Datenschutzbericht 2009

1. Juli 2007 - 31. Dezember 2009

DSK

Zusammenfassender Überblick

Wie die nachstehenden statistischen Darstellungen zeigen, ist es der Datenschutzkommission (DSK) im Berichtszeitraum gelungen, im Bereich der Erledigung von Beschwerdeverfahren und der Bürgerberatung ihre Aufgaben grundsätzlich rechtzeitig und mit der notwendigen Qualität zu erledigen: Es hat nunmehr sehr wenige Säumnisbeschwerden an den Verwaltungsgerichtshof gegeben und die bei den Höchstgerichten inhaltlich bekämpften Bescheide der Datenschutzkommission wurden nur zu einem sehr geringen Prozentsatz aufgehoben. Bei einem zeitweise ungewöhnlich hohen Anfall von Beschwerden nach § 31 DSG 2000 (förmliche Beschwerdeverfahren, die durch Bescheid zu erledigen sind), wie er sich zB im 1. Halbjahr 2008 ergeben hat, muss allerdings die Erledigung von Ombudsmann-Beschwerdeverfahren nach § 30 DSG 2000 angesichts der äußerst knappen Personalausstattung der Datenschutzkommission zurückstehen, sodass es diesbezüglich im Berichtszeitraum gelegentlich zu längerer Verfahrensdauer gekommen ist.

Die anderen Aufgaben einer Datenschutz-Kontrollstelle im Sinne des Art. 28 der RL 95/46/EG konnten mangels Personal allerdings nur mit geringer Intensität betreut werden: Insbesondere im Bereich der Vor-ort-Kontrolle von Datenanwendungen nach § 30 Abs. 2 DSG 2000 und im Bereich der europäischen Zusammenarbeit in der Art. 29 Gruppe bestehen erhebliche Defizite, die mit der derzeitigen Personalausstattung nicht behoben werden können.

Hinsichtlich des Datenverarbeitungsregisters hat im Berichtszeitraum eine weitere technische Systemänderung stattgefunden, mit der im Jänner 2009 ein einheitliches Datenbanksystem eingeführt wurde, das derzeit allerdings erst intern in Betrieb ist. Dennoch zeigen sich bereits positive Auswirkungen, da es zu Ende des Berichtszeitraums im 2. Halbjahr 2009 zum ersten Mal gelungen ist, Eingang und Erledigungen zahlenmäßig ins Gleichgewicht zu bringen. Freilich bestehen noch erhebliche Erledigungsrückstände aus den früheren Jahren. Die Aufarbeitung dieser Rückstände wird aber durch die Übergangsbestimmungen der DSG-Novelle 2010 erleichtert, da davon auszugehen ist, dass eine inhaltliche Prüfpflicht für die nicht-vorabkontrollpflichtigen Meldungen auch für die vor Inkrafttreten der DSG-Novelle 2010 eingebrachten Meldungen wegfällt, sobald die neue DVR-VO erlassen ist.

Was die Forderungen an den Gesetzgeber betrifft, die sich aus dem Inhalt von Beschwerdefällen ergeben haben, steht die Regelung des Bonitätsinformationswesens noch immer aus. Sie wäre – wie die große Anzahl von Beschwerden in diesem Bereich zeigt – dringend erforderlich. Ebenso notwendig sind Korrekturen im Bereich des Versicherungsvertragsrechts, was den Datenaustausch zwischen behandelnden Gesundheitsdienstanbietern und privaten Versicherern im Rahmen der Leistungsverrechnung betrifft. Diesbezüglich hat das hiefür zuständige Bundesministerium für Justiz jüngst einen Gesetzentwurf vorgelegt, der den Ergebnissen der eingehenden Sachverhaltsuntersuchungen der Datenschutzkommission weitgehend entspricht. Was in diesem Entwurf noch ergänzt werden sollte, wäre eine ausdrückliche gesetzliche Regelung hinsichtlich des Zentralen Informationssystems der Versicherungswirtschaft, dessen Rechtsgrundlagen nach Auffassung der Datenschutzkommission derzeit zweifelhaft erscheinen.

