Datenschutzbericht 2005

1. Jänner 2002 bis 30. Juni 2005

1. Einleitung

Der vorliegende elfte Datenschutzbericht umfasst den Zeitraum vom 1. Jänner 2002 bis 30. Juni 2005. Wie noch näher zu erläuten sein wird, hat es die besonders schwierige organisatorische Situation der Kommission in den Jahren 2002 - 2004 bedauerlicherweise unmöglich gemacht, den mit Jänner 2004 fälligen Bericht zu erstatten.

Da das Ende des Berichtszeitraums mit dem Ende der Funktionsperiode der ersten nach Inkrafttreten des DSG 2000 eingesetzten Datenschutzkommission zusammenfällt, soll dieser Datenschutzbericht auch zum Anlass genommen werden, einige grundsätzliche Erwägungen zur Situation einer Datenschutz-Kontrollbehörde in Österreich anzustellen (vgl. Pkt. 3.3). Zur besseren Erkennbarkeit von Entwicklungen sind die statistischen Schaubilder auch für die gesamte Amtsperiode der Bericht erstattenden Kommission, nämlich für die Zeit vom 1. Juli 2000 bis 30. Juni 2005 ausgelegt (vgl. Pkt. 4.3.2).

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)

Sämtliche Mitglieder nehmen ihre Tätigkeit in der Datenschutzkommission nur neben ihrem Hauptberuf wahr.

2.1 Die Kommission

Die Kommission als Kollegialorgan hat die Stellung eines Tribunals iSd EMRK; ihre Mitglieder sind unabhängig, ihr Vorsitzender ist Richter.

Der Kommission als Kollegialbehörde obliegt vor allem die Beschlussfassung hinsichtlich der rechtsförmlichen und vollstreckbaren Entscheidungen der Datenschutzkommission (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 Zusammensetzung der Datenschutzkommission im Zeitraum vom 1. Juli 2000 bis 30. Juni 2005 war wie folgt:

Mitglieder:

- Dr. Gustav MAIER, Vorsitzender (SenPräs. d. OGH, richterliches Mitglied)
- Dr. Waltraut KOTSCHY, geschäftsführendes Mitglied
- Dr. Ludwig STAUDIGL
- Mag. Helmut HUTTERER
- Mag. Daniela ZIMMER
- Dr. Claudia ROSENMAYR-KLEMENZ

Ersatzmitglieder:

- Dr. Anton SPENLING, stv. Vorsitzender (HR d. OGH, richterliches Ersatzmitglied)
- Dr. Eva SOUHRADA-KIRCHMAYER, stv. geschäftsführendes Mitglied
- Dr. Klaus HEISSENBERGER (seit 5. März 2004, vorher: Dr. Christoph KLEISER)
- Dr. Michaela BLAHA
- Mag. Joachim PREISS
- Dr. Alfred DUSCHANEK

2.2 Das geschäftsführende Mitglied

Neben der Kommission als Kollegialorgan wird aufgrund der Verfassungsbestimmung des § 38 Abs. 1 DSG 2000 das von der Geschäftsordnung bestimmte geschäftsführende Mitglied (gfM) als Organ der Datenschutzkommission tätig: „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).

Nach der Geschäftsordnung ist das gfM für alle Kommissionsgeschäfte verantwortlich, soweit sie nicht der kollegialen Beschlussfassung unterliegen oder dem Vorsitzenden oder einem Berichterstatter ausdrücklich vorbehalten sind. Das gfM führt[1] den gesamten Geschäftsapparat der DSK und ist nach außen verantwortlich für die laufende Geschäftsbesorgung der Datenschutzkommission.

Zu den Aufgaben des Geschäftsführenden Mitglieds im Rahmen der Führung des Geschäftsapparates der DSK gehören insbesondere

[1] nach der Geschäftseinteilung des Bundeskanzleramtes (BKA) nur als Fachvorgesetzter des Geschäftsapparates, während Dienstvorgesetzter der Leiter der Geschäftsstelle ist

- die Vorbereitung aller Entscheidungen des Kollegiums einschließlich der Leitung der Ermittlungsverfahren

- die Führung der Ombudsman-Verfahren nach § 30 DSG 2000 (mit Ausnahme der Beschlussfassung über Empfehlungen des DSK und über Maßnahmen nach § 30 Abs. 6 DSG 2000)

- die Führung des Datenverarbeitungsregisters (mit Ausnahme der bescheidmäßigen Ablehnung der Registrierung)

- die Wahrnehmung der Aufgaben der Stammzahlenregisterbehörde (mit Ausnahme der bescheidmäßigen Ablehnung der Registrierung im Ergänzungsregister)

- die Öffentlichkeitsarbeit der DSK, soweit sie nicht dem Vorsitzenden vorbehalten ist

- die Vertretung der österreichischen Datenschutzkommission in den supra- und internationalen Datenschutz-Gremien (insbesondere in der Arbeitsgruppe nach Art. 29 der RL 95/46/EG und in den Gemeinsamen Kontrollinstanzen von Schengen, Europol, ZIS etc.).

Die Funktion des geschäftsführenden Mitglieds, die nur nebenberuflich ausgeübt wird, wurde im Berichtszeitraum von MR Mag. Dr. Waltraut KOTSCHY ausgeübt. Das geschäftsführende Mitglied ist seit 1. November 2004 hauptberuflich nicht mehr als Leiter der für Datenschutz zuständigen Abteilung für das Bundeskanzleramt tätig, sondern ausschließlich für die Datenschutzkommission, und zwar als Leiterin der Geschäftsstelle. Stellvertretendes geschäftsführendes Mitglied war im Berichtszeitraum MR Dr. Eva SOUHRADA-KIRCHMAYER, seit 1. November 2004 mit der provisorischen Leitung der für Datenschutz zuständigen Abteilung im BKA betraut.

3. Die Geschäftsstelle der Datenschutzkommission

3.1 Einführung

3.1.1 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 Datenschutzkommission eine Geschäftsstelle beigegeben, die sich entsprechend der geltenden Geschäftsordnung der DSK in

- das Büro der Datenschutzkommission
- das Datenverarbeitungsregister und
- das Stammzahlenregister

gliedert.

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

3.1.2 Exkurs: Kurzer Abriss der Organisationsgeschichte des Geschäftsapparats der Datenschutzkommission

Diese Ausführungen scheinen notwendig, um die Entwicklung der letzten 5 Jahre und die daraus unter Pkt. 3.3 abgeleiteten Folgerungen zu erklären:

Als mit 1. Jänner 1980 das (erste) österreichische DSG in Kraft trat, wurde der DSK ein sog. „Büro“ als Geschäftsapparat zur Verfügung gestellt, das als – im Status nicht genau definierte – Organisationseinheit im Verfassungsdienst des Bundeskanzleramtes angesiedelt war. Sämtliche Mitarbeiter waren ausschließlich für das Büro tätig und fachlich nur dem Büroleiter bzw. dem geschäftsführenden Mitglied und dem Vorsitzenden unterstellt. Der Leiter des Büros war gleichzeitig stv. Geschäftsführendes Mitglied der DSK.

Das Datenverarbeitungsregister war als nachgeordnete Dienststelle des Bundeskanzleramtes im Statistischen Zentralamt eingerichtet.

In den späten 80er Jahren wurde die bisherige selbständige Organisation des „Büros“ aufgegeben: Zwecks Lukrierung von Synergieeffekten – samt daraus resultierenden Planstellen-Einsparungen – wurde die für Datenschutz zuständige Abteilung im Verfassungsdienst des Bundeskanzleramtes mit dem Büro der DSK fusioniert.

Anlässlich der Umsetzung der Datenschutz-RL 95/46 durch das DSG 2000, das in den Jahren 1998/99 ausgearbeitet und im Juli 1999 beschlossen wurde, war – abgesehen von der Vergrößerung der DSK um zwei zusätzliche Mitglieder, die von der Wirtschaftskammer Österreich und der Bundesarbeitskammer der Bundes-

regierung zur Nominierung gegenüber dem Bundespräsidenten vorgeschlagen werden, und dem Umstand, dass das Datenverarbeitungsregister der DSK eingegliedert wurde - wie es die RL 95/46/EG vorschreibt - kein politischer Wille zu einer grundsätzlichen Neuordnung der DSK und ihres Geschäftsapparates vorhanden, da sich die bestehende Organisation als funktionsfähig erwiesen hatte. Da Österreich zu den allerersten Ländern gehörte, die die RL95/46/EG umsetzten, war damals auch noch nicht im Detail absehbar, was künftig als organisatorischer Standard für eine „Unabhängige Kontrollstelle“ iSd Art. 28 der RL 95/46/EG gelten werde.

Während der Funktionsperiode der Bericht erstattenden Kommission war der Geschäftsapparat der DSK so organisiert, dass im Rahmen der zuständigen Abteilung im Bundeskanzleramt/Verfassungsdienst zur besseren organisatorischen Handhabbarkeit der Geschäftsbesorgung zwei eigene Referate eingerichtet waren: das „Büro der DSK“ und das „Datenverarbeitungsregister (DVR)“. Es stellte sich jedoch bald heraus, dass das organisatorische Potential dieser Struktur im Büro der DSK aufgrund der verschlungenen Besetzung der Leitungsfunktionen und der daraus resultierenden mangelnden Konzentration auf die Aufgaben der DSK nicht wirklich ausgeschöpft werden konnte: Zusammen mit einer insgesamt nicht genügenden Personalausstattung des Geschäftsapparates hat dies dazu geführt, dass auch bei Aufwendung von großem Arbeiteinsatz die Datenschutzkommission beträchtliche Rückstände angesammelt hat, was in der Öffentlichkeit und insbesondere auch von der Volksanwaltschaft immer wieder rügend vermerkt wurde. Das geschäftsführende Mitglied der DSK hat immer wieder versucht, alle Beteiligten davon zu überzeugen, dass die Situation des Büros der DSK unhaltbar sei und dass das Büro der DSK einen Leiter brauche, der sich dieser Aufgabe voll widmen könne. Es ist jedoch aus den verschiedensten Gründen nicht gelungen, mit diesen Vorhaltungen durchzudringen. Im Gegenteil: Von September 2002 bis November 2004, also über zwei Jahre lang, war die Stelle des Leiters des Büros der DSK überhaupt verwaist.

Erst im Anschluss an die Vorlage eines Berichts der internen Revision des BKA über den Geschäftsapparat der DSK kam es im März 2004 zu einer entscheidenden Neuorientierung: Es wurde beschlossen, den Geschäftsapparat der DSK und die Funktionsträger der DSK von der für Datenschutz zuständigen Abteilung im Verfassungsdienst des Bundeskanzleramtes zu trennen, letzteres spätestens mit der

Neubestellung der Kommission am 1. Juli 2005. Diese Beschlüsse wurden bisher wie folgt umgesetzt:

Die Trennung des Geschäftsapparats der DSK von der Abteilung V/3 wurde durch Änderung der Geschäftseinteilung des BKA mit 1. Juli 2004 verfügt.

Das geschäftsführende Mitglied ist nicht mehr gleichzeitig als Leiter der für Datenschutz zuständigen Abteilung tätig.

3.2 Der Personalstand der Geschäftsstelle

3.2.1 Zur Personalsituation im Büro der DSK

Angesichts der organisatorischen Wirren, welchen das Büro der DSK im Berichtszeitraum ausgesetzt war, kann über die Entwicklung des Personalstandes nur so viel gesagt werden, dass aus dem gesamten Personalbestand der Abt. V/3 des BKA für die Bearbeitung der Beschwerdeverfahren der DSK durchgehend in etwa die Arbeitskraft von insgesamt drei Mitarbeitern zur Verfügung stand. Anlässlich der vollständigen Trennung des Geschäftsapparats der DSK von der Abteilung V/3 wurde mit 1. November 2004 eine Personalaufteilung im Ausmaß von etwa 50:50 vorgenommen. Die Funktion des Leiters der Geschäftsstelle wurde mit diesem Datum von einer 1/3 Verwendung in eine ganztägige Verwendung umgewandelt. Mit 1. November 2004 wurde weiters eine zusätzliche Planstelle für das Sitzungsmanagement der DSK geschaffen und seit 1. Mai 2005 eine Planstelle für die Betreuung der supra- und internationalen Agenden der DSK zur Verfügung gestellt, sodass nunmehr im Büro folgende Personalausstattung vorhanden ist:

1 A/a Planstelle: LeiterIn der Geschäftsstelle (führt neben der Leitung des Büros die Dienstaufsicht über die gesamte Geschäftsstelle; untersteht in fachlicher Hinsicht dem Geschäftsführenden Mitglied der DSK, in dienstaufsichtsmäßiger Hinsicht dem Leiter der Sektion Verfassungsdienst)

3 A/a Planstellen: SachbearbeiterInnen für Verfahren der DSK

1 A/a Planstelle: SachbearbeiterIn für juristische und EDV-organisatorische Angelegenheiten

1 A/a Planstelle: SachbearbeiterIn für internationale Angelegenheiten

1 B/b Planstelle: SachbearbeiterIn für Sitzungsmanagement

1 c Planstelle: Teamassistenz/Sekretariat/Kanzlei

1 d Planstelle: Sekretariat/Kanzlei

Der 1999 im Vorblatt zur Regierungsvorlage zum DSG 2000 unter „Kosten“ ausgewiesene zusätzliche Bedarf von 4 Planstellen wurde daher nunmehr endlich wenigstens im Ausmaß von 2 2/3 Planstellen erfüllt.

Hinzuzufügen ist, dass das Fehlen von speziell ausgebildetem hochwertigem Informatikerpersonal im Personalstand des Büros dadurch erfolgreich kompensiert wurde, dass für Prüfverfahren, die die technische Einschau und Beurteilung von Datenanwendungen notwendig machen, regelmäßig die Dienste von A-SIT (Zentrum für sichere Informationstechnologie - Austria) in Anspruch genommen werden. Der dadurch entstehende Sachaufwand ist gegenüber den sonst anfallenden Personalkosten deshalb gerechtfertigt, weil auf diese Weise angesichts der sachlichen Nähe von A-SIT zur angewandten wissenschaftlichen Forschung technischer Sachverstand höchster Qualität auf dem jeweils neuesten Stand für die Belange der DSK nutzbar gemacht werden kann.

Eine wichtige Aufgabe einer Datenschutz-Kontrollstelle kann mit dem vorhandenen Personal des Büros nach wie vor jedoch nicht im notwendigen Ausmaß abgedeckt werden: Das ist die Vornahme von amtswegigen Prüfverfahren, die in besonders ausgewählten Bereichen unabhängig vom Vorliegen konkreter Beschwerden durchgeführt werden sollten. Dass Österreich aus Ressourcenmangel hier nicht ausreichend tätig wird, hat sich erst voriges Jahr im Rahmen der Evaluierung von nationalen Prüfungen im Bereich des Schengen-Informationssystems wieder deutlich gezeigt. Die Einrichtung einer Organisationseinheit im Geschäftsapparat der DSK, die derartige Prüfungen nach einem jährlichen Kontrollplan durchführt, wäre erforderlich, wenn der heute in Europa übliche Standard einer Datenschutz-Kontrollstelle auch in Österreich erreicht werden soll.

3.2.2 Zur Personalsituation des Datenverarbeitungsregisters

Die Entwicklung des Personalstandes im Datenverarbeitungsregister stellt sich wie folgt dar:

1.7.2000: 15,5 Planstellen

1.1.2002: 12,25 Planstellen

1.7.2005: 10,25 Planstellen

Wie ersichtlich wurde im Datenverarbeitungsregister in der Berichtsperiode kontinuierlich Personal eingespart. Die derzeitige Personalausstattung setzt sich zusammen wie folgt:

1 Planstelle A/a LeiterIn des Datenverarbeitungsregisters

1 Planstelle A/a jur. SachbearbeiterIn

3,75 Planstellen B/b SachberarbeiterInnen

0,30 Planstellen C/c SachbearbeiterIn

2 Planstellen C/c Kanzlei

2 Planstellen d Hilfstätigkeiten

Es ist richtig, dass durch die Einführung der nicht (mehr) meldepflichtigen Standardverarbeitungen durch das DSG 2000 eine gewisse Reduktion der Anzahl der Meldungen an das Register bewirkt werden konnte (vgl. hiezu die Ausführungen unter Pkt. 6). Durch die gleichzeitige Personalreduktion besteht jedoch derzeit schon wieder eine angespannte Ressourcensituation. Es muss auch in Rechnung gestellt werden, dass die Prüfungstätigkeit, die der Registrierung vorausgeht, angesichts zunehmender Komplexität heutiger Datenanwendungen juristisch immer anspruchsvoller und zeitaufwändiger wird. Das Datenverarbeitungsregister wird ein neues elektronisches Datenbanksystem für die Bearbeitung der Meldungen erhalten, das demnächst in Betrieb gehen soll; es ist zu hoffen, dass es einen wesentlichen Beitrag zur Bewältigung des Arbeitsanfalls mit den vorhandenen Personalressourcen leisten wird.

3.2.3 Zur Personalsituation im Stammzahlenregister

Hinsichtlich der neuen Kompetenzen der DSK als Stammzahlenregisterbehörde muss ein Geschäftsapparat überhaupt erst aufgebaut werden. Der Personalbedarf ist diesbezüglich schwer abzuschätzen, da keinerlei Erfahrungswerte darüber bestehen,

mit welchem Mengengerüst beim Arbeitsanfall etwa des Ergänzungsregisters zu rechnen sein wird und inwieweit dies angesichts der umfangreichen Dienstleistungsfunktionen des BMI und des BMF tatsächlich auf die Stammzahlenregisterbehörde durchschlagen wird. Derzeit sind zwei Planstellen in Rechnung gestellt; für die Besetzung einer Planstelle wurde im Juni 2005 eine Ausschreibung vorgenommen, deren Ergebnis umgehend zur Besetzung zumindest einer Planstelle führen sollte.

3.2.4 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:

AUFSTELLUNG DER VOLLBESCHÄFTIGTEN IN DEN DATENSCHUTZBEHÖRDEN DES EWR SOWIE BULGARIEN, MONACO, RUMÄNIEN UND SCHWEIZ IM JAHRE 2004 (EXKL. DEUTSCHLAND)
(SORTIERT NACH VERHÄLTNIS DER BESCHÄFTIGTEN ZU EINWOHNERN)[2]

	LÄNDER	EINWOHNER	VOLLZEIT-BESCHÄFTIGTE	VERHÄLTNIS BESCH. : E INW.
1	MONACO	30.000	7	1 : 4.285
2	ISLAND	300.000	11	1 : 27.272
3	MALTA	400.000	10	1 : 40.000
4	ZYPERN	700.000	12	1 : 58.333
5	LUXEMBURG	450.000	5	1 : 90.000
6	ESTLAND	1.400.000	15	1 : 93.333
7	LETTLAND	2.300.000	23	1 : 100.000
8	LITAUEN	3.000.000	30	1 : 100.000
9	TSCHECHISCHE REPUBLIK	10.000.000	79	1 : 126.582
10	NORWEGEN	4.500.000	29	1 : 155.172
11	SLOWAKEI	5.370.000	33	1 : 162.727
12	UNGARN	10.000.000	54	1 : 185.185
13	DÄNEMARK	5.300.000	26	1 : 203.846
14	IRLAND	4.000.000	19	1 : 210.526
15	SCHWEDEN	9.000.000	39	1 : 230.769
16	NIEDERLANDE	16.000.000	65	1 : 246.153
17	FINNLAND	5.200.000	20	1 : 260.000

[2] Die Angaben sind einem Fragebogen entnommen, der für eine Konferenz der Datenschutzbehörden im April 2005 erstellt wurde.

