wo grundsätzlich nur Behörden aufgrund besonderer gesetzlicher Ermächtigung Videoüberwachung betreiben dürfen, also im „öffentlichen Raum“, können Private als Dienstleister solcher

Ort / Zweck	öffentl. Raum	beschränkt öff. Raum	Nicht öff. Raum (nicht privat)	Privater Raum
Fremdschutz	nein	nein	nein	nein
Verantwortungsschutz	Nein (**Ausnahmen**: im Randbereich zum beschränkt öff. Raum z.B. wegen Verkehrssicherungspflichten)	ja	ja	ja
Eigenschutz	Nein (**Ausnahmen**: im Randbereich zum beschränkt öff. Raum z.B. zum Schutz vor Immissionen)	ja	ja	ja

Auftraggeber an der Videoüberwachung mitwirken – sie leiten ihre Berechtigung diesfalls aus den gesetzlichen Zuständigkeiten der Auftraggeber ab.

Unter „**Fremdschutz**“ soll in der vorstehenden Matrix der Schutz von Personen verstanden werden, zu welchen ein privater Auftraggeber einer Videoüberwachung in keiner Rechtsbeziehung steht. Der „Fremdschutz“ gegen sicherheitspolizeiliche Gefahren ist Monopol der Sicherheitsbehörden und kann von Privaten nicht als Rechtsgrundlage für ihre Videoüberwachung in Anspruch genommen werden.

Mit „**Verantwortungsschutz**“ sollen jene Fälle bezeichnet werden, in welchen der Auftraggeber den Schutz von Personen aus dem Titel der Verkehrssicherungspflicht oder aus vorvertraglichen Verpflichtungen und dergl. vorzusorgen hat.

„**Eigenschutz“** umfasst schließlich den Schutz der Person und des Eigentums des Auftraggebers, aber auch den Schutz seiner Organe (Organwalter), also seiner Mitarbeiter etc.

10. Wann liegt ein „überwiegendes berechtigtes Interesse“ an der Durchführung von Videoüberwachung vor?

Bei der Vornahme von Videoüberwachung für Zwecke der Wahrnehmung *behördlicher* Aufgaben wird diese Frage durch jene gesetzlichen Bestimmungen beantwortet, die angesichts des Gesetzesvorbehalts des § 1 Abs. 2 DSG 2000 als Grundlage eines solchen Grundrechtseingriffs vorhanden sein müssen.

Bei der Vornahme von Videoüberwachung für nichtbehördliche, also „private Zwecke“ besteht – wie bereits oben ausgeführt – kein strenger Gesetzesvorbehalt, sodass die gesamte Rechtsordnung als mögliche Grundlage für das Vorliegen überwiegender berechtigter Interessen heranzuziehen ist. Ob daher die Vornahme einer konkreten Videoüberwachung zulässig ist, hängt (- sofern nicht die Zustimmung der Betroffenen oder ihr lebenswichtiges Interesse die Videoüberwachung rechtfertigt -) davon ab, ob in der konkreten Fallkonstellation der mit der Videoüberwachung verfolgte Zweck nach objektiven Kriterien als vorrangig gegenüber dem Datenschutzinteresse der von der Überwachung Betroffenen zu werten ist.

Wenn als Zweck der Videoüberwachung der Schutz vor bestimmten Gefahren angegeben wird, muss das Vorliegen dieser Gefährdung glaubhaft gemacht werden. Eine besondere Gefährdungssituation im Hinblick auf die Begehung von strafbaren Handlungen wurde bisher etwa bei der Registrierung von Videoüberwachung in den Ausstellungsräumen von Museen angenommen; sie wird auch etwa hinsichtlich von Kassenhallen von Banken oder etwa im unmittelbaren Zugangsbereich zu Geldautomaten anzunehmen sein. Schutz gegen Unfälle bzw. Unfallfolgen kann als überwiegendes berechtigtes Interesse für Videoüberwachung z.B. im Bereich von Bahnsteigen von Eisenbahn oder U-Bahn angenommen werden.