Zum künftigen Schicksal der Datenschutzkommission ist angesichts der Pläne zur Schaffung einer Verwaltungsgerichtsbarkeit erster Instanz und der Übertragung von Kompetenzen des Datenschutzkom-

mission an diese neuen Behörden zu sagen, dass insgesamt nur ein kleiner Teil (etwa 10 %) der Aufgaben der Datenschutzkommission überhaupt denkmöglicherweise übertragbar ist und dass daher jedenfalls eine Nachfolgeinstitution geschaffen werden müsste, falls die Datenschutzkommission aufgelöst werden sollte, wie dies der Entwurf der Verwaltungsgerichtsbarkeits-Novelle vorsieht. Art. 28 der RL 95/46/EG schreibt die Existenz einer Datenschutz-Kontrollstelle zwingend vor, sodass künftig allenfalls die Frage zu lösen sein wird, ob die Datenschutzkommission neu organisiert werden soll, aber keineswegs, ob sie tatsächlich in den neuen Verwaltungsgerichten aufgehen könnte.

1. Einleitung

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

Ihr hiermit vorgelegter dreizehnter Datenschutzbericht umfasst den Zeitraum vom 1. Juli 2007 bis 31. Dezember 2009. Es handelt sich hiebei um den zweiten Datenschutzbericht der bis zum 30. Juni 2010 im Amt befindlichen Datenschutzkommission.

Wie im letzten Datenschutzbericht müssen grundsätzliche Erwägungen zur Situation einer Datenschutz-Kontrollbehörde in Österreich, insbesondere auch im Zusammenhang mit der sog. Staatsreform[1] (vgl. Pkt. 5.3. des 12. Datenschutzberichtes) und der beabsichtigten Einführung einer zweistufigen Verwaltungsgerichtsbarkeit[2] angestellt werden; der vorliegende Bericht wird auch die im letzten Berichtszeitraum diesbezüglich gewonnenen Erfahrungen darstellen und kommentieren.

Zur besseren Erkennbarkeit von Entwicklungen nehmen die statistischen Schaubilder so wie im vorigen Bericht auch auf vorhergehende Berichtszeiträume der Datenschutzkommission Bezug.

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

[1] BGBl. I Nr. 2/2008

[2] Entwurf einer Verwaltungsgerichtsbarkeits-Novelle 2010, zur Begutachtung versendet unter Zl BKA-601.999/0001-V/1/2010

2. Die Organe der Datenschutzkommission

Als Organe der Datenschutzkommission werden das Kollegium der Mitglieder als Kollegialorgan, weiters in bestimmten Angelegenheiten der Vorsitzende und aufgrund des § 38 Abs. 1 DSG 2000 das in der Geschäftsordnung bestimmte geschäftsführende Mitglied (GfM) – jeweils allein – tätig.[3]

2.1 Zur rechtlichen Stellung der Mitglieder der Datenschutzkommission

„Die Mitglieder der Datenschutzkommission sind in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden“ (§ 37 Abs. 1 DSG 2000). Diese Bestimmung, die 2008 im Zuge der Bereinigung von außerhalb des B-VG stehenden Verfassungsbestimmungen ihres Verfassungsrangs entkleidet wurde[4], ist nunmehr vor dem Hintergrund des neuen Art. 20 Abs. 2 B-VG[5] zu sehen, der die Voraussetzungen für das Bestehen weisungsfreier Verwaltungsbehörden neu und allgemein regelt. Nähere Ausführungen zu den Konsequenzen dieser Neuregelung finden sich in Kapitel 5.

Seit 1. Juli 2000 beträgt die Zahl der Kommissionsmitglieder und Ersatzmitglieder jeweils 6 Personen, die vom Bundespräsidenten ernannt werden. Durch die Datenschutzgesetz-Novelle 2010 wurde nunmehr verbindlich festgeschrieben, dass sämtliche Mitglieder der Datenschutzkommission ihre Tätigkeit in der Datenschutzkommission nur neben ihrem Hauptberuf ausüben (vgl. § 36 Abs. 3a). Gleichzeitig wurde durch die DSG-Novelle 2010 klargestellt, dass als richterliches Mitglied sowie als geschäftsführendes Mitglied nur aktive Richter bzw. Bundesbedienstete tätig sein können und es wurde für die übrigen Mitglieder eine Altersgrenze von 65 Jahren eingeführt[6].