18	BELGIEN	10.300.000	36	1 : 286.111
19	ENGLAND	59.500.000	205	1 : 290.243
20	POLEN	38.191.000	115	1 : 332.095
21	LIECHTENSTEIN	340.000	1	1 : 340.000
22	SCHWEIZ	7.000.000	20	1 : 350.000
23	GRIECHENLAND	10.000.000	27	1 : 370.370
24	**ÖSTERREICH**	**8.000.000**	**20**	1 : **400.000**
25	SPANIEN	43.200.000	97	1 : 445.360
26	BULGARIEN	8.000.000	15[1)]	1 : 533.333
27	RUMÄNIEN	22.000.000	37	1 : 594.594
28	ITALIEN	58.000.000	94	1 : 617.021
29	SLOWENIEN	2.000.000	3	1 : 666.666
30	PORTUGAL	10.400.000	15	1 : 693.333
31	FRANKREICH	62.000.000	83	1 : 746.987

Aus dieser Statistik wird deutlich, dass Österreich am unteren Ende der europäischen Skala rangiert, was – wie bereits dargelegt – naturgemäß dazu führt, dass nicht alle Aufgaben einer Datenschutz-Kontrollbehörde im wünschenswerten Ausmaß wahrgenommen werden können.

3.3 Zusammenfassende Stellungnahme zur Organisations- und Personalsituation

Die Personalsituation im Büro der DSK konnte verbessert werden. Ein gravierender Mangel im Verhältnis zur Summe der aufgetragenen Aufgaben besteht derzeit hauptsächlich noch im Bereich der amtswegigen Prüfverfahren. Es ist zu hoffen, dass auch das neue EDV-gestützte System der Registrierung im DVR (vgl. hiezu die Ausführungen unter 4.2 und 6.8.2) eine Verbesserung der dortigen Ressourcenlage bewirkt, damit allenfalls freie Kapazitäten für die neuen Kompetenzen der DSK als Stammzahlenregisterbehörde gefunden werden können.. Der Aufbau eines funktionsfähigen Geschäftsapparats im Bereich der Stammzahlenregisterbehörde wird zu beschleunigen sein, da mit dem roll-out der e-card jeder Österreicher eine Bürgerkarten-fähige Signaturkarte in Händen hat, was voraussichtlich zu einem sprunghaften Ansteigen der Arbeit im Bereich der Stammzahlenregisterbehörde führen wird.

Ein gewisses Problem ist die Stellung des geschäftsführenden Mitglieds, und zwar vor allem in dienstrechtlicher Hinsicht:

Zunächst zur dienstrechtlichen Stellung: Die Funktion des geschäftsführenden Mitglieds der Datenschutzkommission ist in ihrem Ausmaß und ihrer Wertigkeit nicht erkennbar festgeschrieben. Es handelt sich jedenfalls um eine Nebentätigkeit, die entsprechend ihrer Remunerierung (bei Zugrundelegung eine durchschnittlichen Bezuges der Dienstklasse VIII) als Tätigkeit im Ausmaß von etwa 2 ½ Arbeitstagen im Monat vorgesehen ist. Schon die Aufzählung der Kompetenzen in Pkt. 2.2. macht aber deutlich, dass diese unmöglich in 2 ½ Arbeitstagen pro Monat wahrgenommen werden können. Bisher wurden die zur Erfüllung dieser Funktion notwendigen Arbeitsleistungen vom jeweiligen Funktionsinhaber im Rahmen seiner haupt-beruflichen Tätigkeit erbracht, also freiwillig und unentgeltlich durch unbezahlte Überstunden. Dies sollte jedoch angesichts der Fülle der Aufgaben, die bei der Führung einer heutigen europäischen Datenschutz-Kontrollstelle anfallen, nicht als Dauerlösung angesehen werden. Hier besteht Handlungsbedarf.

Zur Ausübung der Dienstaufsicht über den Geschäftsapparat der DSK: Nachdem die Grenze zwischen „Geschäftsführung“ (obliegt dem gfM) und „Dienstaufsicht“ (obliegt dem BKA) nicht eindeutig ist und die „Führung der Geschäfte“ wohl unvermeidlicher Weise auch organisatorische und dienstaufsichtsartige Maßnahmen mit umschließt, kann die Abgrenzung Schwierigkeiten bereiten. Das bestehende Organisationsmodell ist jedoch lebbar, wenn die Dienstaufsicht des BKA unter äußerster Zurückhaltung und mit größter Sensibilität ausgeübt wird. Dies ist im Übrigen auch im Hinblick auf Art. 28 der RL 95/46/EG geboten, wonach jeder Mitgliedstaat vorzusorgen hat, dass die nationale Datenschutzkontrollstelle „ihre Tätigkeit in völliger Unabhängigkeit“ ausüben kann. Ergänzend wird – wie schon im letzten Bericht – festgestellt, dass auch der Mangel eines eigenen Budgets der Datenschutzkommission in allfälligen Reorganisationsüberlegungen als Problem-bereich Berücksichtigung finden sollte. Eine gewisse Verfügungsgewalt über Budgetmittel stellt einen nicht unwesentlichen Ausdruck jener Unabhängigkeit dar, die Art. 28 der EU Datenschutz-Richtlinie für eine Datenschutz-Kontrollstelle einfordert. Auch aus der neuen Zuständigkeit der Datenschutzkommission als Stammzahlenregisterbehörde ergäbe sich das dringende Bedürfnis einer Neubewertung der haushaltsrechtlichen Stellung der DSK.

Wie schon in der Einleitung angekündigt, soll ein Ausblick auf die wünschenswerte zukünftige Entwicklung der DSK als Datenschutz-Kontrollstelle gemäß Art. 28 der RL 95/46/EG gegeben werden: Neben der gerichtsähnlichen Funktion, die die österreichische Datenschutzkommission bisher hauptsächlich – und durchaus mit Erfolg – ausgeübt hat, müsste eine stärkere Betonung der Funktionen der DSK als umfassend tätiger Garant der Datenschutzinteressen der Bürger erfolgen. Die Datenschutzkommission müsste von der Bevölkerung als Trust-Center in Sachen „Datenschutz“ wahrgenommen werden: Dies bedeutet nicht nur vermehrte Präsenz in den tagespolitischen Datenschutzfragen, sondern vor allem auch vermehrte Kontrolltätigkeit gegenüber den aus der Sicht des Bürgers besonders relevanten Datenverarbeitungen. Gerade die Einführung eines umfassenden e-Government-Konzeptes in Österreich verschafft der Stellung der DSK als Stammzahlen-registerbehörde und damit Hüterin der elektronischen Identitäten der Bürger besondere Bedeutung. Wenn die Bevölkerung nicht den Eindruck gewinnt, dass sich eine kompetente und wachsame Stelle um die Datenschutzinteressen der Bürger gegenüber der fortschreitenden Elektronisierung des öffentlichen Lebens erfolgreich annimmt, wird der dringend notwendige Innovationsschub in der öffentlichen Verwaltung auf Akzeptanzprobleme stoßen. Diese Wachsamkeit muss dauernd, allgemein und auch unabhängig vom Vorliegen einer konkreten Beschwerde ausgeübt werden. Es wird in erster Linie an der Datenschutzkommission selbst liegen, diesem Ziel möglichst nahe zu kommen. Es wird aber auch im ureigensten Interesse der staatlichen Verwaltung liegen, jene organisatorischen Voraus-setzungen zu fördern, deren Vorliegen notwendig ist, um die geschilderten Aufgaben, die sich seit der Einrichtung des DSK im Jahre 1980 etwas gewandelt haben, erfolgreich wahrnehmen zu können.

4. Der Geschäftsgang der Datenschutzkommission

4.1 Zuständigkeiten der Datenschutzkommission nach dem DSG 2000

Für Zwecke des Berichts über den Geschäftsgang der DSK im Berichtszeitraum 1. Jänner 2002 bis 30. Juni 2005 wird folgende Einteilung der Kategorien von Geschäftsfällen getroffen:

4.1.1 Individualbeschwerdeverfahren nach § 31 DSG 2000 (K120-Verfahren)

Wegen behaupteter Verletzung im Recht auf Geheimhaltung, Richtigstellung oder Löschung durch einen Auftraggeber des öffentlichen Bereichs sowie wegen behaupteter Verletzung im Recht auf Auskunft durch Auftraggeber des öffentlichen oder des privaten Bereichs können Betroffene Beschwerde an die Datenschutzkommission mit dem Ziel einer rechtsförmlichen, durchsetzbaren Entscheidung erheben.

4.1.2 „Ombudsman“-Verfahren (K210-Verfahren und K211-Verfahren)

Seit Inkrafttreten des DSG 2000 hat die Datenschutzkommission auch die Aufgabe, gemäß § 30 DSG 2000 nicht-förmliche, Ombudsman-artige Verfahren über Eingaben von Betroffenen durchzuführen. Im privaten Bereich besteht bei behaupteten Verletzungen des Rechts auf Geheimhaltung, Richtigstellung oder Löschung nur diese Form der Rechtsverfolgung vor der Datenschutzkommission zu – eine rechtsförmliche, exekutionsfähige Entscheidung kann nur durch Anrufung der ordentlichen Gerichte erwirkt werden. Hinsichtlich von behaupteten Datenschutz-verletzungen im öffentlichen Bereich kann der Betroffene wählen, ob er ein rechtsförmliches Verfahren oder ein Ombudsman-Verfahren anstrebt. Bestimmte Auftraggeberpflichten, welchen kein subjektives Recht auf Seiten des Betroffenen gegenübersteht (z.B. die Meldepflicht an das DVR), können nur im Rahmen eines Verfahrens nach § 30 DSG 2000 vom Betroffenen wirksam eingemahnt werden.

4.1.3 Rechtsauskünfte an Bürger (K209-Verfahren)

Art. 28 der RL 95/46/EG nennt unter den Aufgaben einer Datenschutz-Kontrollstelle auch die Pflicht, die Bürger hinsichtlich ihrer Datenschutzrechte zu beraten. Diese Inanspruchnahme des Geschäftsapparats hat seit der Verbreitung des Gebrauchs von E-Mails enorm zugenommen. Angesichts der zahlenmäßigen Bedeutung dieser Tätigkeit der Datenschutzkommission und der damit einhergehenden Notwendigkeit, gegebene Auskünfte auch allenfalls wieder auffinden zu können, werden diese Fälle seit 2003 durch Vergabe von Geschäftszahlen erfasst und dokumentiert.

4.1.4 Genehmigung der Datenverwendung für wissenschaftliche oder statistische Zwecke und Genehmigung der Verwendung von Adressdaten gemäß § 46 und § 47 DSG 2000 (K202-Verfahren)

Gemäß §§ 46 und 47 DSG 2000 ist die Datenschutzkommission zur Entscheidung über die Zulässigkeit der Verwendung von personenbezogenen Daten für wissenschaftliche Forschung[3] und Statistik (§ 46 DSG 2000) sowie der Verwendung von Adressdaten zur Benachrichtigung oder Befragung des Betroffenen (§ 47 DSG 2000) zuständig.

4.1.5 Genehmigung von Fällen des internationalen Datenverkehrs (K178-Verfahren)

Soweit aus Datenanwendungen in Österreich Daten für Zwecke, die nicht in § 12 Abs. 3 DSG 2000 (in Umsetzung des Art. 26 Abs. 1 der RL 95/46/EG) angeführt sind, ins Ausland außerhalb der Europäischen Union übermittelt oder überlassen werden sollen, bedarf dies einer Genehmigung durch die Datenschutzkommission gem. § 13 DSG 2000, es sei denn, dass das Bestimmungsland aufgrund eines Beschlusses der EU-Kommission[4] oder aufgrund einer Verordnung des Bundeskanzlers als Staat mit angemessenem Datenschutz anerkannt wurde.[5]

4.1.6 Registrierungsverfahren (K505-Verfahren)

Die Ablehnung der Registrierung einer gemeldeten Datenanwendung hat, da sie einen Eingriff in subjektive Rechte eines Auftraggebers darstellt, mit Bescheid zu geschehen. Derartige Bescheide unterliegen der kollegialen Beschlussfassung der DSK.

Seit Inkrafttreten des DSG 2000 besteht darüber hinaus die Möglichkeit, bei Datenanwendungen, die der Vorabkontrolle unterliegen, mit Bescheid Auflagen für die Führung der Datenverarbeitung zu erteilen. Hiedurch kann ganz wesentlich Einfluss auf Organisation und Inhalt von Verarbeitungen mit besonderem

[3] Die Zuständigkeit nach § 46 DSG 2000 hat sich als äußerst bedeutsam erwiesen im Zusammenhang mit der Ermittlung von Daten für die Arbeit der Historikerkommission (vgl. auch FN 10).

[4] Derartige Entscheidungen existieren für die Schweiz, Ungarn, Kanada, Guernsey, Argentinien und für den sog. „safe harbour“, das sind US-Unternehmen, die sich durch Eintragung in eine im Internet abrufbare Liste, die vom US Department of Commerce geführt wird, zur Einhaltung gewisser datenschutzrechtlicher Grundsätze („Grundsätze des safe harbor“) verpflichtet haben (http://www.export.gov/safeharbor/. Vgl im Übrigen FN 11 und 12.

[5] Dies ist derzeit nur hinsichtlich der Schweiz und Ungarn durch Verordnung festgestellt (BGBl. II Nr. 521/1999). Diese Verordnung wurde vor den diesbezüglichen Entscheidungen der EU-.Kommission erlassen. Da die Entscheidungen der EU-Kommission unmittelbar anwendbares und verbindliches Recht darstellen, wurde von einer Wiederholung in einer nationalen Verordnung Abstand genommen.

Gefährdungspotential genommen werden, was für effektiven Datenschutz sehr wichtig ist (vgl. hiezu auch Pkt. 5.7). Auch diese Entscheidungen unterliegen der kollegialen Beschlussfassung.

4.1.7 Amtswegige Prüfverfahren

Aus § 30 Abs. 2 DSG 2000 ergibt sich weiters auch die Zuständigkeit der Datenschutzkommission, Prüfverfahren (samt Einschau) bei Datenverarbeitungen „im Falle eines begründeten Verdachts auf Verletzung der im [§ 30] Abs. 1 genannten Rechte und Pflichten“ durchzuführen. Diese Zuständigkeit kann bei Datenverarbeitungen, die der so genannten „Vorabkontrolle“ (vgl. § 18 Abs. 2 DSG 2000) unterliegen, weil es sich um Verarbeitungstypen mit besonderem daten-schutzrechtlichem Gefährdungspotential handelt, von Amts wegen „auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung“ (§ 30 Abs. 3 DSG 2000), d.h. also auch ohne Vorliegen einer Eingabe eines Betroffenen vorgenommen werden. Das Prüfrecht der Datenschutzkommission besteht gleichermaßen gegenüber Datenverarbeitungen des öffentlichen wie des privaten Bereichs. Als Ergebnis einer derartigen Prüfung kann insbesondere auch eine Empfehlung der Datenschutzkommission an die an der Verarbeitung beteiligten Auftraggeber und Dienstleister ergehen. Daneben steht der Datenschutzkommission die Ergreifung auch anderer geeigneter Maßnahmen zur Herstellung des gesetzmäßigen Zustands offen (wie z.B. amtswegige Wiedereröffnung eines Registrierungsverfahrens, Erstattung einer Anzeige an die zuständige Strafbehörde, im privaten Bereich: Klageerhebung bei Gericht usw.).

4.1.8 Äußerung in Beschwerdeverfahren vor dem Verfassungs- oder Verwaltungsgerichtshof (K078-Verfahren und K079-Verfahren)

Ganz generell ist eine steigende Tendenz zur Erhebung von höchstgerichtlichen Beschwerden gegen Bescheide der Datenschutzkommission zu verzeichnen. Dies könnte nicht zuletzt darauf zurückzuführen sein, dass die Beschwerdeführer vor der Datenschutzkommission zunehmend anwaltlich vertreten sind. Abgesehen von den erhobenen Säumnisbeschwerden, deren Gründe in den organisatorisch unzureichenden Arbeitsbedingungen der Jahre 2002 bis 2004 zu suchen sind (vgl hiezu die Ausführungen unter Punkt 3.1.2), liegt die Rate der gegen Bescheide der DSK erhobenen höchstgerichtlichen Beschwerden derzeit bei etwa 10%.

4.1.9 Auskünfte über Vormerkungen im Schengener Informationssystem (K250-Verfahren)

Der Umstand, dass Österreich eine lange Schengen-Außengrenze besitzt, führt dazu, dass viele Personen, welchen die Einreise in die Schengen- Staaten verweigert wird, sich an Österreich und hier wiederum gerne zunächst an die Datenschutzkommission wenden, die allerdings in aller Regel die Auskunftsersuchen nur an das BM für Inneres weiterleiten kann.

4.2 Technische Neuerungen im Geschäftsgang der Datenschutzkommission

Im Berichtszeitraum wurden bei der Datenschutzkommission verstärkt **Anbringen auf elektronischem Weg (E-Mail)** eingebracht. E-Mail hat sich im Berichtszeitraum endgültig neben dem Brief, dem Telefax und dem Telefon als vorrangiges Mittel der Kontaktaufnahme mit der Behörde etabliert.

Das Datenverarbeitungsregister ersucht sogar ausdrücklich darum, Meldungen nur noch mit jenen elektronischen Meldeformularen einzubringen, die auf der Website der Datenschutzkommission angeboten werden.

Die BürgerInnen bringen zahlreiche informelle Anfragen und Ersuchen um Rechtsauskünfte ein, die von der Geschäftsstelle der Datenschutzkommission ebenso informell (und rasch) beantwortet werden. In diesem Punkt hat E-Mail das Telefon als Medium für Rechtsauskünfte ergänzt und teilweise verdrängt. Dieses Phänomen ist auch auf die Website der Datenschutzkommission zurückzuführen, die von den Bürgern intensiv genützt wird. Auf der Website wird auch die E-Mail-Adresse der Datenschutzkommission angeboten.

Weiters ist E-Mail zum bevorzugten Mittel der Kommunikation im Rahmen der Zusammenarbeit zwischen den Datenschutz-Behörden im internationalen Bereich geworden.