Schwieriger ist die Beurteilung, ob ein überwiegendes berechtigtes Interesse vorliegt, in Fällen der Videoüberwachung von Verkaufsräumen, des Eingangsbereich zu Wohnhäusern oder Wohnungen, von Gebäudefassaden etc. Die Frage etwa, ob grundsätzlich von einer besonderen Gefährdung durch Wohnungseinbrüche oder Fassadenbeschädigung durch Grafitti auszugehen ist und daher die Videoüberwachung des Eingangs- oder Fassadenbereichs von Häusern immer ein „überwiegendes berechtigtes Interesse“ darstellt, muss differenziert beantwortet werden: Wesentlich ist zunächst, ob und wieweit durch die Überwachung auch öffentlicher Raum (z.B. der Gehsteig vor dem Haustor) betroffen ist; dies ist entsprechend der obigen Matrix nur im Ausnahmefall zulässig, d. h. nur im absolut unvermeidlichen sachlichen und räumlichen Ausmaß. Es wird daher z.B. einer den Eingang vom Hausinnern her überwachenden Anlage der Vorzug zu geben sein vor einer auch den Gehsteig erfassenden Vorrichtung. Es muss in jedem Fall der Verhältnismäßigkeitsgrundsatz und das „Prinzip des gelindesten (Eingriffs)Mittels“ zur Anwendung gebracht werden.

Im nicht-öffentlichen Raum sind es nicht die Datenschutzinteressen der Allgemeinheit, die durch Videoüberwachung betroffen werden, sondern die der speziell zutrittsberechtigten Personen. Wo hier das überwiegende berechtigte Interesse jeweils liegt (- ei der Datenermittlung durch Videoüberwachung oder beim Recht auf Datenschutz -) hängt vom Zweck der Videoüberwachung, von der Natur der Rechtsbeziehung zwischen Auftraggeber und Überwachten etc. ab. Die Videoüberwachung eines solchen Raumes zu Zeiten, in welchen sich dort niemand zulässigerweise aufhält (etwa während der Nachtstunden), wird regelmäßig als zulässig anzusehen sein, da hier niemand vorrangige Datenschutzinteressen geltend

machen kann, wenn er unberechtigterweise solchen Raum betreten hat und dabei gefilmt wird. (Festzuhalten ist, dass ein- und derselbe Raum seinen Charakter je nach Widmung durch den Verfügungsberechtigten ändern kann – etwa von „beschränkt öffentlich“ während der Tageszeit auf „nicht-öffentlich“ während der Nachtstunden**). Konflikte hinsichtlich gegenläufiger berechtigter Interessen können sich jeweils nur gegenüber solchen Personen ergeben, die berechtigt sind, sich im überwachten Bereich aufzuhalten.**

11. Registrierte Fälle

In den folgenden Fällen (Stand: Juni 2007) wurde in bisher durchgeführten bzw. laufenden Registrierungsverfahren das Vorliegen eines überwiegenden berechtigten Interesses an der Videoüberwachung angenommen:

- Kassensaal einer Bank (Zweck: Eigenschutz und Verantwortlichkeitsschutz)
- Öffentlich zugänglicher Teil eines Museums (Zweck Eigenschutz)
- Eingang und Verkaufsraum eines Juweliergeschäftes (Zweck Eigenschutz)
- Waffen- und Munitionshersteller (Zweck: Eigenschutz, besondere Sicherheitsanforderungen auch aufgrund entsprechender behördlicher Auflagen)
- Fahrzeuge von Unternehmen des öffentlichen Verkehrs (Zweck Eigenschutz [einschl. Schutz der Mitarbeiter] und Verantwortungsschutz [Fahrgäste])
- Bahnhöfe bzw. Stationsgebäude/anlagen an öffentlichen Verkehrslinien (Zweck: wie 5)
- Fassade von denkmalgeschützten Gebäuden**,** die an öffentlichen Platz angrenzt (Zweck: Eigenschutz: Schutz vor Vandalismus)