Der für die Ernennung der Datenschutzkommission Mitglieder durch den Bundespräsidenten notwendige Vorschlag der Bundesregierung wird erstattet hinsichtlich

des richterlichen Mitglieds und des richterlichen Ersatzmitgliedes aufgrund eines Dreiervorschlages des Präsidenten des OGH ,

zweier Mitglieder und zweier Ersatzmitglieder aufgrund eines Vorschlags der Länder

eines Mitglieds und eines Ersatzmitglieds aufgrund eines Dreiervorschlags der Bundeskammer für Arbeiter und Angestellte, sowie hinsichtlich

eines Mitglieds und eines Ersatzmitglieds aufgrund eines Dreiervorschlags der Wirtschaftskammer Österreich.

Ein Mitglied und eine Ersatzmitglied sind von der Bundesregierung aus dem Kreis der Bundesbediensteten[7] vorzuschlagen.

[3] „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).

[4] BGBl. I Nr. 2/2008

[5] BGBl. I Nr. 2/2008

[6] Vgl. § 36 Abs. 6 DSG 2000 idF der DSG-Novelle 2010

[7] Vgl. Neufassung des § 36 Abs. 3 DSG 2000 durch die DSG-Novelle 2010

2.2. Die Mitglieder der Datenschutzkommission im Berichtszeitraum

Die Zusammensetzung der Datenschutzkommission im Berichtszeitraum 1. Juli 2007 bis 31. Dezember 2009 war wie folgt:

Mitglieder:

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

Ersatzmitglieder:

- Dr. Gerhard KURAS, stv. Vorsitzender (richterliches Ersatzmitglied)
- Dr. Eva SOUHRADA-KIRCHMAYER, stv. geschäftsführendes Mitglied
- Dr. Michaela BLAHA
- Mag. Huberta MAITZ-STRASSNIG
- Dr. Klaus HEISSENBERGER
- Mag. Gerda HEILEGGER

2.3 Die Organe der Datenschutzkommission

2.3.1 Das Kollegium der Datenschutzkommission

Die Datenschutzkommission als Kollegialorgan hat die rechtliche Stellung eines Tribunals iSd EMRK: Ihre Mitglieder sind in dieser Funktion weisungsfrei, ihr Vorsitzender ist Richter. Die Datenschutzkommission war und ist allerdings keine Art. 133 Z 4 B-VG Behörde, sondern auch organisatorisch eine Behörde sui generis (vgl. die §§ 36 ff DSG 2000). Art. 20 Abs. 2 B-VG (neu) bietet eine verfassungsrechtliche Grundlage für die Weisungsfreiheit auch solcher Verwaltungsbehörden, die – im Gegensatz zu jenen gemäß Art. 133 Z 4 B-VG - erste Instanz sind (wie die Datenschutzkommission) oder die nicht als Kollegium tätig werden (wie zB das geschäftsführende Mitglied der Datenschutzkommission).

Der Datenschutzkommission als Kollegialbehörde obliegt vor allem die Beschlussfassung hinsichtlich der rechtsförmlichen Entscheidungen der Datenschutzkommission im Verfahren nach § 31 DSG 2000 sowie die Beschlussfassung in allen Angelegenheiten von richtungweisender Bedeutung (vgl. § 38 Abs. 1 DSG 2000 und die in Ausführung hiezu ergangene Geschäftsordnung der Datenschutzkommission).

2.3.2 Der Vorsitzende

Der Vorsitzende vertritt die Datenschutzkommission nach außen, soweit er dies nicht dem geschäftsführenden Mitglied übertragen hat (vgl. hiezu § 2 Abs. 1 der Geschäftsordnung).

Der Vorsitzende führt weiters den Vorsitz in den Sitzungen des Kollegiums der Datenschutzkommission; die Beschlüsse des Kollegiums werden von ihm gefertigt.