Im Jahr 2001 wurde der „**elektronische Akt“** (kurz „ELAK“) als System der elektronischen Aktenverwaltung bei der Datenschutzkommission eingeführt. Seit Feber 2004 steht das Nachfolgeprodukt „ELAK im Bund“ (kurz EiB) in Verwendung. Nach Überwindung zahlreicher Anfangsschwierigkeiten wird zumindest im Büro der DSK der elektronische Akt erfolgreich eingesetzt. Er wird in Zukunft auch die

Kommunikation mit den Mitgliedern der DSK, die ja nur „außer Haus“ erreichbar sind, wesentlich erleichtern. Nicht geklärt ist allerdings derzeit noch die Verwendbarkeit von elektronischen Akten im Zusammenhang mit der Vorlageverpflichtung von Akten in höchstgerichtlichen Beschwerdeverfahren, weshalb die rechtsförmlichen Verfahren der DSK noch parallel mit Papierakten geführt werden.

Im Datenverarbeitungsregister hatten sich seit Einführung des ELAK viele Probleme mit dem Übergang zwischen der alten Host-Datenbank und dem ELAK ergeben. Um die Auskunftsfähigkeit des Registers zu erhalten, wird derzeit noch, wenn ein bereits in der Applikation der Statistik Austria registrierter Auftraggeber eine Folge- oder Änderungsmeldung einbringt, der in Papierform vorhandene Altbestand so weit wie möglich rückerfasst und eingescannt und in den ELAK übernommen. Insgesamt hat sich herausgestellt, dass der ELAK keine ressourcensparende Methode zur Behandlung der Geschäftsfälle des DVR darstellt. Deshalb wurde für das Datenverarbeitungsregister die Entwicklung eines eigenen Datenbanksystems in Auftrag gegeben, das unmittelbar vor der Inbetriebnahme steht und zu größerem Komfort bei der Abfrage des Registers und zur Beschleunigung bei der Bearbeitung der Registrierungsanträge beitragen soll. Das Projekt hat u.a. die Schaffung einer über Internet abrufbaren Datenbank der DVR-Meldungen, elektronische Meldeformulare mit Fehlerkorrektur, Unterstützung der elektronischen Unterschrift und andere Verbesserungen zum Ziel.

4.3 Statistische Darstellung des Geschäftsganges der Datenschutzkommission

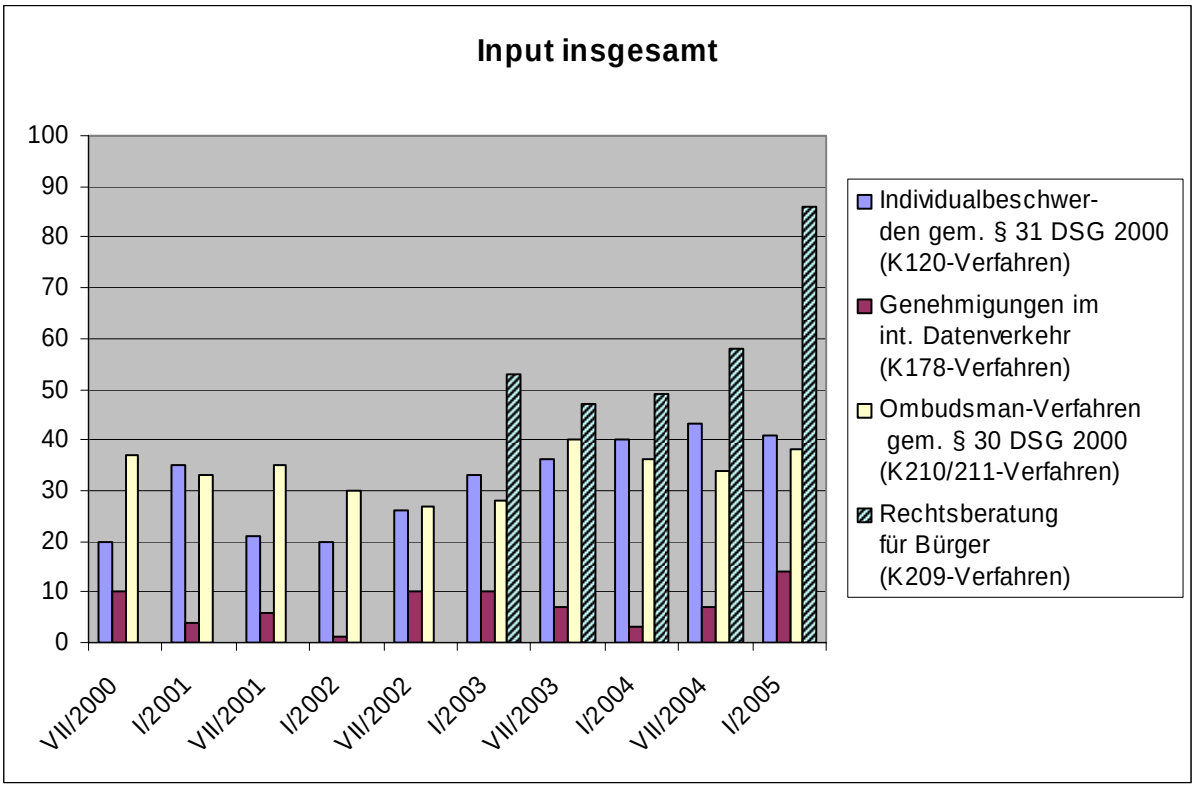
4.3.1 Gesamtübersicht

Statistische Darstellung des Geschäftsganges der Datenschutzkommission:

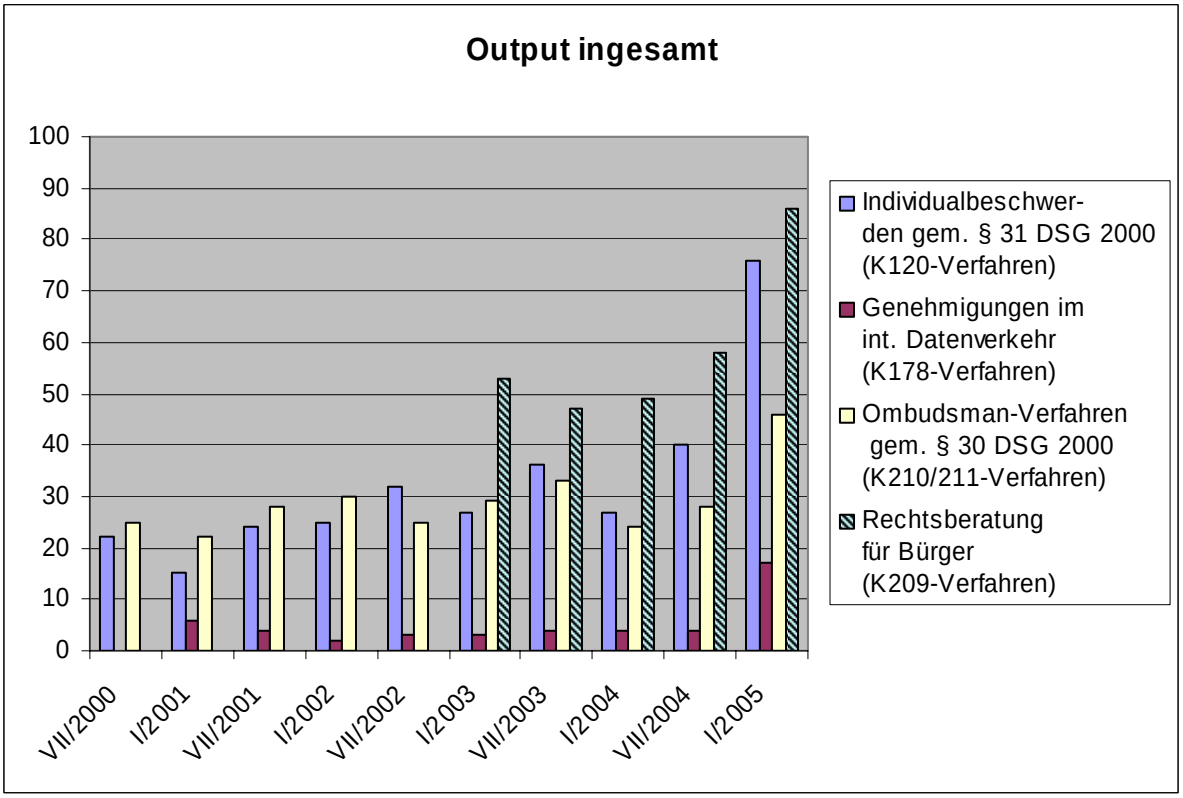
	1.1.2002 in Bearbeitung	Eingangsstücke				Erledigungen				am 30.6.2005 in Bearbeitung	davon Rückstände (älter als 6 Monate)
		2002	2003	2004	1. Hj 2005	2002	2003	2004	1. Hj 2005		
Individualbeschwerden (K120)	60	46	69	83	41	57	63	67	76	36	1
Ombudsmanverfahren nach § 30 DSG 2000 (K210 + K211)	49	57	68	70	38	55	62	52	46	67	29
Rechtsauskünfte (K209)	-	-	100	107	86	-	100	107	86	0	0
Genehmigungen nach §§ 46 und 47 DSG 2000 (K202)	3	7	8	3	0	3	8	7	1	2	2
Genehmigungen im Internationalen Datenverkehr (K178)	19	11	17	10	14	5	7	8	17	34	20

	1.1.2002 in Bearbeitung	Eingangsstücke				Erledigungen				am 30.6.2005 in Bearbeitung	davon Rückstände (älter als 6 Monate)
		2002	2003	2004	1. Hj 2005	2002	2003	2004	1. Hj 2005		
Entscheidungen der DSK im Registrierungs-verfahren (K503)		Ca. 770 Fälle hpts. betr. die „Warnliste der Banken“			3	Ca. 770 Fälle hpts. betr. die „Warnliste der Banken“			2	1	0
Überprüfung von Datenanwen-dungen (K095)	1	3	5	6	1	3	5	6	0	2	1
Verfassungs- und Verwaltungs-gerichtshof-beschwerden (K078 und K079)	0	4	6	23	11	4	6	23	11	0	0
Auskunft Schengener Informations-system (K250)	-	5	20	20	9	5	16	18	11	4	0

4.3.2 Graphische Übersicht des Arbeitsanfalls



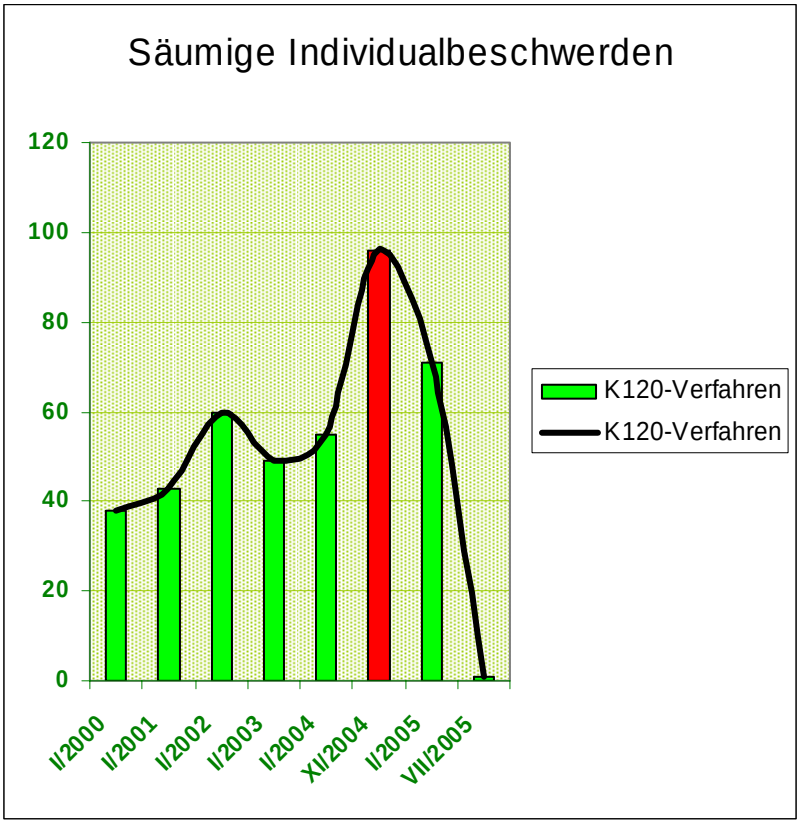
4.3.3 Graphische Übersicht der Erledigungen



Die graphische Darstellung ist auf Halbjahre bezogen, um angesichts des Beginns der Funktionsperiode mit 1. Juli 2000 und des Endes der Funktionsperiode mit 30. Juni 2005 vergleichbares Zahlenmaterial zu erhalten.

Aus dem Diagramm ergibt sich deutlich, dass der Arbeitsanfall (Input) in den meisten Verfahrensarten stetig steigt.

Was den Output betrifft, zeigt die diesbezügliche Graphik, dass er nach einem Absacken in den Jahren 2002 bis 2004 seit dem 1. November 2004 und insbesondere im heurigen Jahr enorm gesteigert werden konnte, und zwar in allen erfassten Verfahrenarten. Besonders deutlich wird dies bei der Erledigung von Individualbeschwerden gemäß § 31 DSG 2000, wo im ersten Halbjahr 2005 bereits doppelt so viele Beschwerden erledigt wurden wie in den früheren Halbjahresabschnitten.



Besonders deutlich lässt sich das Leistungsergebnis an der Anzahl der jeweils säumigen Individualbeschwerden nach § 31 DSG 2000 messen: Zunächst schnellte die Anzahl der Rückstände im zweiten Halbjahr 2001 hinauf, sodass am 1. Jänner 2002 50% mehr Rückstände vorhanden waren als ein halbes Jahr zuvor. Um die

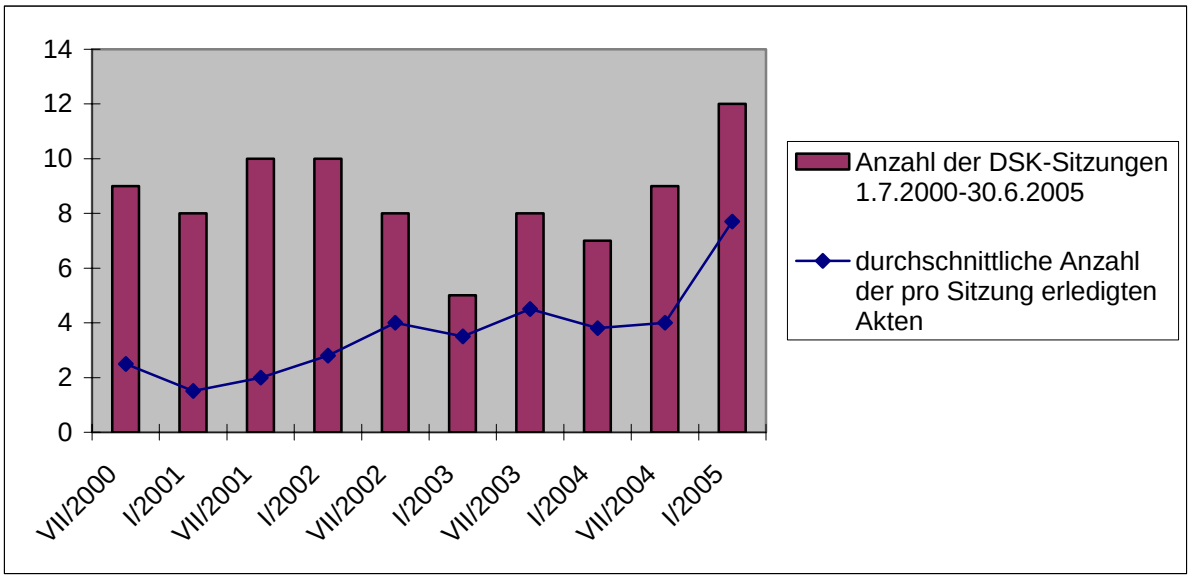
Jahreswende 2002/2003 wurden unter tatkräftiger Mithilfe der Mitglieder der DSK besondere Anstrengungen unternommen, um die ärgsten (= ältesten) Rückstände bei den Beschwerdeverfahren nach § 31 DSG 2000 aufzuarbeiten, was im Diagramm auch sichtbar ist (Desgleichen wurde Anfang 2003 endlich der seit 1998 fällige Datenschutzbericht erstattet).

In der zweiten Jahreshälfte 2003 stiegen die Rückstände bei den Erledigungen der DSK – auch durch stark vermehrten Eingang – jedoch wieder deutlich an, sodass zu Beginn 2004 das ursprüngliche Rückstandsniveau schon wieder erreicht war, das sich in der zweiten Hälfte 2004 geradezu dramatisch steigerte. (Zu den ursächlichen organisatorisch/personellen Defiziten vgl. die Ausführungen unter Punkt 3.1.2).

Die Bestandsaufnahme anlässlich der Besetzung des neu geschaffenen Postens eines Leiters der Geschäftsstelle mit 1. November 2004 ergab folgendes Bild: Der Zustand der Geschäftserledigung im Büro der DSK wies neben beachtlichen Rückständen in allen Geschäftsbereichen vor allem 96 Verfahren gem. § 31 DSG 2000 auf, bei welchen die Entscheidungsfrist gem. § 73 AVG bereits abgelaufen war. Dieser Umstand hat – obwohl Rückstande in der Geschichte der DSK angesichts der seit langem ungenügenden Konstruktion des Geschäftsapparats nichts Ungewöhnliches waren – 2004 und auch noch 2005 zu einer unverhältnismäßig hohen Anzahl von Säumnisbeschwerden an den VwGH geführt.

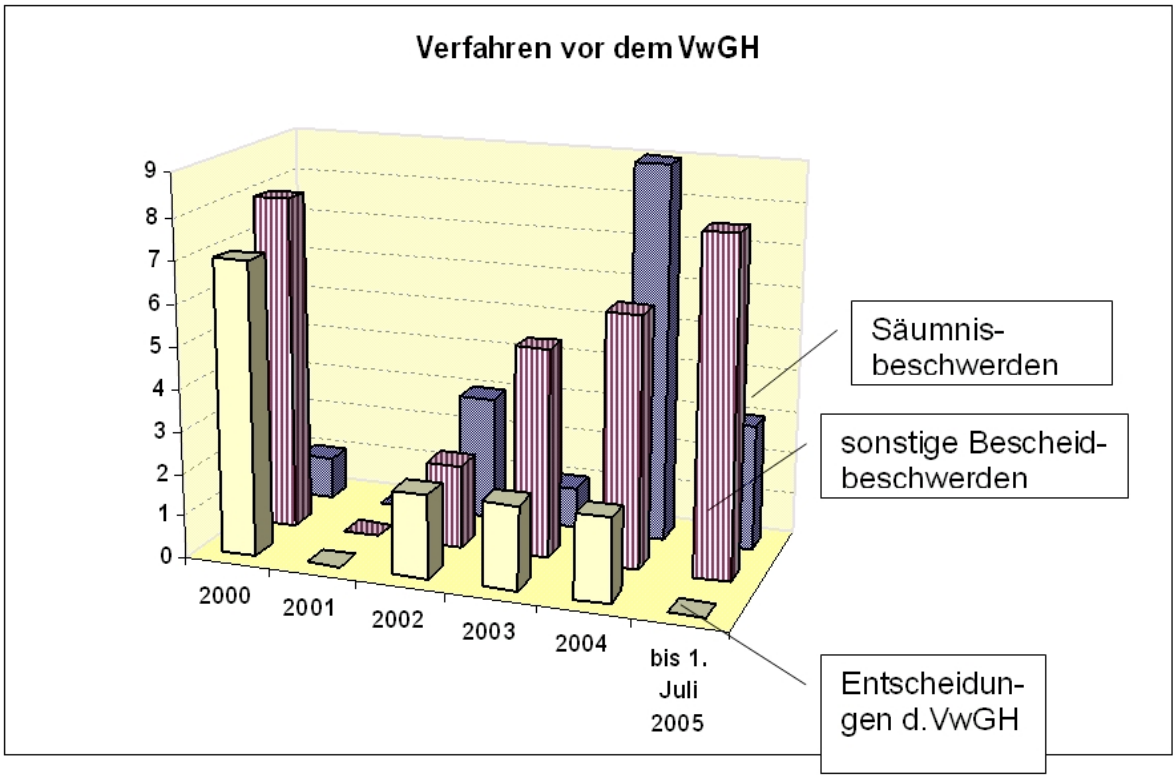
Seit November 2004 wurden - auch nach Vornahme gewisser personeller Änderungen in der Geschäftsstelle - alle erdenklichen Anstrengungen unternommen, um die Rückstände aufzuarbeiten. Insbesondere hinsichtlich der Beschwerde-verfahren nach § 31 DSG 2000 ist dies bis zum Ende der Geschäftsperiode der derzeit im Amt befindlichen Kommission mit 30. Juni 2005 auch tatsächlich gelungen, wie die vorliegende Graphik eindrucksvoll zeigt. Auch bei den anderen Verfahrens-arten ist die Beseitigung von Rückständen bestens unterwegs, wie aus dem Diagramm über den „Output insgesamt“ ersichtlich ist.

4.3.4 Sitzungshäufigkeit und Effizienz



Nicht nur die Effizienz der Arbeit des Geschäftsapparats der DSK sondern auch die der Arbeit in den Sitzungen der DSK konnte wesentlich gesteigert werden: Es konnte nicht nur die Zahl der Sitzungen erhöht werden, sondern insbesondere auch die Anzahl der pro Sitzung erledigten Akten, und zwar um etwa 100%.

4.3.5 Verfahren vor dem Verwaltungsgerichtshof



Beschwerden wegen Säumnis und inhaltliche Beschwerden sind gesondert ausgewiesen.

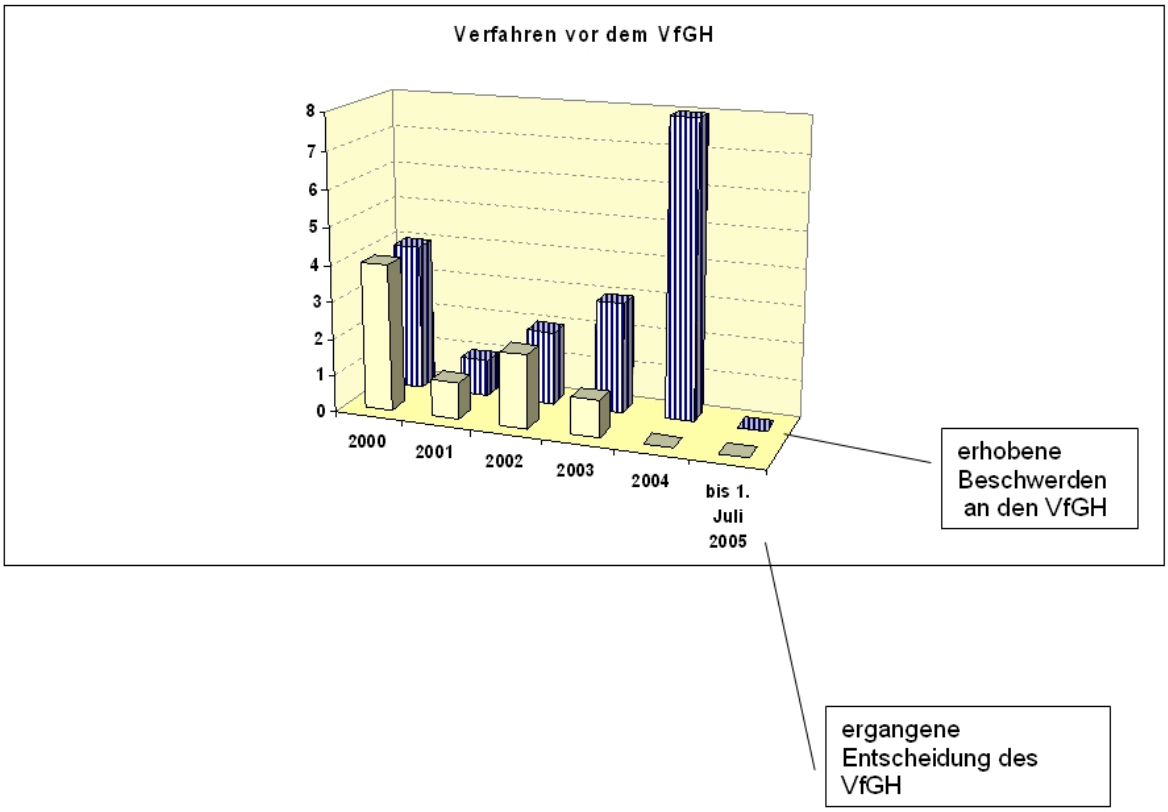
Die enormen Rückstände, die sich während des Jahres 2004 in besonderem Maße angesammelt haben, haben sich in einer im DSK-Bereich bisher nie erreichten Anzahl von Säumnisbeschwerden niedergeschlagen. Dass daraus dem BKA Kosten entstanden sind, muss als Preis dafür gesehen werden, dass das für die Personalfragen des Geschäftsapparats der DSK zuständige Bundeskanzleramt die vielfachen Appelle des geschäftsführenden Mitglieds der DSK, den Posten des Büroleiters zumindest interimistisch zu besetzen, die längste Zeit ungehört verhallen ließ.[6] Da mit dem Ende des Berichtszeitraums die säumigen Verfahren jedoch erledigt sind, ist zu hoffen, dass eine Häufung von Säumnisbeschwerden grundsätzlich der Vergangenheit angehört.

Ergänzend sei noch die Anmerkung gestattet, dass die besondere Stellung der DSK als erste und letzte Instanz die Einhaltung der 6-monatigen Entscheidungsfrist oft nicht leicht macht. Dies deshalb, weil der Sachverhalt erst zur Gänze ermittelt werden muss, was oft einige Zeit in Anspruch nimmt, und weil die sich daraus ergebenden Rechtsprobleme mit einer Gründlichkeit und Qualität behandelt werden müssen, die einer – unmittelbar anschließenden – Prüfung durch die Höchstgerichte möglichst standhalten soll.

Was die Erhebung von Beschwerden an den Verwaltungsgerichtshof wegen inhaltlicher Fragen betrifft, zeigt die erstellte Graphik ein stetiges, wenn auch nicht dramatisches Ansteigen. Zu erwähnen ist, dass die DSK in höchstgerichtlichen Verfahren grundsätzlich immer eine Stellungnahme abgibt. (Vgl. die unter Punkt. 4.3.1 ersichtliche Gesamtstatistik des Geschäftsgangs). Von den 10 inhaltlichen Beschwerden, über die der VwGH seit 1. Juli 2000 entschieden hat, wurden die Entscheidungen der DSK in 8 Fällen bestätigt und in den 2 restlichen Fällen teilweise bestätigt, teilweise aufgehoben.

[6] Dies obwohl allen Beteiligten bekannt war, dass die aushilfsweise Übernahme von Arbeit durch die Abteilungsleitung infolge des Sonderprojekts der Ausarbeitung eines E-Government-Gesetzes völlig unmöglich war und im Gegenteil die Abteilungsleitung selbst dringend zusätzliche Unterstützung gebraucht hätte.

4.3.6 Verfahren vor dem Verfassungsgerichtshof



Hier fällt auf, dass im Jahre 2004 die Anzahl der Verfassungsgerichtshof-beschwerden ganz unverhältnismäßig zugenommen hat, während im 1. Halbjahr 2005 – nach dem Kenntnisstand der DSK - noch keine einzige eingebracht wurde. Diese Entwicklung resultiert daraus, dass hinsichtlich eines ganz bestimmten Rechtsproblems (Löschung von bestimmten Daten aus Polizeiakten) im Jahre 2004 gleichartige Beschwerden für viele Betroffene eingebracht wurden.

Als Ergebnis der Beschwerdebehandlung durch den VfGH ist Folgendes festzuhalten: Von den seit dem 1. Juli 2000 insgesamt 18 erhobenen Beschwerden wurden bis dato 8 Fälle entschieden. Dabei wurde in 5 Fällen die Beschwerde abgewiesen, in einem Fall erfolgte eine Einstellung und in 2 Fällen wurde ein Gesetzes- bzw. Verordnungsprüfungsverfahren eingeleitet. Bemerkt sei, dass die DSK selbst kein Anfechtungsrecht vor dem VfGH besitzt, sodass Bedenken gegen Rechtsvorschriften von der DSK nur allenfalls in der Begründung einer Entscheidung releviert werden können.

5. Schwerpunktbereiche in den Verfahren vor der Datenschutzkommission

5.1 Allgemeine Bemerkungen

In den früheren Datenschutzberichten war es üblich, einzelne Entscheidungen, geordnet nach Fachgebieten, zu präsentieren. Dieser Bericht geht einen neuen Weg:

Da die Datenschutzkommission ihre Entscheidungen im öffentlich zugänglichen Rechtsinformationssystem des Bundes (RIS) an der Internetadresse http://www.ris.bka.gv.at/dsk/ regelmäßig publiziert, konzentriert sich der Datenschutzbericht 2005 nicht auf die Wiedergabe einzelner Entscheidungen, sondern auf Schwerpunktbereiche und daraus resultierende Erfahrungen.

5.2 Auskunftsverfahren nach § 26 iVm § 31 DSG 2000

Es fällt auf, dass im Bereich der Individualbeschwerden der Anteil der Auskunftsverfahren nach § 26 DSG 2000 sehr hoch war. Im Jahr 2002 wurde in 26 von 46 Beschwerden, im Jahr 2003 in 34 von 69 Beschwerden eine Verletzung des Auskunftsrechts behauptet. Auch im Jahr 2004 betrafen annähernd die Hälfte der Beschwerden das Auskunftsrecht (48 von 83 Fällen). Dieses Zahlenverhältnis ist vor allem darauf zurückzuführen, dass gemäß den §§ 1 Abs. 5 und 31 Abs. 1 DSG 2000 nur die Datenschutzkommission für Beschwerden wegen eines Verstoßes gegen das Auskunftsrecht zuständig ist, unabhängig davon ob der belangte Auftraggeber zum öffentlichen oder privaten Bereich gehört. Beschwerden wegen anderer Rechte können hingegen nur dann vor die Datenschutzkommission gebracht werden, wenn der belangte Auftraggeber dem öffentlichen Bereich angehört.

Viele dieser Auskunftsbeschwerden erfolgten, weil Auftraggeber nicht bereit waren, korrekt und innerhalb der Frist von acht Wochen ihrer Pflicht zur Auskunftserteilung nachzukommen.

In einer großen Anzahl von Fällen lag kein gesetzlicher Grund vor, der zur Verweigerung zur Auskunft berechtigt hätte. Diese unterblieb vielmehr regelmäßig auf Grund von Untätigkeit, schlechter Organisation, Unkenntnis der Rechtslage (und mangelnder Bereitschaft, sich zu informieren) oder „Geheimniskrämerei“. Viele Beschwerden hätten mit etwas mehr Kunden- oder Bürgerfreundlichkeit der datenschutzrechtlichen Auftraggeber vermieden werden können.

Ein in diesem Zusammenhang häufig gemachter Fehler der Auftraggeber besteht darin, lediglich über die zur Verarbeitung vorgesehene Datenarten statt über die tatsächlich zur Person des Betroffenen verarbeiteten Dateninhalte Auskunft zu geben. Um die Datenrichtigkeit zu überprüfen, bedarf der Betroffene der konkreten Information, zum Beispiel, dass sein „Geburtsdatum“ mit „01. 05. 1969“ verarbeitet wird, nicht nur der Angabe, dass sein Geburtsdatum gespeichert wird.

Im Berichtszeitraum ereigneten sich mehrere Fälle, in denen Betroffene gleichzeitig mit der Auskunft auch die Löschung der Daten verlangten. Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen dürfen Daten über den Betroffenen, der das Auskunftsverlangen stellt, für einen Zeitraum von vier Monaten keinesfalls gelöscht werden. Falls der Betroffene Beschwerde an die Datenschutzkommission erhebt, gilt das Löschungsverbot bis zum rechtskräftigen Abschluss des Verfahrens (§ 26 Abs. 7 DSG 2000). Wer Daten vorsätzlich zu früh löscht, macht sich nach § 52 Abs. 1 Z 4 DSG 2000 strafbar (Verwaltungsübertretung mit Geldstrafe bis zu 18.890 Euro).

Im Übrigen kann das Auskunftsrecht über eigene Daten nur dann geltend gemacht werden, wenn der Betroffene dem Auftraggeber seine Identität nachweist (etwa durch Übersendung einer Ausweiskopie mit einem Vergleichsmuster seiner Unterschrift). Diese Bestimmung in § 26 Abs. 1 DSG 2000 ist nicht, wie von Betroffenen manchmal vermutet, eine Schikane zur Erschwerung der Geltendmachung des Auskunftsrechts, sondern eine sinnvolle Sicherheitsvorkehrung, um den Missbrauch des Auskunftsrechts zur Informationsbeschaffung über Dritte auszuschließen.

Auch ohne Identitätsnachweis muss der Auftraggeber zwar auf das Auskunftsbegehren reagieren, dies erschöpft sich jedoch zunächst darin, den Auskunftswerber zur Erbringung des Identitätsnachweises aufzufordern und ihm mitzuteilen, dass im Fall der Nichterbringung des Identitätsausweises eine Auskunftserteilung unterbleiben wird. Das Fehlen eines Identitätsnachweises führt also in jedem Fall zu einem Mehraufwand beim Auftraggeber wie auch beim Auskunftswerber und zu einer Verzögerung der Erteilung einer inhaltlichen Auskunft.

Es steht dem Auskunftswerber jedoch nicht zu, die Zustellung der Datenauskunft per eigenhändigem Rückscheinbrief zu verlangen. Freilich steht es dem Auftraggeber

frei, selbst diesen Weg der Zustellung zu wählen, um eine Zustellung an die richtige Person zu gewährleisten.

5.3 Schwerpunktthemen bei Verfahren nach § 30 und § 31 DSG 2000

5.3.1 Sicherheitsverwaltung

Mit 9 Beschwerden im Jahr 2002 und je 16 Beschwerden in den Jahren 2003 und 2004 stellte der Bereich der Sicherheitsverwaltung einen wichtigen Schwerpunkt in der Arbeit der Datenschutzkommission dar. Dies ergibt sich naturgemäß aus dem Umstand, dass die Sicherheitsbehörden in einem Bereich arbeiten, in dem personenbezogene Daten in großer Zahl anfallen und meist gegen den Willen der Betroffenen verwendet werden.

Im Berichtszeitraum wurde mehrfach der Wunsch nach Löschung (Vernichtung) von Daten aus Akten bzw. aus Aktenverwaltungssystemen der Sicherheitsbehörden an die Datenschutzkommission herangetragen.

Bei der Behandlung dieser Fälle musste die Datenschutzkommission die Rechte der Betroffenen auf Löschung gegen die Verpflichtung der Behörden zur korrekten Aktenführung abwägen. Weiters hatte die Datenschutzkommission zwischen dem Papierakt selbst und den Kartei- und Aktenverwaltungssystemen, mit denen die Papierakten verwaltet werden, zu unterscheiden. Diese Unterscheidung betrifft an sich alle Aktenverwaltungssysteme; die Entscheidungen der DSK betrafen jedoch fast ausschließlich Akten und Aktenverwaltungssysteme der Sicherheitsverwaltung, und dabei vor allem die Akten über Anzeigen und polizeiliche Ermittlungen. Da gemäß den §§ 1 Abs. 5 und 31 Abs. 2 DSG 2000 eine Beschwerde gegen die Aktenführung der Gerichte nicht vor die Datenschutzkommission gebracht werden kann, konzentrierten sich die Beschwerden im Bereich der Strafverfolgung auf die Aktenführung der Sicherheitsbehörden.

Nach ständiger Rechtssprechung der Datenschutzkommission bildet ein **Papierakt keine Datei** im Sinne des Datenschutzgesetzes. Unter einer Datei ist nur eine Sammlung strukturierter Datensätze zu verstehen, die als Sammlung wiederum nach mindestens einem Suchkriterium geordnet ist (§ 4 Z 6 DSG 2000). Die subjektiven Rechte gemäß der Verfassungsbestimmung des § 1 Abs. 3 DSG 2000

(Auskunftsrecht, Löschungsrecht, Richtigstellungsrecht) sind bei manueller Datenverarbeitung auf andere Formen der Daten- bzw. Informationssammlung als „Dateien“ iSd § 4 Z 6 DSG 2000 nicht anwendbar: Dies gilt insbesondere für Papierakten (vgl. z.B. die Bescheid der Datenschutzkommission vom 4. Juni 2002, GZ K120.810/005-DSK/2002; vom 10. November 2000, GZ 120.707/7-DSK/00 und vom 2. September 2003, GZ K120.846/007-DSK/2003). Dem Begehren auf „Löschung“ von Papier-Akten (verlangt wurde unter anderem die Vernichtung kompletter Akten, die Entfernung einzelner Aktenstücke sowie das Unleserlichmachen bestimmter Passagen) konnte daher nicht Folge gegeben werden. Diese Ansicht steht im Einklang mit Erwägungsgrund 27 der EU-Datenschutzrichtlinie 95/46/EG, wonach „Akten und Aktensammlungen sowie deren Deckblätter, die nicht nach bestimmten Kriterien strukturiert sind, ..unter keinen Umständen in den Anwendungsbereich der Richtlinie [fallen].“

Diese Spruchpraxis wirkt ebenso wie die ständige Rechtssprechung der Datenschutzkommission zur „Berichtigung“ von behördlichen Entscheidungen den Wünschen von Personen entgegen, die unter Umgehung des normalen Instanzenzuges von der Datenschutzkommission die Korrektur einer behördlichen Entscheidung verlangen. Sie beruht weiters auf der Erkenntnis, dass zwischen der Aufbewahrung von Informationen und ihrer Weiterverwendung für einen neuen Zweck unterschieden werden muss. Datenschutzrechtlich bedenklich wäre es z.B., auf der Grundlage einer zwecks interner Dokumentation der Aktenerledigung geführten Aktenkartei improvisierte Leumundsauskünfte u. dgl. zu erteilen.