2.3.3 Das Geschäftsführende Mitglied

Das geschäftsführende Mitglied (in der Folge: GfM) führt die täglichen Geschäfte der Datenschutzkommission. Hiezu gehören nach der Geschäftsordnung der Datenschutzkommission auch die meisten Angelegenheiten, die keiner Beschlussfassung durch das Kollegium bedürfen, wie insbesondere die Erledigung von Ombudsmann-Verfahren (nicht aber zB die Erstattung von Empfehlungen) oder die Vornahme von Registrierungen im Datenverarbeitungsregister (nicht aber zB die Ablehnung einer Registrierung).

In wichtigen Fragen stellt das GfM das Einvernehmen mit dem Vorsitzenden her. Es hat weiters das Recht, das Kollegium jederzeit mit einer Angelegenheit zu befassen, ohne dass dies allerdings einen Kompetenzübergang zur Entscheidung zur Folge hätte.

2.4 Die Datenschutzkommission als Stammzahlenregisterbehörde

Aufgrund des E-Government-Gesetzes § 8 hat die Datenschutzkommission auch die Rolle der Stammzahlenregisterbehörde wahrzunehmen. Mit dieser Funktion ist vor allem die Verantwortung für die sichere und ordnungsgemäße Erzeugung und Verwendung der Stammzahlen verbunden sowie die Erlaubnis, bereichsspezifische Personenkennzeichen zu verwenden (vergleiche hierzu Näheres im Kapitel 9).

Die Vollziehung des E-Government-Gesetzes fällt, sofern nicht ausnahmsweise mit Bescheid vorzugehen wäre, in die Zuständigkeit des GfM.

3. Der Geschäftsapparat der Datenschutzkommission

3.1 Aufgaben und Organisation der Geschäftsstelle

Die Geschäftsstelle unterstützt die Datenschutzkommission in allen Angelegenheiten der Datenschutzkommission, einschließlich ihrer Aufgaben als Stammzahlenregisterbehörde. Seit Mitte 2006 besitzt die Geschäftsstelle auch zwei Referate, nämlich das Büro der Datenschutzkommission, das für die vorbereitende Behandlung der Beschwerdefälle zuständig ist, und das Datenverarbeitungsregister (DVR).

Gemäß § 38 Abs. 2 DSG 2000 hat der Bundeskanzler die notwendige Sach- und Personalausstattung für die Geschäftsführung der Datenschutzkommission zur Verfügung zu stellen. Dies gilt auch für das Datenverarbeitungsregister, dessen technische Aufrüstung Voraussetzung für das Inkrafttreten der neuen Bestimmungen in der DSG-Novelle 2010 über die online-Registrierung ist.

Hinsichtlich des zur Verfügung gestellten Personals bestimmt § 37 Abs. 2 DSG 2000, dass der Bundeskanzler die Dienstaufsicht führt. Den Organen der Datenschutzkommission kommt nur die Fachaufsicht über die Bediensteten des Geschäftsapparats zu. (Zur Frage, inwiefern dieses Organisationsmodell, das aus 1980 stammt, dem heutigen europäischen Standard entspricht, vgl. Abschnitt 5).

Derzeit ist die der Datenschutzkommission zur Unterstützung in der Geschäftsführung beigegebene Geschäftsstelle organisatorisch als Abteilung im Verfassungsdienst des Bundeskanzleramtes eingerichtet.

3.2 Der Personalstand der Geschäftsstelle

Derzeit verfügt die Geschäftsstelle über insgesamt 20 Planstellen auf Vollbeschäftigungsäquivalent-Basis (19 Planstellen + 1 Behinderten-Planstelle) mit folgender Wertigkeit;

- 11 A/a Planstellen (einschließlich einer Behinderten-Planstelle),
- 2 B/b Planstellen,
- 6 C/c Planstellen und
- 1 d Planstelle.

Davon entfallen 11,5 Planstellen auf das Datenverarbeitungsregister und 8,5 Planstellen auf den restlichen Teil der Geschäftsstelle.

Es hat sich somit an der Gesamtzahl der Planstellen gegenüber dem vorigen Berichtszeitraum nichts geändert, wohl aber ist es gelungen, die Wertigkeit des Personals im Datenverarbeitungsregister entsprechend den steigenden fachlichen Anforderungen zugunsten von juristisch ausgebildetem Personal zu erhöhen.