Ein anderer wesentlicher Beschwerdefall im Bereich der Sicherheitsverwaltung betraf die Verweigerung der Auskunftserteilung über DNA-Daten. Die Datenschutzkommission musste im Jahre 2002 entsprechend der damals geltenden Rechtslage die Beschwerde gegen eine Verweigerung der Auskunft abweisen, da gemäß § 80 SPG in der damals gelten Fassung die Bestimmungen des datenschutzrechtlichen Auskunftsrechts auf erkennungsdienstliche Daten, die gemäß den §§ 70 oder 75 SPG verarbeitet werden, nicht anzuwenden waren. In der Begründung ihrer Entscheidung hat die DSK – die kein Anfechtungsrecht beim Verfassungsgerichtshof besitzt – jedoch Zweifel an der Verfassungsmäßigkeit dieser Regelung erkennen lassen. In der Folge wurde das SPG novelliert. Der Verfassungsgerichtshof stellte im Übrigen anlässlich der Entscheidung über die gegen den Bescheid der DSK

erhobene Beschwerde fest, dass die ursprüngliche Nichtanwendbarkeit des Auskunftsrechts auf erkennungsdienstliche Daten verfassungswidrig war.

5.3.2 Das Zentrale Melderegister

Die Datenschutzkommission hat im Jahr 2003 ein Kontrollverfahren gemäß § 30 DSG 2000 über das Zentrale Melderegister (ZMR) durchgeführt.

Gemäß § 16a Abs. 5 MeldeG war eine beschränkte Abfrage des Zentralen Melderegisters durch Personen außerhalb der öffentlichen Verwaltung („sonstige Abfrageberechtigte“ gemäß § 1 Z 4 MeldeV) zulässig, die einen regelmäßigen, rechtlich begründeten Bedarf nach Meldeauskünften bescheinigen können, wie beispielsweise berufsmäßige Parteienvertreter (Notare, Rechtsanwälte etc.), Banken oder Versicherungen.

Es hatte sich herausgestellt, dass einige dieser Unternehmen, denen das Bundesministerium für Inneres Zugriff auf das Zentrale Melderegister eröffnet hatte, diese Befugnis rechtswidrig verwendeten, um anderen, nicht befugten Personen Abfragen aus dem Zentralen Melderegister zu ermöglichen. Weiters gab es Probleme mit der Gestaltung der Abfrage aus dem Zentralen Melderegister, die auch entsprechende Erwähnung in den abschließenden Empfehlungen fanden. Die dieses Verfahren abschließenden Empfehlungen vom 9. Mai 2003 sind auf der Website der Datenschutzkommission veröffentlicht (http://www.dsk.gv.at/p30_zmr.htm).

Die Vorgänge um inkorrekt handelnde Abfrageberechtigte erzeugten ein beträchtliches Echo in der Öffentlichkeit. Beigetragen hat hiezu auch die Formulierung der – an sich datenschutzrechtlich unbedenklichen – einschlägigen Verordnung des Bundesministers für Inneres[7], in der die Abfrageberechtigten als ‚Business-Partner’ bezeichnet werden. Dies hat in der Öffentlichkeit bei manchen den Eindruck erweckt, die Daten des ZMR würden gezielt zwecks Geldbeschaffung an Private verkauft, ein Eindruck, der sich im Ermittlungsverfahren der Datenschutz-kommission allerdings so nicht bestätigt hat.

Einzelnen ‚Business-Partnern’ des BMI wurde die Abfrageberechtigung inzwischen auch entzogen; in zumindest einem Fall wurde diese Maßnahme aber erfolgreich

[7] Verordnung über die Bestimmung der Support-Unit Zentrales Melderegister (ZMR) als Organisationseinheit, bei der die Flexibilisierungsklausel zur Anwendung gelangt, BGBl. II Nr. 20/2003

beim Verwaltungsgerichtshof angefochten (VwGH Erkenntnis vom 16. Dezember 2003, Zl. 2003/05/0078)

5.3.3 Wahlwerbung durch politische Parteien und Wählerevidenz

Neben der Werbung durch private Stellen musste die Datenschutzkommission im Berichtszeitraum auch Fälle von Werbung durch politische Parteien behandeln. Analog zur Werbung im privaten Bereich (siehe unten) konnte auch hier beobachtet werden, dass in der Öffentlichkeit das Wissen über die datenschutzrechtlichen Grundlagen der Wahlwerbung nicht sehr ausgeprägt ist. Gemäß § 3 Wählerevidenzgesetz 1973, BGBl. Nr. 601/1973, haben die in allgemeinen Vertretungskörpern vertretenen Parteien das Recht, die Daten der Wähler für politische Werbung aus der Wählerevidenz zu erhalten. In den Wahlordnungen der Länder gibt es ähnliche Bestimmungen.

Ein weiteres Problem im gegebenen Zusammenhang besteht darin, dass Adressdaten, für die eine melderechtliche Auskunftssperre besteht (z.B. wegen gefährlicher Drohungen), in der Wählerevidenz weiter zugänglich bleiben. Die Datenschutzkommission hat im Zuge ihrer Tätigkeit festgestellt, dass Bürger, die eine derartige melderechtlichen Auskunftssperre gemäß § 18 Abs. 2 Meldegesetz 1991 (MeldeG), BGBl. Nr. 9/1992, in Anspruch nehmen, oft nicht auf die rechtlichen Grenzen der Auskunftssperre hingewiesen wurden.

5.3.4 Direktmarketing

Im Berichtszeitraum wurde die Gewerbeordnung (GewO 1994) novelliert, wobei die vorher in § 268 GewO 1994 enthaltenen Bestimmungen über das Gewerbe der Adressverlage und Direktmarketingunternehmen durch § 151 GewO 1994, idF BGBl. Nr. 194, idF. BGBl. I Nr. 111/2002, ersetzt wurden.

Die auffallende Häufung von Beschwerdefällen im Zusammenhang mit Direktmarketing in den Jahren 2003 und 2004 war fast ausschließlich auf die sog. „Herold CD“[8] zurückzuführen. Mehrere Bürger machten von ihrem Recht auf Auskunft nach § 26 DSG 2000 Gebrauch und erhoben anschließend Beschwerde an die Datenschutzkommission. Diese Beschwerden wurden im Oktober und November 2003 eingebracht.

[8] Da dieser Fall in der Öffentlichkeit unter dieser Bezeichnung größte Beachtung fand, nimmt die DSK keine Anonymisierung bei der Darstellung des Falles vor.

Mit dem Projekt der „Herold Marketing CD private“ hatte sich die die Datenschutzkommission aber auch schon davor intensiv im Rahmen eins Verfahrens nach § 30 DSG 2000 beschäftigt:

Anlässlich der geplanten Einführung eines Produkts namens „HEROLD Marketing CD private“ wurde in den vorab verbreiteten Medieninformationen der Firma HEROLD behauptet, dass dieses Produkt Daten über eine sehr große Zahl von Privatpersonen (ca. 4 Millionen Menschen mit österreichischem Wohnsitz) nach verschiedensten Datenarten strukturiert, auswählbar und für die Durchführung von Werbeaussendungen unmittelbar geeignet, enthalte. Dieses Produkt könne von jedermann käuflich erworben werden. Diese Ankündigung erregte einiges Aufsehen und entfachte eine lebhafte öffentliche Diskussion über Fragen des Problemkreises Datenschutz und Direktmarketing.

Da eine erste Einschätzung des Dateninhalts der Marketing CD-ROM durch die Datenschutzkommission ergab, dass möglicherweise sensible Daten verarbeitet wurden, und da noch keine Meldung an das bei der Datenschutzkommission eingerichtete Datenverarbeitungsregister (DVR) vorlag, sah sich die Datenschutzkommission dazu veranlasst, die Datenanwendung in Form der auf CD-ROM gespeicherten und übermittelten Daten vorläufig zu untersagen und ein Ermittlungsverfahren einzuleiten (Mandatsbescheid vom 22. August 2003, GZ K211.507/003-DSK/2003). Die Datenschutzkommission hat im Ermittlungsverfahren den Dateninhalt der CD-ROM, die technischen Sicherungen der Daten und die programmtechnischen Mechanismen zur Aktualisierung des Datenbestands einer genauen Prüfung durch A-SIT (Österreichisches Zentrum für sichere Informationstechnologien) als Sachverständigen unterziehen lassen.

Die Sachverhaltsermittlungen haben ergeben, dass auf der Marketing CD neben Identitäts- und Adressdaten so genannte „Marketinganalysedaten“ enthalten sind, d.s. Daten wie etwa Kaufkraftklasse oder Ein- oder Mehrpersonenhaushalt. Solche Daten werden mit Hilfe statistischer Verfahren geschätzt oder aufgrund bestimmter Parameter (z.B. gleicher Adresse) auch nur vermutet.

Besondere Fragen der rechtlichen Beurteilung ergaben sich daraus, dass die hier von der Firma HEROLD gewählte Form der Datenübermittlung und -verwendung für Marketingzwecke in kein gesetzlich vorgesehenes Schema passt. Der Käufer der

CD-ROM erhält die Daten zwar physisch übermittelt und kann sie auf seiner EDV-Anlage verarbeiten. Durch ein ausgeklügeltes System von Verschlüsselung und Validierung können die Daten allerdings nur in einer vom Lizenzgeber, der Firma HEROLD, vorgegebenen Weise benützt und rechtmäßig nicht ohne dessen Mithilfe verändert werden. So besteht etwa ein technischer Zwang, eine regelmäßig aktualisierte Negativliste der Personen, die der Verwendung ihrer Daten (bei HEROLD und dm-plus) widersprochen bzw. die sich in die so genannte „Robinsonliste“ (s. unten) eintragen haben lassen, herunter zu laden und die entsprechenden Personendatensätze zu sperren (ein physisches Löschen ist auf der CD-ROM selbst ohne Zerstörung dieses Datenträgers unmöglich). In wirtschaftlicher Hinsicht kann man davon sprechen, dass es sich um eine Auslagerung der Tätigkeit eines Adressverlags und Direktmarketingunternehmens vom Unternehmen zu dessen Kunden handelt.

Mit Beschluss vom 28. November 2003, GZ K211.507/024-DSK/2003, hat die Datenschutzkommission gemäß § 30 Abs. 6 DSG 2000 Empfehlungen zur Herstellung und Sicherung gesetzmäßiger Verhältnisse bei der Verwendung personenbezogener Daten für Zwecke der Datenanwendung „Herold Marketing CD private“ an die Firma HEROLD als Auftraggeberin der „HEROLD Marketing CD private“ ausgesprochen. Darin wurden gewisse Beschränkungen bei der Verwendung von Marketinganalysedaten, ein kürzere Aktualisierungszyklus für wegen Widerspruchs gesperrte Daten und auf Grundlage der eingeholten Sachverständigengutachten auch einzelne Maßnahmen zur Verbesserung der technischen Datensicherheit empfohlen. Weiters wurde empfohlen, in den vertraglichen Vereinbarungen von HEROLD mit seinen Kunden sicherzustellen, dass die Pflichten eines Direktmarketingunternehmens gemäß § 151 GewO 1994 auch von den Nutzern der CD-ROM übernommen werden.

Diesen Empfehlungen wurde umgehend entsprochen.

Die CD-ROM ist inzwischen für einen beschränkten Nutzerkreis – laut Angaben auf der HEROLD-Website sind dies Unternehmen und registrierte Vereine – erwerbbar. Neben den vertragsrechtlichen rechtlichen Bindung der Käufer und dem auf der CD-ROM angebrachten Übermittlungs- und Kopierschutz, sorgt im Übrigen auch der Preis der CD dafür, dass diese Datei nicht unbeschränkt Verbreitung finden wird.

Die Datenschutzkommission möchte als Ergebnis dieses Verfahrens auch festhalten, dass sie feststellen musste, dass in der Öffentlichkeit das Wissen um das Funktionieren von Direktmarketing und die Möglichkeit, die Verwendung von Daten für Werbezwecke durch Direktmarketingunternehmen auszuschließen, nicht sehr ausgeprägt ist. Insbesondere war auch vielen Betroffenen und Medienvertretern die bei der Wirtschaftskammer Österreich eingerichtete „Robinson-Liste“ unbekannt.In diese Liste kann sich jedermann kostenlos eintragen lassen, der die Verwendung seiner Daten für Werbezwecke durch Adressverlage und Direktmarketingunternehmen untersagen will (§ 151 Abs. 9 GewO 1994). Die Adressverlage und Direktmarketingunternehmen sind gesetzlich verpflichtet, Eintragungen in die Robinson-Liste zu beachten.

5.3.5 Bonitätsprüfung beim Vertragsabschluss mit einem Mobilfunk-Betreiber

Die Datenschutzkommission war mehrmals mit diesem Problemkomplex konfrontiert und hatte sich insbesondere mit dem Bonitätsprüfungssystem der ONE GmbH in mehreren Fällen (nach den §§ 30 und 31 DSG 2000) auseinander zu setzen. Es handelt sich um eine Verbindung zwischen einer alten Problemstellung (Prüfung der Bonität von Kunden) und einem relativ neuen Geschäftsbereich (Mobilfunk). Die Mobilfunk-Betreiber erbringen für den Kunden eine Leistung, die erst im Nachhinein abgerechnet wird. Der Wunsch der Mobilfunk-Betreiber, sich über die finanzielle Situation eines neuen Kunden zu informieren, ist daher durchaus verständlich und als überwiegendes berechtigtes Interesse im Sinnen des § 1 Abs. 2 DSG 2000 zu werten[9]. Das dabei immer wieder auftretende Problem liegt in der Behauptung der Mobilfunkunternehmen, Bonitätsauskünfte von befugten Gewerbebetrieben lediglich einzuholen (und bei der Entscheidung über den Vertragsabschluss einzubeziehen), aber Bonitätsdaten nicht selbst zu speichern. Daher ist es häufig nicht möglich, im Wege eines Auskunftsbegehrens an den Mobilfunkanbieter die bei der Prüfung verwendeten Bonitätsdaten in Erfahrung zu bringen. Will der Betroffene die Quelle von Bonitätsinformationen, die er für falsch bzw. unrechtmäßig verarbeitet hält, erfahren, ist er auf den guten Willen des Betreibers bzw. auf Vermutungen angewiesen. Der Datenschutzkommission ist es jedoch in den anhängigen Fällen gelungen, zumindest die Ursachen negativer Bonitätsprüfungen offen zu legen.

[9] So auch das TKG 2003, das in § 92 Abs. 3Z 3 lit. f iVm § 97 Abs. 1 die Verarbeitung von Bonitätsdaten durch Betreiber ausdrücklich vorsieht

5.3.6 Die Rundfunkgebühr

Viele Betroffene ersuchten die Datenschutzkommission um Information, woher die mit der Einbringung der Rundfunkgebühren betraute GIS Gebühren Info Service GmbH ihre Adressdaten bezieht. Gemäß § 4 Rundfunkgebührengesetz, BGBl. I Nr. 159/1999, darf die GIS von den Meldebehörden die Namen (Vor- und Familiennamen), Geschlecht, Geburtsdatum und Unterkünfte der in ihrem Wirkungsbereich gemeldeten Personen verlangen. Unterlässt ein Meldepflichtiger überdies die von der GIS verlangte Erklärung über den Betrieb von Rundfunkempfangsanlagen, so dürfen seine (Melde-)Daten nicht nur befristet, sondern auf Dauer von der GIS verarbeitet werden (§ 4 Abs. 3 letzter Satz Rundfunkgebührengesetz).

Drei Betroffene erhoben Beschwerden im Zusammenhang mit der Eintreibung der Rundfunkgebühren, andere Betroffene ersuchten um Rechtsauskünfte oder rechtliche Hilfe.

Darunter waren auch Anfragen, wie man mit Hilfe des Datenschutzrechts der Verpflichtung zur Ermittlung der Rundfunkgebühr entrinnen könne. In diesem Zusammenhang war - wie so oft auch in anderen Rechtsbereichen – darauf hinzuweisen, dass es im Allgemeinen nicht möglich ist, sich unter dem Vorwand des Datenschutzes rechtlichen Verpflichtungen zu entziehen.

5.3.7 Datensicherheit

Im Berichtszeitraum war die Datenschutzkommission verstärkt mit Problemen der Datensicherheit befasst. In der Vergangenheit waren Themen der Datensicherheit für die Datenschutzkommission vorwiegend auf Datenverarbeiter des öffentlichen Bereichs beschränkt. Im Berichtszeitraum hat sich dieses Bild grundlegend verändert. Dies liegt zum einen an den veränderten Kompetenzen der Datenschutzkommission, die im privaten Bereich grundlegende Kontrollbefugnisse erlangt hat, zum andern aber auch an der Verbreitung von Technologien, die große Sicherheitsrisiken in sich bergen, wie E-Mail und andere Formen der Nutzung des Internets.

Komplexe Organisationsformen, schwer überschaubare Computersysteme, zu wenig Budget für die Sicherheit und menschliche Fehler ergeben häufig eine gefährliche Kombination, die derartige Vorfälle ermöglichen. Die Datenschutzkommission kann in derartigen Angelegenheiten nur empfehlen, die Verpflichtungen des § 14 DSG 2000

(Datensicherheitsmaßnahmen) sehr ernst zu nehmen (K210.401/001-DSK/2002 vom 5. Feber 2002).

Die Computeranlage eines Unternehmens wurde von einem Computervirus befallen. Dieses Virus war unter dem Namen „SirCam“ weltweit bekannt und grassierte in den Jahren 2001 und 2002 auch in Österreich. „SirCam“ verbreitete sich, indem es Kopien des Virus per E-Mail an alle Absender im E-Mail-Adressbuch des befallenen Computers verschickte. Dabei versendete „SirCam“ zur Tarnung seiner Aktivitäten irgendein Dokument, das sich auf dem befallenen Computer befand als Anlage. Auf diese Weise wurde ein sehr vertrauliches Dokument an einen ahnungslosen Bürger versendet, der diesen Umstand der Datenschutzkommission meldete, nachdem er – vollkommen richtig - die Datei samt Virus gelöscht hatte. Die Datenschutzkommission hat den Vorfall untersucht und konnte nur die Empfehlung abgeben, verstärkt auf die Datensicherheit und den Virenschutz zu achten. (K211.428/001-DSK/2002 vom 22. März 2002).

5.3.8 Belästigungen via Internet, insbesondere Spam

Seit etwa 2003 hat sich für die Datenschutzkommission ein neues Betätigungsfeld eröffnet: Auskunftsverfahren gegen Privatunternehmen wegen unerbetener Direktwerbung per E-Mail (Spam).

Mit der Verbreitung von E-Mail als Mittel der weltweiten Kommunikation hat das Phänomen des „Spamming“ das Internet überschwemmt. Angesichts der Flut an unerbetener E-Mail-Werbung ist der Wunsch nach wirkungsvollen rechtlichen Abwehrmaßnahmen nur zu verständlich. Die angemessene Vorgangsweise gegen Spamming ist eine Anzeige beim zuständigen Fernmeldebüro wegen Verstoßes gegen die §§ 107 und 109 Telekommunikationsgesetz 2003 (TKG 2003), BGBl. I Nr. 70/2003.

Den Betroffenen steht an sich auch die Möglichkeit offen, vom Absender einer unerwünschten Direktwerbung Auskunft gemäß § 26 DSG 2000 über die Herkunft der e-Adresse und in der Folge auch deren Löschung zu verlangen. In der Praxis ergeben sich aber dabei regelmäßig Probleme, weil die Spammer in der Regel nicht in Österreich ansässig sind. Dazu kommt, dass der typische Spammer nur die E-Mail-Adresse des Betroffenen hat und daher den Betroffenen – für Zwecke der Auskunft - nicht einwandfrei identifizieren kann. Die Adressen werden regelmäßig

von Webseiten, Publikationen und anderen öffentlich zugänglichen Quellen beschafft oder auch aufgrund bloßer Namenskombinationen versuchsweise erstellt (eine so genannte „Dictionary Attack“).

Neben zahlreichen informellen Beschwerden und Verlangen nach Rechtsberatung gab es in den Jahren 2003 und 2004 auch je drei formelle Beschwerden wegen Verweigerung der Auskunft durch Spammer.

Wie oben dargestellt, ist das Auskunftsrecht oft keine zielführende Maßnahme gegen Spam und bringt meistens auch keine verwertbaren Erkenntnisse. Die Datenschutzkommission beobachtet diese Entwicklung mit einer gewissen Sorge, da hinsichtlich dieser Beschwerden kaum Erfolge zu erzielen sind.

In einem anderen Fall wurde eine Betroffene ebenfalls durch den Missbrauch des Internets durch einen Dritten (in Form der Verbreitung unrichtiger Daten via Internet) belästigt: Nachdem sie wiederholt am Telefon sexuell belästigt worden war, fand sie heraus, dass ein Unbekannter ein Inserat auf einer Internetseite für einschlägige Kontaktanzeigen mit ihrem Namen, ihrer Telefonnummer und anderen Daten eingeschaltet hatte. In dem Inserat wurde der Eindruck erweckt, die Bürgerin sei an einem „erotischen Abenteuer“ interessiert. Die Bürgerin wollte Auskunft gemäß § 26 DSG 2000 vom Inhaber des Online-Forums über die Person, die das Inserat eingeschaltet hatte. Die Auskunft wurde nicht erteilt, und die Bürgerin erhob Beschwerde an die Datenschutzkommission. Die Beschwerde wurde abgewiesen, weil dem Inhaber die Eigenschaft eines Auftraggebers nach dem Datenschutzgesetz mangelte: Er bot auf der Seite nur die Möglichkeit an, Inserate zu veröffentlichen, ohne dass er Einfluss darauf nahm, welche Daten verarbeitet werden. Es ist zu betonen, dass solche Vorgehensweisen jedoch keineswegs legal sind und durchaus Möglichkeiten bestehen, den Verursacher festzustellen und rechtlich zu verfolgen (Sanktionen nach dem E-Commerce-Gesetz, Strafe wegen Ehrenbeleidigung oder übler Nachrede, zivilrechtlicher Unterlassungsanspruch; vgl. den Bescheid K120.831/005-DSK/2003 vom 2. September 2003).

In einem anderen Fall beschwerte sich eine Bürgerin, weil ein Unbekannter sich in diversen Online-Foren für Sie ausgegeben und durch beleidigende Postings in Verruf gebracht hatte. Die Beschwerde musste negativ enden, weil das Datenschutzgesetz

keine „Beschwerde gegen Unbekannt“ kennt (K121.012/0001-DSK/2005 vom 14. Jänner 2005). Derartige Sachverhalte können nur strafrechtlich verfolgt werden.

5.4 Genehmigung zur Datenübermittlung für Zwecke der wissenschaftlichen Forschung und Statistik und Genehmigungen bzw. zur Benachrichtigung und Befragung von Betroffenen

Bei der Datenschutzkommission wurden im Berichtszeitraum vor allem Anträge auf Genehmigung für die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik gemäß § 46 Abs. 3 DSG 2000 gestellt.

Waren im Berichtszeitraum des Datenschutzberichtes 2001 einige Anträge aus dem Fachbereich der Medizin gestellt worden, so waren es im Berichtszeitraum des Datenschutzberichtes 2005 vor allem Historiker und Sozialforscher, die derartige Anträge stellten. Im Jahr 2002 langten fünf Anträge nach § 46 Abs. 3 DSG 2000 ein, davon vier aus dem Bereich der Geschichtsforschung und einer aus dem Bereich der Sozialwissenschaften. Im Jahr 2003 gab es acht Anträge, davon einen aus dem Bereich der Geschichtsforschung, zwei aus dem Bereich der Sozialwissenschaft und fünf aus dem Fachgebiet der Medizin. Im **Bereich der Sozialwissenschaften und der Medizin** war das Feld der Genehmigungsanträge weit gestreut, von der Erforschung von Unfällen im Straßenverkehr über die Analyse von Selbstmorden bis hin zu Jugendwohlfahrt und Berufsausbildung.

Die **Anträge von Historikern** gemäß §§ 46 Abs. 3 und 47 DSG 2000 bezogen sich fast ausschließlich auf Datenbestände aus der Zeit des Nationalsozialismus. Dies steht im Zusammenhang mit der Arbeit der Historikerkommission[10].

Die Datenschutzkommission erteilte Genehmigungen mit Bescheid gemäß § 46 Abs. 3 DSG 2000 unter Bedingungen und Auflagen, wenn dies notwendig war, um sicherzustellen, dass die im DSG 2000 verankerten Grundsätze der Zweckgebundenheit (§ 6 Abs. 1 Z 1 DSG 2000), der Wesentlichkeit (§ 6 Abs. 1 Z 3 DSG 2000) und der zeitlichen Begrenztheit (§ 6 Abs. 1 Z 5 DSG 2000) der Datenverwendung gewahrt bzw. nicht in überschießender Weise beeinträchtigt werden.

[10] Die Historikerkommission der Republik Österreich wurde eingerichtet durch Beschluss der österreichischen Bundesregierung vom 1. Okt. 1998 mit dem Mandat, die Fragen des Vermögensentzuges in nationalsozialistischer Zeit und Rückstellungen und Entschädigungen durch die Republik Österreich nach 1945 zu erforschen und darüber Bericht zu erstatten.

Bei einigen Anträgen gab es auch Missverständnisse. So musste die Datenschutzkommission klarstellen, dass eine Genehmigung gemäß §§ 46 oder 47 DSG 2000 kein Recht des Wissenschaftlers auf Herausgabe von Daten gegenüber dem Inhaber des Datenmaterials verschafft. Dies betrifft in erster Linie den Zugang zu Archiven. Die Genehmigung nach § 46 DSG 2000 berechtigt den Inhaber der Daten zur Übermittlung und den Genehmigungswerber zur Verwendung der übermittelten Daten, sie kann aber niemanden zur Herausgabe von Unterlagen zwingen.

Inzwischen hat das Bundeskanzleramt unter anderem auf Anregung der Datenschutzkommission in einem Rundschreiben vom Jänner 2004 (GZ K810.018/002-V/3/2003 die datenschutzrechtliche Situation im Hinblick auf § 46 DSG 2000 erläutert.

5.5 Genehmigungen im internationalen Datenverkehr (§ 13 DSG 2000)

Das Datenschutzgesetz 2000 hat – entsprechend der Richtlinie 95/46/EG - den internationalen Datenverkehr bereits stark liberalisiert und vor allem die Genehmigungsfreiheit von Datenübermittlungen innerhalb der europäischen Union normiert (§ 12 DSG 2000).

Im Berichtszeitraum (1.1.2002 bis 30.6.2005) wurden bezüglich des Datentransfers in andere Staaten noch folgende zusätzliche Maßnahmen und Entscheidungen erlassen, die von Relevanz für die Reduzierung der Aufgaben der Datenschutzkommission betreffend den internationalen Datenverkehr sind:

- Entscheidung der Europäischen Kommission vom 30. Juni 2003 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Argentinien (Abl. L 168, 5. Juli 2003);

- Entscheidung der Europäischen Kommission vom 21. November 2003 über die Angemessenheit des Schutzes personenbezogener Daten auf der britischen Kanalinsel Guernsey (ABl. L 308, 25. November 2003).

Die „Safe Harbor“-Vereinbarung mit den vereinigten Staaten von Amerika entfaltete ihre Wirkung[11]; und auch die Standardvertragsklauseln der europäischen Union kamen zum Einsatz.

[11] Weitere Informationen finden Sie auf der Website des amerikanischen Handelsministeriums (U.S. Department of Commerce): http://www.export.gov/safeharbor/

Auf der Website der Europäischen Kommission ist eine eigene Seite für Entscheidungen der Kommission zur Angemessenheit des Schutzes persönlicher Daten in Drittstaaten eingerichtet.[12]

In der Praxis hatte und hat die Datenschutzkommission gerade in diesem Bereich auch damit zu kämpfen, dass einige wesentliche Rechtsfragen nicht entsprechend geklärt waren und auch noch nicht geklärt sind. Da diese Rechtsfragen in besonderem Maße von dem Gebot nach EU-einheitlichen Lösungen geprägt sind, besteht eine gewisse Zurückhaltung seitens der österreichischen Datenschutzkommission bei Alleingängen. So besteht etwa derzeit keinerlei gemeinsame Auffassung hinsichtlich jener Gründe, aus welchen in Konzernen z.B. Personaldaten zulässigerweise an andere (ausländische) Konzernmitglieder übermittelt werden dürfen. Hinzu kommt Folgendes:

- Die komplexe Materie sorgt immer wieder für in sich widersprüchliche Anträge, die von den Mitarbeitern der Geschäftsstelle der DSK in mühevoller Kleinarbeit richtig gestellt werden müssen.
- Die Beteiligung großer internationaler Konzerne mit wenig Kenntnis der deutschen Sprache und geringem Wissen über europäisches Recht schafft zusätzliche Komplikationen.
- Die schwierige Kommunikation zwischen der DSK, dem vertretenden Anwalt, dem Antragsteller und dessen Partnern im Ausland führt häufig zu beträchtlichen Verzögerungen.

5.6 Mitteilungen von der Heranziehung eines Dienstleisters gemäß § 10 Abs. 2 DSG 2000

Das Datenschutzgesetz 2000 sieht vor, dass die beabsichtigte Heranziehung eines Dienstleisters durch einen Auftraggeber des öffentlichen Bereichs im Rahmen einer Datenanwendung, die der Vorabkontrolle gemäß § 18 Abs. 2 DSG 2000 unterliegt, der Datenschutzkommission mitzuteilen ist. In diesem Tätigkeitsbereich war im Berichtszeitraum ein rasanter Anstieg der Meldungszahlen zu verzeichnen. Dies war teilweise bedingt durch den anhaltenden Trend zum Outsourcing von EDV-Leistungen Teilweise hat auch der verstärkte Einsatz von „intelligenten“ Geräten, die personenbezogene Daten speichern können, bewirkt, dass immer mehr Wartungs- und Reparaturtätigkeiten datenschutzrechtlich relevant werden können. Auf diese Weise werden immer mehr Unternehmen, die ein Produkt warten und betreuen, zum

[12] http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_de.htm

datenschutzrechtlichen Dienstleister. Dies betrifft u.a. auch die Fernwartung von Computersystemen, die sich immer größerer Beliebtheit erfreut.

5.7 Entscheidungen der Kommission in Registrierungsverfahren

Ende 2001 hat die Datenschutzkommission im Rahmen eines Kontrollverfahrens betreffend die „Warnliste der österreichischen Kreditinstitute“ die Empfehlung ausgesprochen, eine entsprechende Meldung über die Teilnahme als Auftraggeber an dem Informationsverbundsystem zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten. Im Berichtszeitraum wurden die diesbezüglichen Meldungen von ca. 770 involvierten Kreditinstituten eingebracht. Die gegenständliche Datenanwendung unterliegt der Vorabkontrolle, da sie die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Inhalt hat (§ 18 Abs. 2 Z 3 DSG 2000) und darüber hinaus in Form eines Informationsverbundsystems geführt wird (§ 18 Abs. 2 Z 4 DSG 2000). § 21 Abs. 2 DSG 2000 sieht vor, dass bei Datenanwendungen, die gemäß § 18 Abs. 2 2000 der Vorabkontrolle unterliegen, auf Grund der Ergebnisse des Prüfverfahrens bei der Meldung dem Auftraggeber Auflagen für die Vornahme der Datenanwendung durch Bescheid erteilt werden können, soweit diese zur Wahrung der durch das DSG 2000 geschützten Interessen der Betroffenen notwendig sind.

Anlässlich der Registrierung der „Warnliste“ wurden jedem teilnehmenden Auftraggeber Auflagen gemäß § 21 Abs. 2 DSG 2000 für die Vornahme der Datenanwendung durch Bescheid erteilt.

Aufgrund einer Vereinbarung zwischen dem Bund und den Ländern gemäß Art. 15a B-VG wurde von 35 Auftraggebern die Datenanwendung „Teilnahme am Informationsverbundsystem: Betreuungsinformationssystem über die Gewährleistung der vorübergehenden Grundversorgung für hilfs- und schutzbedürftige Fremde in Österreich“ gemeldet. Von jenen teilnehmenden Auftraggebern, in deren Wirkungsbereich eine landesgesetzliche Umsetzung der Grundversorgungsvereinbarung, BGBl I Nr. 80/2004, noch nicht erfolgt ist, wurde sowohl bei den besonderen Rechtsgrundlagen für die gemeldete Datenanwendung als auch bei der Frage der Rechtsgrundlage für das gesamte Informationsverbundsystem angegeben, dass die Zustimmung des Betroffenen bei Verwendung von sensiblen Daten eingeholt werde.

Die DSK hat im Registrierungsverfahren Auflagen erteilt, die gewährleisten sollen, dass die im konkreten Fall eingeholten Zustimmungserklärungen den Voraussetzungen für ihre datenschutzrechtliche Gültigkeit genügen.

Im Rahmen der Registrierung einer Meldung betreffend die Datenanwendung „Patientenindex zwischen Landeskrankenanstalten und anderen öffentlichen Krankenanstalten“, welche in Form eines Informationsverbundsystems im Sinne des § 50 DSG 2000 zum Zweck der übergeordneten Verwaltung von Patientenstammdaten und Patientenaufenthaltsdaten sowie zur Fallübersicht durchgeführt wird, wurden Auflagen erteilt, um durch geeignete Garantien Rahmenbedingungen für die Verwendung der zum Teil sensiblen Daten zu schaffen, die erwarten lassen, dass die schutzwürdigen Geheimhaltungsinteressen der Betroffenen im konkreten Fall gewahrt werden.

Die Registrierung der Meldung einer Bundespolizeidirektion betreffend “Allgemeine Protokolle zur Verwaltung der Dienststücke (Akten, Depositen etc.)“ wurde mangels Vorliegens geeigneter Rechtsgrundlagen gemäß § 20 Abs. 4 DSG 2000 abgelehnt. (Bescheid der DSK vom 1. Juli 2003, GZ K501.349-040/003-DVR/2003,)

5.8 Rechtsauskünfte

Während Rechtauskünfte früher weitestgehend ohne Dokumentation erteilt wurden, ist die Geschäftsstelle der Datenschutzkommission seit November 2002 dazu übergegangen, kompliziertere Rechtsauskünfte zu dokumentieren. In den Jahren 2003 und 2004 wurden bereits an die hundert Fälle von solchen Rechtsauskünften dokumentiert. Darüber hinaus gibt es eine große Anzahl von Rechtsauskünften per Telefon oder E-Mail, die Standardanfragen sind, für die kein Nachweis erforderlich ist, weshalb sie nicht formell erfasst wurden. Dabei handelte es sich hauptsächlich um Informationen zu Rechtsquellen, Anleitungen für Anträge und Hinweise allgemeiner Art. Ihre Anzahl kann auf etwa 6-10 pro Arbeitstag geschätzt werden.

Die Anfragen kommen nicht nur von Betroffenen selbst, sondern auch von Rechtsanwälten, Behördenvertretern und Unternehmern. Die unmittelbare Wirkung einer Rechtsauskunft ist schwer zu bewerten, aber der Datenschutzkommission sind genügend Fälle bekannt, in denen eine kurze Rückfrage in der Geschäftsstelle der Datenschutzkommission schwerwiegende Probleme hätte vermeiden können.

6. Das Datenverarbeitungsregister

Das Datenverarbeitungsregister (DVR) in der derzeitigen Form ist gemäß § 16 Abs. 1 DSG 2000 mit Wirksamkeit vom 1. Jänner 2000 Teil der Datenschutzkommission mit dem besonderen Zweck der Führung eines Registers gemeldeter Datenanwendungen und der Prüfung der Rechtmäßigkeit der Meldungen von Datenanwendungen vor ihrer Registrierung. Der Teil des Geschäftsapparats der Datenschutzkommission, der das Datenverarbeitungsregister betreut, ist als Referat im Rahmen der Geschäftsstelle der Datenschutzkommission eingerichtet. Die Bediensteten der Datenverarbeitungsregisters sind als Teil der Geschäftsstelle der DSK gemäß § 37 Abs. 2 DSG 2000 in Anerkennung der Unabhängigkeit der Datenschutzkommission fachlich nur an die Weisungen des Vorsitzenden und des geschäftsführenden Mitglieds der Datenschutzkommission gebunden.

Im Referat „Datenverarbeitungsregister“ werden die Registrierungsverfahren durchgeführt und auch die das Registrierungsverfahren betreffenden Bescheide der Kommissionsorgane vorbereitet.

Gemäß § 2 Abs. 3 DVRV 2002 besteht das Register der Datenverarbeitungen aus:

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

6.1 Allgemeine Bemerkungen

Das vom Österreichischen Statistischen Zentralamt für das Datenverarbeitungs-register im Jahre 1986 geschaffene EDV-Programm („Applikation HOST“) steht für Abfragen aus dem Register hinsichtlich jener Eintragungen, die bis Ende 2001 vorgenommen wurden, nach wie vor zur Verfügung. Mit dem Suchkriterium „DVR-Nummer“ oder „Bezeichnung des Auftraggebers“ können nur eingeschränkte Informationen abgefragt werden. Der Inhalt dieser registrierten Meldungen liegt in Papierform vor. Derzeit befinden sich im Register ca. 70.000 aufrecht registrierte Auftraggeber, deren Meldungen in Papierform vorhanden sind. Der Umfang der bei den Auftraggebern registrierten Datenanwendungen ist unterschiedlich. Insbesondere im öffentlichen Bereich sind bei einzelnen Auftraggebern über hundert Datenanwendungen registriert. Meldungen, die seit Jänner 2002 erstattet wurden,

werden mittels des im Bundeskanzleramt eingeführten „ELAK“ („elektronischer Akt“) bzw. „EiB“ („ELAK im Bund“) verwaltet.