Kritisch bemerkt werden muss jedoch, dass das Datenverarbeitungsregister nach wie vor 60 % der gesamten Personalressourcen der Geschäftsstelle verschlingt, was angesichts des von der Geschäftsstelle zu besorgenden Aufgabenbündels nicht angemessen ist. Theoretisch sollte daher nach Umsetzung des neuen Registrierungsverfahrens gemäß der DSG-Novelle 2010 eine Personalumschichtung zugunsten anderer Tätigkeiten des Geschäftsapparats erfolgen können – freilich steht zu befürchten, dass tatsächlich auch nach Einschränkung der inhaltlichen Prüfung von Meldungen an das Datenverarbeitungsregister auf vorabkontrollpflichtige Datenanwendungen das derzeit im DVR verwendete Personal gerade ausreicht, um den Arbeitsanfall im DVR zeitgerecht zu erledigen und Rückstände – die derzeit erheblich sind – zu vermeiden.

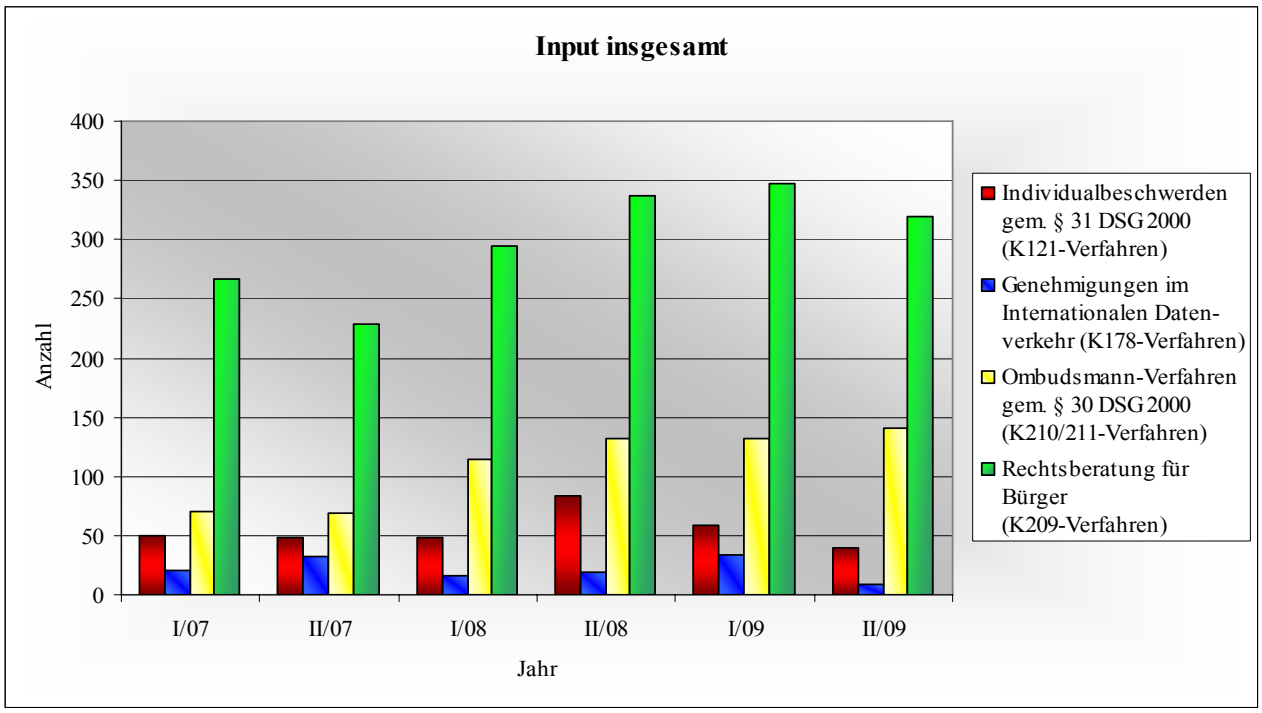
Es wird nochmals darauf hingewiesen, dass von dem 1999 im Vorblatt zur Regierungsvorlage zum DSG 2000 unter „Kos-