Umfassende Daten vom 1. Jänner 2002 bis zum Ende des Berichtszeitraumes können seitens des DVR nicht zur Verfügung gestellt werden, da die Daten, die den seinerzeitigen Tätigkeitsberichten zu Grunde lagen, zum größten Teil von der Statistik Austria über die HOST-Applikation ausgewertet wurden, die hiefür nicht mehr verwendet werden kann. Im „ELAK“ wurden ca. 34.500 Protokollzahlen vergeben, diese lassen aber keine verlässlichen Aussagen dahingehend zu, welche bzw. wie viele Meldungen nach dem 1. Jänner 2002 eingelangt sind, da diese Zahlen nicht nach Meldungen, sondern nur nach Geschäftsfällen vergeben werden konnten.

	1. Jänner 2002 bis 31. Dezember 2003	1. Jänner 2004 bis Juni 2005	1. Jänner 2002 bis Juni 2005 Gesamtzahlen
Protokollzahlen im ELAK (einschließlich rückerfasster Meldungen)	23.600	10.900	34.500
Erst- und Folgemeldungen betreffend Auftraggeber (nicht Anzahl der Datenanwendungen)	4.464	2.915	7.379
Neue DVR-Nummern	2.361	1.639	4.000
Erledigungen Insgesamt	6.900	6.600	13.500
davon Verbesserungsaufträge	1.050	1.756	2.806
Registrierungsnachweise	2.200	2.200	4.400
Parteiengehör	150	60	210
Büro- und Berichterstatterentwürfe für Auflagenbescheide	750	80	830
Einstellungen	860	335	1.195
Sonstige Erledigungen (E-Mail-Beantwortungen, Auskünfte aus dem Register, Frist-verlängerungen u dgl.)	2000	2.000	4.000

6.2 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. Auch sind Auftraggeber oftmals nicht in der Lage, selber zu beurteilen, ob die von ihnen durchgeführten Datenanwendungen den Standardanwendungen entsprechen und wenden sich daher zur Klärung dieser Fragen an die MitarbeiterInnen des Registers, was den Aufwandseinsparungseffekt der Standardanwendungen wieder verringert. Weiters zeigt die Praxis, dass die Führung einer DVR-Nummer sowohl aus der Sicht der Auftraggeber als auch aus Sicht der Betroffenen oft als ein „Qualitätssiegel“ betrachtet wird. Besitzt ein Auftraggeber nun keine DVR-Nummer, weil er ausschließlich Standardanwendungen vornimmt, wenden sich des Öfteren Betroffene an das Register und unterstellen einem solchen Auftraggeber die Verletzung seiner datenschutzrechtlichen Pflichten. Es bedarf in diesen Fällen jeweils der Aufklärung über die neue Rechtslage. Dies zeigt, dass über die Verleihung eines Gütesiegels anderer Art nachgedacht werden sollte.

Von den meisten Auftraggebern wird freilich das Entfallen der Meldepflicht bei Standardanwendungen äußerst positiv beurteilt, da damit eine erhebliche Verringerung des Verwaltungsaufwandes erzielt wurde.

Am 1. August 2004 ist die Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004) in Kraft getreten. Der Entwurf dieser Verordnung wurde im Datenverarbeitungsregister ausgearbeitet.

Die in Anlage 1 enthaltenen Datenanwendungen (siehe nachstehende Auflistung) gelten als nicht meldepflichtige Standardanwendungen im Sinne des § 17 Abs. 2 Z 6 DSG 2000:

SA001	Rechnungswesen und Logistik
SA002	Personalverwaltung für privatrechtliche Dienstverhältnisse
SA003	Mitgliederverwaltung
SA004	Abgabenverwaltung der Gemeinden und Gemeindeverbände
SA005	Haushaltsführung der Gebietskörperschaften und sonstigen juristischen Personen öffentlichen Rechts

SA006	Geschworenen- und Schöffenverzeichnisse
SA007	Verwaltung von Benutzerkennzeichen
SA008	Personenstandsbücher
SA009	Staatsbürgerschaftsevidenz
SA010	Melderegister
SA011	Wählerevidenz, Wählerverzeichnisse und Stimmlisten
SA012	Europa-Wählerevidenz und Wählerverzeichnisse
SA013	Personalverwaltung des Bundes und der bundesnahen Rechtsträger
SA014	Inventarverwaltung der öffentlichen Auftraggeber
SA015	Personalverwaltung der Länder, Gemeinden und Gemeindeverbände
SA016	Mitglieder- und Funktionärsdatenverwaltung der Wirtschaftskammerorganisation
SA017	Verwaltung von Entsendungsdaten der Wirtschaftskammerorganisation
SA018	Wirtschaftskammerorganisation: Betreuung von Mitgliedern, künftigen Mitgliedern und Interessenten im In- und Ausland
SA019	Präsenz- und Zivildienstbefreiungen von Mitarbeitern in Mitgliedsunternehmen der Wirtschaftskammer
SA020	Lehrstellenbörse der Wirtschaftskammer
SA021	Statistik der Wirtschaftskammerorganisation
SA022	Kundenbetreuung und Marketing für eigene Zwecke
SA023	KFZ-Zulassung durch Behörden
SA024	Patientenverwaltung und Honorarabrechnung
SA025	Evidenzen der Schüler sowie Evidenz über den Aufwand für Bildungseinrichtungen
SA026	Verrechnung ärztlicher Verschreibungen für Rechnung begünstigter Bezieher durch Apotheken
SA027	Verrechnung ärztlich verordneter Heilbehelfe und Hilfsmittel durch Gewerbetreibende
SA028	Verrechnung ärztlich verordneter Behandlungen und diagnostischer Leistungen durch freiberuflich tätige Angehörige der medizinisch technischen Dienste, klinischen Psychologen und Psychotherapeuten
SA029	Aktenverwaltung (Büroautomation)

Die in Anlage 2 enthaltenen Datenanwendungen (siehe nachstehende Auflistung) gelten als gemäß § 19 Abs. 2 DSG 2000 vereinfacht zu meldende Musteranwendungen:

MA001	Personentransport- und Hotelreservierung
MA002	Zutrittskontrollsysteme
MA003	KFZ-Zulassung durch beliehene Unternehmen
MA004	Teilnahme am Informationsverbundsystem www.fundamt.gv.at
MA005	Teilnahme am Informationsverbundsystem FundInfo.at

Datenanwendungen, die inhaltlich über die in der Standard- und Musterverordnung 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:

- 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, ohne dass eigens Bescheide erlassen werden mussten.

6.3 Informationsverbundsysteme

Mit fortschreitenden technischen Möglichkeiten, insbesondere via Internet, steigt die Zahl der Meldungen, die sich auf eine Teilnahme an einem Informationsverbundsystem beziehen. Dies betrifft sowohl den öffentlichen als auch den privaten Bereich.

Folgende Informationsverbundsysteme wurden registriert:

Betreiber	***Informationsverbundsystem***
Amt der Niederösterreichischen	Wasserdatenverbund Niederösterreich -

Betreiber	*Informationsverbundsystem*
Landesregierung	Modul Abwasserentsorgung
	Wasserdatenverbund Niederösterreich - Modul Messstellen/Hydrologie
	Wasserdatenverbund Niederösterreich - Modul Siedlungswasserwirtschaft
	Wasserdatenverbund Niederösterreich - Modul Umwelthygiene/Trinkwasser
	Wasserdatenverbund Niederösterreich - Modul Verdachtsflächen/Deponien
	Wasserdatenverbund Niederösterreich - Modul Wasserbau
	Wasserdatenverbund Niederösterreich - Modul Wasserrecht
	Wasserdatenverbund Niederösterreich - Modul Wasserversorgung
Amt der Tiroler Landesregierung	TISO Tiroler Informationssystem Sozialverwaltung
Bundesministerium für Finanzen	Register der Abgabenpflichtigen (Dokumentationsregister) der Abgabenbehörden, über die Identität der Abgabenpflichtigen und der Klassifizierung ihrer Tätigkeit
Bundesministerium für Inneres	Asylwerberinformationssystem (AIS)
	Betreuungsinformationssystem
	Evidenthaltung von ausgeschriebenen und widerrufenen Personenfahndungen
	Evidenthaltung von pass- und/oder waffenrechtlichen Informationen
	Fahndung nach Feuerwaffen, Banknoten und Dokumenten, die nach dem 1. 12. 1997 zur Fahndung ausgeschrieben wurden
	Fahndung nach sonstigen Sachen
	Kraftfahrzeug-Fahndung (KFZ-Fahndung)
	Kriminalpolizeilicher Aktenindex (KPA)
	Zentrale Fremdeninformationsdatei (FID)
	Zentrales Identitätsdokumentenregister
	Zentrales Waffenregister
Bundesministerium für Justiz	Automationsunterstützte Führung der Vollzugsverwaltung in den Justizanstalten
BrassRing LLC (USA)	Global Track - Bewerberdatenbank (American Express)
Bundesrechenzentrum IT Solutions	fundamt.gv.at

Betreiber	*Informationsverbundsystem*
GmbH	
Eli Lilly and Company (USA)	MyElvis Adreßdatenbank (Directory)
Hauptverband der Sozialversicherungsträger	SV-DB Österreichische Sozialversicherungs-Datenbank
Hypo Alpe Adria Bank AG	Hypo Risikobewertung
Kreditschutzverband von 1870 und Dataline Datenverarbeitungs GmbH	Warnliste der österreichischen Kreditinstitute zum Zweck des Gläubigerschutzes und der Risiko-minimierung durch Hinweis auf vertrags-widriges Kundenverhalten
Landeskrankenanstalten-Betriebs-gesellschaft - KABEG Management LKH Villach	Patientenindex zwischen Landeskrankenanstalten und anderen öffentlichen Krankenanstalten
Lubrizol Corporation (USA)	Lubrizol - Global Human Resources Information System
Niederösterreichische Gebietskrankenkasse - Kompetenzzentrum Kinderbetreuungsgeld	Informationsverbundsystem Kinderbetreuungsgeld
Österreichische Kardiologische Gesellschaft	Herzschrittmacher-Register
Reed Messe Salzburg GmbH	Ausstellerdatenbank PRISM
	Besucherdatenbank
Siemens AG (CP RS) (Deutschland)	International Development Database ("IDD")
	Mr. Ted (Bearbeitung von Bewerbungen)
Verband der Versicherungsunternehmen Österreichs	Kraftfahrzeug-Zulassungsevidenz

Wie bereits unter Pkt. 5.7. erwähnt, erstattete die Datenschutzkommission aufgrund eines durchgeführten Prüfverfahrens die Empfehlung, das von der überwiegenden Zahl der österreichischen Kreditinstitute gemeinsam betriebene Informations-verbundsystem, in dem vertragsverletzende Kunden evident gehalten werden, zu

registrieren. Dementsprechend haben ca. 770 Kreditinstitute als teilnehmende Auftraggeber an diesem Informationsverbundsystem eine entsprechende Meldung zum Zweck der Registrierung im Datenverarbeitungsregister eingebracht.

Für das im Bereich der Sicherheitspolizeiverwaltung auf Grundlage des § 57 SPG eingerichtete elektronische Informationssystem „EKIS“, das aus den oben angeführten einzelnen Informationsverbund-Datenanwendungen besteht, ist Folgendes festzuhalten: Das EKIS wird vom Bundesministerium für Inneres zur Unterstützung der kriminalpolizeilichen Arbeit der österreichischen Sicherheitsbehörden geführt. Nach Auffassung der Datenschutzkommission kann insbesondere bei Datenanwendungen, deren Inhalt bereits in einem Gesetz determiniert ist, keine Ausnahme von der Registrierungspflicht aus dem Grund der Geheimhaltung geltend gemacht werden. Dementsprechend wurde dem Bundesministerium für Inneres (als Betreiber des Informationsverbundsystems „EKIS“) seinerzeit empfohlen, die im EKIS enthaltenen Dateien nach der neuen Rechtslage zu überprüfen und die notwendigen Meldungen unverzüglich nachzuholen. Seitens der Teilnehmer am Informationsverbundsystem „EKIS“ wurde der Empfehlung der Datenschutzkommission nachgekommen und die entsprechenden Meldungen zum Zweck der Registrierung im Datenverarbeitungsregister erstattet.

Das Informationsverbundsystem „Kinderbetreuungsgeld“ wurde zum Zweck der Administration der finanziellen Abwicklung des Kinderbetreuungsgeldes (Kinderbetreuungsgeldgesetz, BGBl I Nr. 103/2001 idgF) sowie des Zuschusses zu dieser Leistung und der Koordinierung der Krankenversicherungsträger eingerichtet und dem Datenverarbeitungsregister gemeldet. Betreiber dieses Informationsverbundsystems ist die Niederösterreichische Gebietskrankenkasse als Kompetenzzentrum. Teilnehmende Auftraggeber sind die zuständigen Krankenversicherungsträger. Als allfällige Übermittlungsempfänger aus dieser Datenanwendung sind Krankenfürsorgeanstalten, Abgabenbehörden, Gerichte, Jugendwohlfahrtsbehörden und Sozialversicherungsträger in anderen Mitgliedstaaten der EU ausgewiesen. Das Informationsverbundsystem „Betreuungsinformationssystem“ dient der administrativen Unterstützung der teilnehmenden Auftraggeber im Zusammenhang mit der Gewährleistung der vorübergehenden Grundversorgung für hilfs- und schutzbedürftige Fremde in Österreich (entsprechend der Grundversorgungsvereinbarung gemäß Art. 15a B-VG).

Teilnehmende Auftraggeber am „Betreuungsinformationssystem“ sind die Organe der Vertragspartner der Grundversorgungsvereinbarung gemäß Art. 15a B-VG. Andere Einrichtungen, wie beispielsweise Betreuungseinrichtungen der Vertragspartner der Grundversorgungsvereinbarung (z.B.: humanitäre, kirchliche oder private Einrichtungen oder Institutionen der freien Wohlfahrtspflege) sind ausschließlich als Übermittlungsempfänger angeführt.

Im Informationsverbundsystem „Register der Abgabenpflichtigen (Dokumentationsregister) der Abgabenbehörden, über die Identität der Abgabenpflichtigen und der Klassifizierung ihrer Tätigkeit“ sind primär Stammdaten der Abgabepflichtigen enthalten. Diese Stammdaten werden von den Abgabenbehörden für andere Datenanwendungen, die sie in ihrem Wirkungsbereich durchführen, weiterverwendet.

6.4 Manuelle Dateien

Aufgrund der Übergangsbestimmung § 61 Abs. 5 DSG 2000, sind manuelle Datenanwendungen, die gemäß § 58 der Meldepflicht unterliegen, soweit sie schon im Zeitpunkt des Inkrafttretens des DSG 2000 bestanden haben, dem Datenverarbeitungsregister bis spätestens 1. Jänner 2003 zu melden.

Solche Datenanwendungen wurden insbesondere von den Bundespolizeidirektionen, Bezirksverwaltungsbehörden und Gendarmeriekommanden gemeldet.

6.5 Richtigstellung des Registers

Um das Register auf einem möglichst aktuellen Stand halten zu können, ist gemäß § 22 DSG 2000 eine fortgesetzte Richtigstellung des Datenverarbeitungsregisters erforderlich. In diesem Berichtszeitraum wurden die Richtigstellungen mangels freier Personalressourcen vernachlässigt.

6.6 Registrierung wegen Fristablaufs

Gemäß § 21 Abs. 2 DSG 2000 ist eine Meldung in das Datenverarbeitungsregister einzutragen, wenn zwei Monate nach Einlangen der Meldung bei der Datenschutzkommission verstrichen sind, ohne dass ein Verbesserungsauftrag gemäß § 20 Abs. 1 DSG 2000 erteilt wurde. Im Berichtzeitraum mussten wegen zu knapper Personalressourcen ca. 60 Meldungen wegen Fristablauf registriert werden. Kommt es hiedurch zu einer Registrierung von Verarbeitungen, deren Rechtmäßigkeit

zweifelhaft erscheint, kann gemäß § 20 Abs. 4 DSG 2000 ein Verfahren zur Feststellung des für die Erfüllung der Meldepflicht erheblichen Sachverhaltes von der Datenschutzkommission eingeleitet werden. Das Datenverarbeitungsregister ist in der Folge entsprechend dem Ergebnis des Verfahrens zu berichtigen.

6.7 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 und soweit nicht überwiegende schutzwürdige Geheimhaltungsinteressen des Auftraggebers oder eines Dritten vorliegen.

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

6.8 Weitere Vorhaben

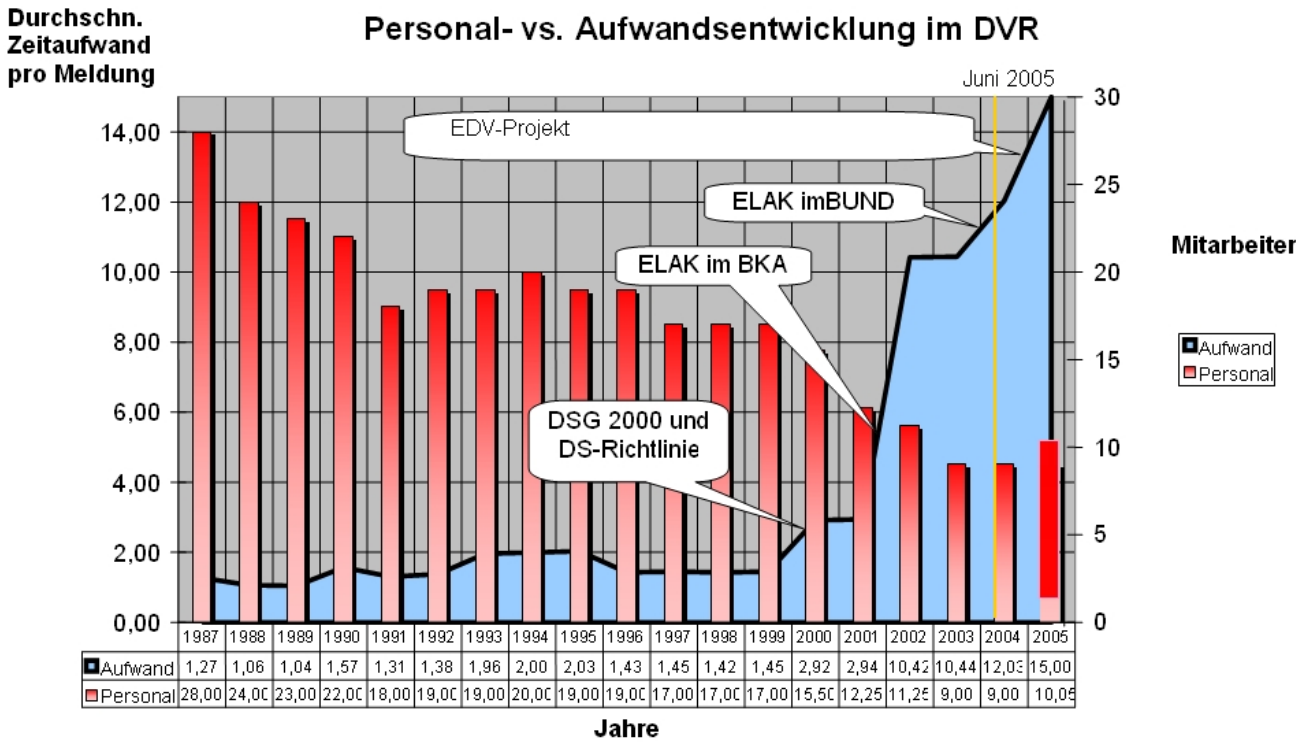
6.8.1. Ausarbeitung von neuen und Aktualisierung von vorhandenen Ausfüllmustern für Auftraggeber bestimmter Berufsgruppen

Als Serviceleistung für meldepflichtige Auftraggeber, die gleichartige Datenanwendungen vornehmen (z.B. freiberuflich tätige Angehörige der medizinisch technischen Dienste, Rechtsanwälte, Notare, Unternehmensberater, Vermögensberater, Versicherungsvermittler, u.a.), wurden bereits in der Vergangenheit Ausfüllmuster ausgearbeitet und auf Wunsch für die Meldungen gemäß DSG 2000 zur Verfügung gestellt. Diese Vorgangsweise wurde seitens der Meldepflichtigen begrüßt und hat sich auch für die Mitarbeiter des Datenverarbeitungsregisters als sehr praktikabel erwiesen. In Zukunft sollen in Zusammenarbeit z.B. mit beruflichen Interessensvertretungen weitere Muster erstellt und den Auftraggebern in der neuen Datenbank als Serviceleistung angeboten werden.