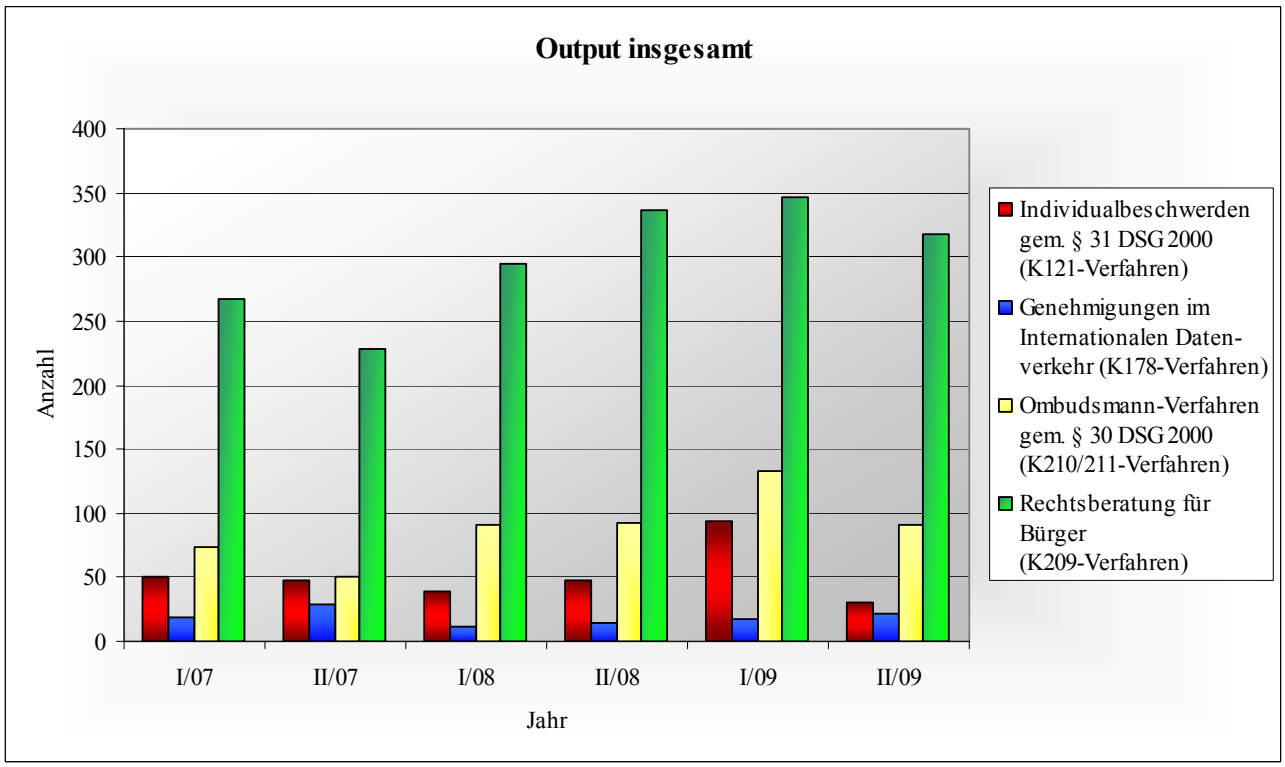
ten“ ausgewiesenen zusätzlichen Bedarf von 4 Planstellen tatsächlich nur 2 Planstellen zugeteilt wurden. Von dem im Vorblatt zur Regierungsvorlage zum E-GovG für das Stammzahlenregister veranschlagten Personalbedarf von 2 Planstellen steht nur eine zur Verfügung. Für die durch die DSG-Novelle 2010 im Bereich der Videoüberwachung entstandenen neuen Aufgaben für die Datenschutzkommission (zB Schlüsselverwaltung) wurde überhaupt kein zusätzliches Personal in Rechnung gestellt. Sollte im Zusammenhang mit der Einführung der Vorratsdatenspeicherung die Datenschutzkommission mit den für das Gesamtkonzept der Vorratsdatenspeicherung so wichtigen Kontrolle der Datenverwendung bei den Betreibern betraut werden, wird dafür jedenfalls zusätzliches Personal zu veranschlagen sein, auch wenn in den im Begutachtungsverfahren versendeten Erläuterungen jede Bezugnahme auf dieses Problem fehlt.

An dem Umstand, dass die österreichische Datenschutzkommission im europäischen Vergleich hinsichtlich ihrer Personalausstattung extrem unterdotiert ist, hat sich im Berichtszeitraum somit nichts geändert.

4. Geschäftsgang

4.1 Statistische Darstellung des Geschäftsganges (Gesamtüber-sicht)





Im Folgenden wird die Tätigkeit der Datenschutzkommission, soweit sie in „Verfahren“ (im weitesten Sinn) gegliedert werden kann, statistisch dargestellt. Davon ausgenommen sind naturgemäß – ebenfalls sehr arbeitsintensiven – Bereiche wie etwa die europäische und internationale Zusammenarbeit in der Art. 29 Gruppe oder die Öffentlichkeitsarbeit der Datenschutzkommission.

Die wichtigsten Geschäftsfallstypen aufgrund von Beschwerden/Eingaben/Anträgen von Parteien.

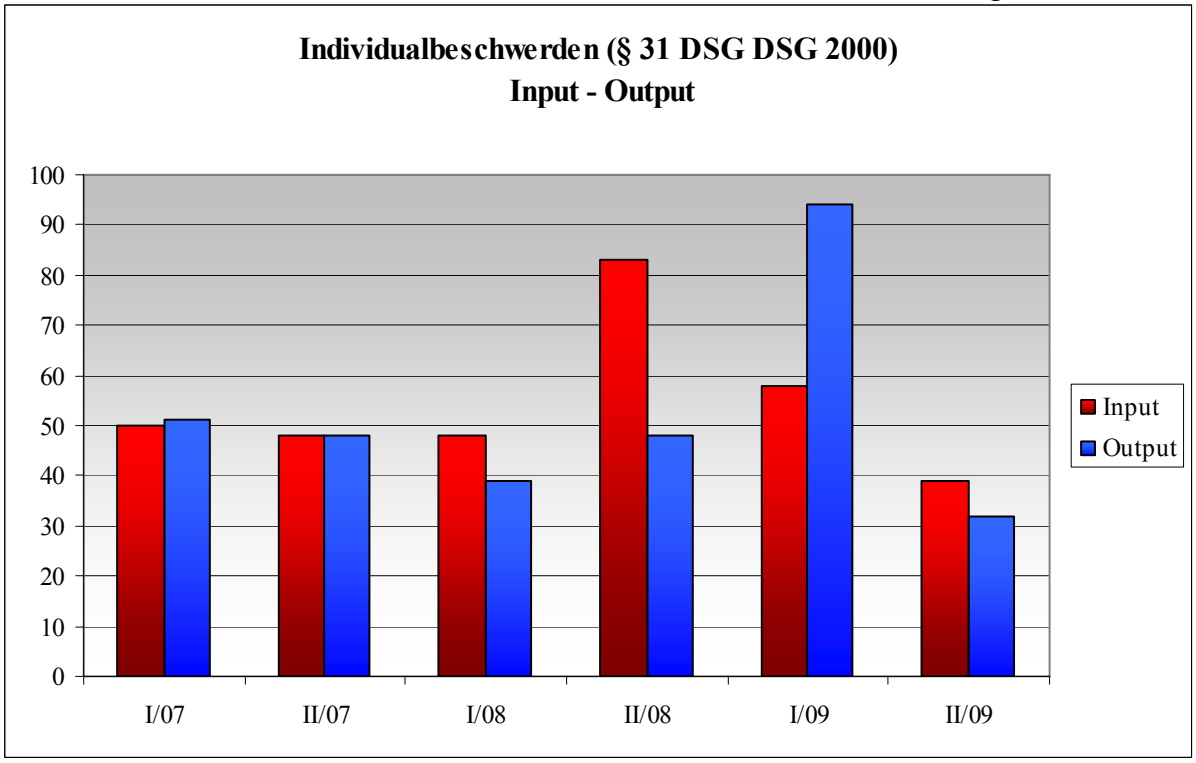
	Eingangsstücke					Erledigungen				
	2. Halbjahr 2007	1. Halbjahr 2008	2. Halbjahr 2008	1. Halbjahr 2009	2. Halbjahr 2009	2. Halbjahr 2007	1. Halbjahr 2008	2. Halbjahr 2008	1. Halbjahr 2009	2. Halbjahr 2009
Individualbeschwerden (K120 und K121-Verfahren)	48	48	83	58	39	48	39	48	94	32
Ombudsmannverfahren nach § 30 DSG 2000 (K210 + K211[2])	69	115	132	132	169	51	85	107	124	142
Rechtsauskünfte (K209)	231	297	330	346	318	231	297	330	346	318
Genehmigungen nach § 46 und 47 DSG 2000 (K202)	5	9	5	7	9	6	4	7	7	6
Genehmigungen im Internationalen Datenverkehr (K178)	32	16	19	34	12	29	12	15	17	38
Auflagenbescheide der Datenschutzkommission in Registrierungsverfahren (K503 und K600)	716 Fälle in der Zeit vom 01.07.07 bis 31.12.09					564 Fälle in der Zeit vom 01.07.07 bis 31.12.09 (davon 526 Bescheide über Teilnahme an der KKE)				
Registrierungsverfahren Im Datenverarbeitungsregister		3905	5932	3500	3599		2750	2749	2082	3465