6.8.2 Projekt „DVR goes eGovernment“

Wie bereits unter Pkt. 3.2.2 erwähnt, ist der durchschnittliche Bearbeitungsaufwand pro Meldung in letzter Zeit aufgrund immer komplexer werdender Datenanwendungen kontinuierlich gestiegen und der Personalaufwand gekürzt worden. Aus diesem Grunde wurde nach einer IST-Standerhebung im Zuge einer Prüfung durch die Innenrevision des BKA ein Projekt für ein neues Datenbanksystem konzipiert und ein Maßnahmenpaket gegen die steigende Arbeitsbelastung ausgearbeitet.

Mit der nachstehenden Tabelle soll die Personal- und Aufwandsentwicklung im DVR veranschaulicht werden:



	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005
Aufwand	1,27	1,06	1,04	1,57	1,31	1,38	1,96	2,00	2,03	1,43	1,45	1,42	1,45	2,92	2,94	10,42	10,44	12,03	15,00
Personal	28,00	24,00	23,00	22,00	18,00	19,00	19,00	20,00	19,00	19,00	17,00	17,00	17,00	15,50	12,25	11,25	9,00	9,00	10,05

Ziel dieses Projektes ist einerseits die Reduzierung des Arbeitsaufwandes im Datenverarbeitungsregister durch Schaffung eines elektronischen Registrierungssystems, das in der Lage ist, die Daten der Meldung, die auf elektronischem Wege erfolgt, automatisiert in das System zu übernehmen (E-Government-Anwendung). Weiters soll als Endprodukt des Registrierungssystems eine im Internet einsichtsfähige Datenbank der registrierten Meldungen entstehen.

Das Datenverarbeitungsregister soll in der Endausbaustufe eine der großen Anwendungen des österreichischen E-Government-Konzepts werden: Die Auftraggeber können sich mit Hilfe ihrer Bürgerkarte gegenüber dem System identifizieren und authentifizieren und jederzeit elektronisch Meldungen erstatten oder abgegebene Meldungen einsehen und modifizieren. Von den üblicherweise unterschiedenen fünf Interaktionsstufen (Stufe 0 bis 4) für Geschäftsprozesse in der öffentlichen Verwaltung in Verbindung mit e-Government soll das DVR in der Stufe 4 arbeiten (Österreich befindet sich in der Mehrzahl seiner Verwaltungsprozesse bei Stufe 3).

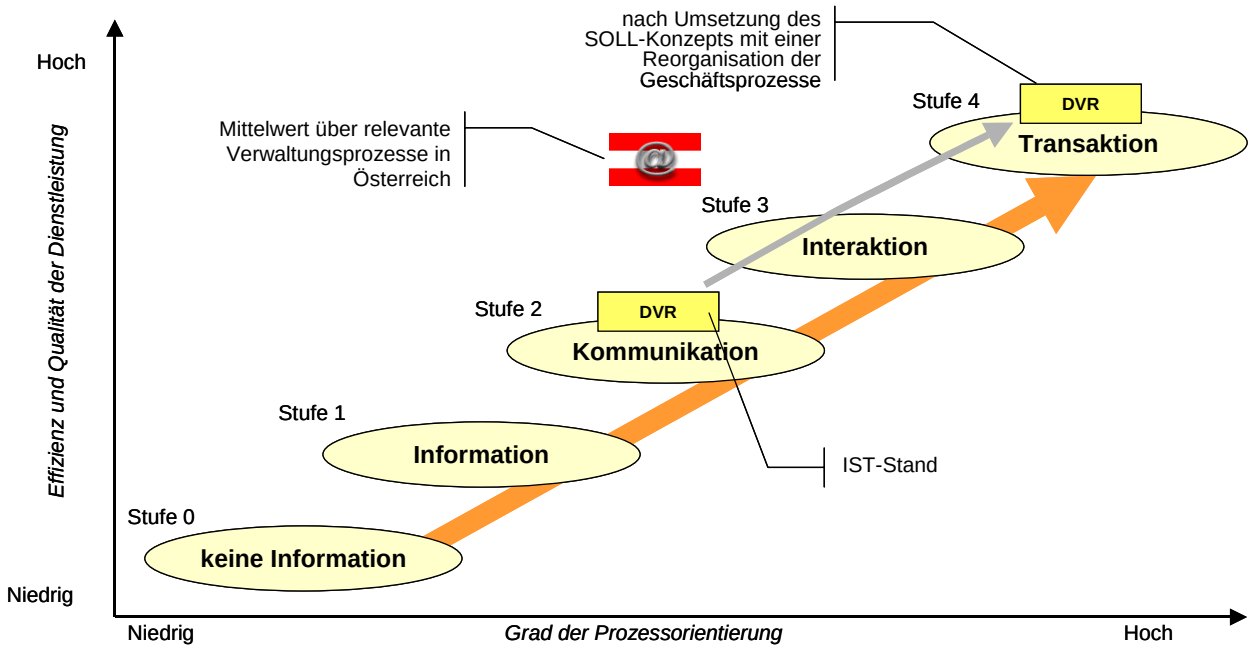


Abbildung: Entwicklung zum prozessorientierten E-Government

Das Datenverarbeitungsregister bietet bereits seit 2000 Formulare im Format Microsoft Word für Windows und Portable Document Format (PDF) im Internet an. Die Meldungen können – und sollen – elektronisch eingebracht werden. Das neue Melde- und Registrierungssystem wird elektronisch signierbare Web-Formulare für die Meldung anbieten. Das DVR eignet sich besonders gut für die e-government taugliche Kommunikation mit den meldepflichtigen Auftraggebern, da diese „per definitionem“ über EDV verfügen (Es gibt zwar auch meldepflichtige manuelle Dateien, aber die große Masse der Meldepflichtigen verarbeitet Daten elektronisch). Die große Mehrheit der Meldungsleger verfügt auch über einen Internetanschluss und ist die elektronische Abwicklung der Kommunikation mit dem DVR auch bereits gewöhnt. Schließlich kann grundsätzlich erwartet werden, dass die Meldepflichtigen nach dem Datenschutzgesetz an elektronischen Methoden des Behördenverkehrs in besonderem Maße interessiert sind.

7. Internationale Zusammenarbeit der Datenschutzkommission mit anderen Kontrollstellen

7.1 Artikel 29-Datenschutzgruppe

Auf der Grundlage des Art. 29 der EG-Richtlinie 95/46/EG wurde die so genannte „Art. 29-Arbeitsgruppe“ eingerichtet. Dieses Beratungsgremium soll gegenüber der

Europäischen Kommission zu Fragen des Datenschutzes Gutachten erstatten, die einheitliche Anwendung der allgemeinen Grundsätze der Datenschutzrichtlinie 95/46/EG fördern und Empfehlungen zum Datenschutz in der europäischen Union abgeben. Die Art. 29-Gruppe nimmt auch zum Schutzniveau in der Gemeinschaft und in Drittländern gegenüber der EU-Kommission Stellung.

Die Gruppe hat inzwischen eine Reihe von Empfehlungen beschlossen, die auf ihrer Website[13] publiziert wurden.

Von den Themen, die die Art. 29-Datenschutzgruppe im Berichtszeitrum behandelt hat, sind vor allem Folgende zu nennen:

- Die Übermittlung von Passagierdaten an die amerikanischen Sicherheitsbehörden;
- Videoüberwachung;
- Internationaler Datenverkehr und
- biometrische Methoden der Identifizierung (Fingerabdrücke, Iriserkennung, usw.).

7.1.1 Passenger Name Records

Im Jahr 2002 verlangte das US Department for Homeland Security von europäischen Fluglinien die Übermittlung der so genannten „Passenger Name Records“ (kurz PNR) aus den elektronischen Buchungssystemen der Fluglinien für Flüge nach oder über die USA (d.h. mit Zwischenstopp in den USA). Mit dieser Maßnahme sollten Terroristen, wenn sie versuchten in die USA einzureisen, frühzeitig erkannt werden.

Die Wünsche der amerikanischen Behörden warfen aus Sicht der EU-Mitgliedstaaten eine Reihe von schwerwiegenden Datenschutzproblemen auf, da es sich um die – zwangsweise – Übermittlung von personenbezogenen Daten aus dem EU-Raum in ein Drittland ohne angemessenes Datenschutzniveau handelte, deren Rechtsgrundlage überdies unklar schien. In langwierigen Verhandlungen zwischen der EU-Kommission und den zuständigen US-Behörden wurden die Bedingungen für die Herstellung eines angemessenen Datenschutzniveaus auf US-Seite ausgehandelt und in der Entscheidung 2004/535/EG der Kommission der Europäischen

[13] http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_de.htm

Gemeinschaften vom 14. Mai 2004 „über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Passenger Name Records enthalten sind, welche dem United States Bureau of Customs and Border Protection übermittelt werden“ festgeschrieben. Eine Rechtsgrundlage für die Übermittlungen selbst wurde in Form eines Abkommens zwischen der Europäischen Gemeinschaft und den USA, Beschluss 2004/496/EG des Rates vom 17. Mai 2004, geschaffen.

Das Europäische Parlament hat in der Folge Klage vor dem Europäischen Gerichtshof gegen beide Rechtsinstrumente erhoben, und zwar u.a. auch wegen Verstoßes gegen die Grundrechte und den Verhältnismäßigkeitsgrundsatz.

Unabhängig vom Ausgang des Verfahrens vor dem EuGH besteht eines der großen praktischen Probleme der PNR-Übermittlungen von datenschutzrechtlicher Bedeutung in der technischen Art und Weise der Datenweitergabe, die häufig durch die Schlagworte „push“ und „pull“ gekennzeichnet werden: Während derzeit die Datenübermittlung im Wege des Direktzugriffs („pull“) der US-Behörden auf die Flugreservierungssysteme erfolgt, ist als die datenschutzrechtlich bessere Lösung darauf hinzuarbeiten, dass die PNR-Daten in Europa vorgefiltert werden und sodann nur jene Daten an die US-Behörden gesendet werden („push“), die nach den erwähnten Rechtsgrundlagen übermittelt werden dürfen. Die österr. Datenschutz-kommission hat sich in diesem Zusammenhang besonders bemüht, die guten Dienste der österr. Bundesregierung zur Schaffung einer europäischen Push-Lösung nutzbar zu machen. Diese Bemühungen sind bedauerlicherweise mangels einer Einigung zwischen der EU-Kommission, den europäischen Luftfahrtunternehmen und den EU- Mitgliedstaaten über die Finanzierung der konzipierten Push-Lösung gescheitert.

Derzeit ist das Verfahren der PNR-Übermittlung an die kanadischen Einwanderungs-behörden im Verhandlungsstadium, wobei eine Lösung angestrebt wird, die formal dem Vorgehen gegenüber den USA entspricht. Inhaltlich bestehen jedoch wesentliche Unterschiede insofern als zum einen Kanada ein Land mit ange-messenem Datenschutz ist und zum anderen das push-System für die Daten-übermittlung verpflichtend vorgesehen ist.

Auf weltweiter Ebene wird derzeit im Rahmen der ICAO (International Civil Aviation Organisation) an Richtlinien für die Übermittlung von PNR-Daten von Fluglinien an Einwanderungs- und Grenzkontrollbehörden gearbeitet.

7.2 Schengen

Die österreichische Datenschutzkommission ist Mitglied der Gemeinsamen Kontrollinstanz von Schengen, welche seit 1995 existiert und die Übereinstimmung der Verwendung der Daten im Schengener (Informations-)System mit dem Schengener Durchführungsübereinkommen überwacht.

Die Gemeinsame Kontrollinstanz von Schengen setzt sich aus Vertretern jener nationalen Behörden zusammen, die von den einzelnen Staaten als „Nationale Kontrollinstanz“ bezeichnet wurden. Für Österreich erfüllt die Datenschutz-kommission die Funktion der nationalen Kontrollinstanz im Sinne des Art. 114 Schengener Durchführungsübereinkommen von 1990 (SDÜ).

Das Bundesministerium für Inneres ist für die Führung des nationalen Teils des Schengener Informationssystems (das N.SIS) zuständig, und erteilt auch Auskünfte an Betroffene. Die Datenschutzkommission hat in Zusammenarbeit mit dem Bundesministerium für Inneres ein Formular (mit englischer Übersetzung) für die Auskunft aus dem N.SIS aufgelegt, das über das Internet abgerufen werden kann (http://www.dsk.gv.at/schengd.htm). Österreich ist das einzige Schengen-Land, das eine solche Leistung anbietet.

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.

7.3 Europol

Neben der Gemeinsamen Kontrollinstanz von Schengen besteht auch eine unabhängige Gemeinsame Kontrollinstanz für Europol, die auf Grundlage der Europol-Konvention eingerichtet und – wie die GKI Schengen - aus den nationalen Kontrollstellen zusammengesetzt ist.

Die Aufgabe der Europol-GKI besteht darin, 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 wurde ein eigener Beschwerdeausschuss eingerichtet, der für die Behandlung der Beschwerden von Betroffenen betr. die Datenverwendung durch Europol zuständig ist.

Die Gemeinsame Kontrollinstanz für Europol verfügt über eine eigene Website: http://europoljsb.ue.eu.int/ .

7.4 Zollinformationssystem (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 Informations-technologie im Zollbereich vom 26. Juli 1995 (ABl. C 316 vom 27. November 1995, S. 34) wurde ein gemeinsames Zollinformationssystem (Abkürzung: 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 Zollinformationssystem 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 folgender Maßnahmen zu ersuchen:

- Feststellung und Unterrichtung,
- verdeckte Registrierung oder

- gezielte Kontrolle.

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.

7.5 „Berliner Gruppe“

Im Bereich der Telekommunikation findet die (informelle) Meinungsabstimmung zwischen den europäischen Datenschutzbehörden regelmäßig unter der Organisationsverantwortung des Berliner Datenschutzbeauftragten statt („International Working Group on Data Protection in Telecommunications“). Unter seiner Leitung finden jährlich Herbsttagungen in Berlin statt, bei welchen der neueste Stand der Technik und der neueste Diskussionsstand in Sachen Telekommunikation und Datenschutz dargestellt werden. Besonderes Augenmerk wird in diesem Zusammenhang auch den Datenschutzproblemen des Internet gewidmet.

Im Berichtszeitraum befasste sich die so genannte „Berliner Gruppe“ mit den neuesten Entwicklungen im Internet, mit Kamerahandys, unerwünschter Direktwerbung per E-Mail („Spam“), Registrierung von Internet-Domains und zahlreichen anderen Themen.

Darüber hinaus veranstaltet der Berliner Datenschutzbeauftragte auch internationale Treffen zu Themen der Telekommunikation, die traditionell im Frühling stattfindet. Diese Treffen der Berliner Gruppe werden seit 2003 auch von Vertretern der amerikanischen Federal Trade Commission besucht, was vor allem auf dem Gebiet der Spam-Bekämpfung hoffen lässt.

7.6 Frühjahrstagung der unabhängigen Datenschutzbehörden der EU-Staaten

Seit mehreren Jahren treffen sich die Vertreter der unabhängigen Datenschutzbehörden der EU-Länder sowie sonstiger europäischer Staaten zum Gedankenaustausch bei einer Frühjahrstagung.

Bei diesen Tagungen wurden jeweils die wichtigsten anstehenden Datenschutzprobleme aus europäischer Sicht diskutiert und Beschlüsse in Form gemeinsamer Resolutionen gefasst. Bei der Frühjahrskonferenz 2002 bildete den wichtigsten Beratungsgegenstand die Erfahrungen nach den Terroranschlägen in den USA vom 11. September 2001, wobei insbesondere die unterschiedlichen Reaktionen in den Teilnehmerstaaten und ihre datenschutzrechtlichen Auswirkungen erörtert wurden. Weitere Themen waren die Auditierung und Zertifizierung von Konzepten für besseren Datenschutz und Datensicherheit und Diskussionen bezüglich Verfahren biometrischer Identifizierung. Themen der Konferenz im Jahr 2003 waren insbesondere Probleme des internationalen Datenverkehrs, Fragen bei der Umsetzung der „Telekom-Datenschutzrichtlinie“ 2002/58/EG in nationales Recht sowie Fragen im Zusammenhang mit der EU-Erweiterung.

7.7 Herbsttagungen der internationalen Datenschutzbehörden

Die jährliche Herbsttagung der internationalen Datenschutzbehörden, zu der alle akkreditierten Datenschutzbehörden der Welt eingeladen sind, haben im Jahre 2002 in Cardiff (Vereinigtes Königreich), im Jahre 2003 in Sydney (Australien) und 2004 in Breslau (Polen) stattgefunden. Auf diesen Tagungen werden die jeweils dringendsten Probleme und Tendenzen des Datenschutzes im internationalen Kontext diskutiert.

Österreich war in Cardiff durch ein Mitglied der Datenschutzkommission vertreten. Themen des ersten Teils dieser Konferenz waren unter anderem das Problem „Terrorismusbekämpfung und Datenschutz“, Verwendung biometrischer Daten, Internet und Spamming, Videoüberwachung und die Speicherung von Verkehrsdaten im Telekommunikationssektor. Hauptthema des zweiten Teils der Konferenz war das Thema „Informationszugang und Datenschutz“ (die Konferenz stand unter dem allgemeinen Motto „Das Recht auf Information im 21. Jahrhundert: Eine Demystifizierung“).

Die Konferenz in Sydney befasste sich unter anderem mit Problemen des Datenschutzes in einer globalisierten und von gegenseitiger Abhängigkeit geprägten Welt und mit der Entwicklung der Informationstechnologien und den damit verbundenen Risiken für die individuellen Rechte und Freiheiten.

Zu den Themen der Konferenz in Breslau 2004 gehörten u.a. Fragen der E-Demokratie, der biometrischen Identifizierung und des internationalen Datenexports.