4.2 Die Verfahren vor der Datenschutzkommission

4.2.1 Individualbeschwerdeverfahren (§ 31 DSG 2000)

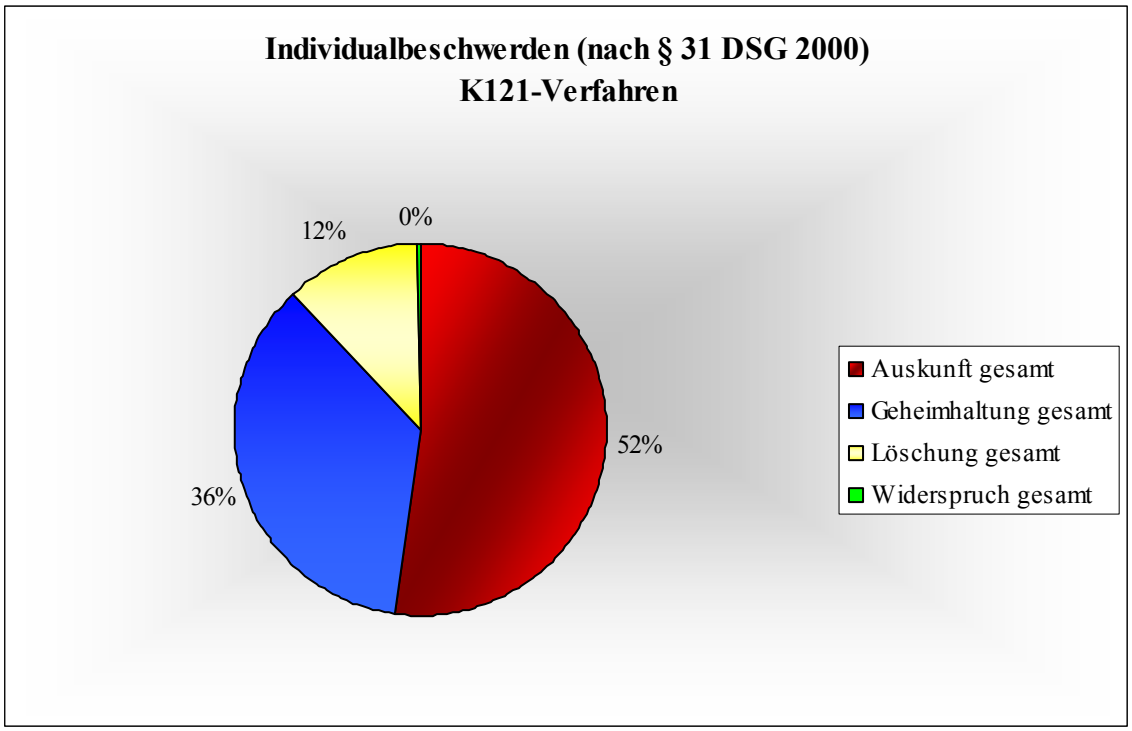
Gemäß § 31 DSG 2000 kann vor der Datenschutzkommission Beschwerde mit verbindlicher Wirkung der Entscheidung in Auskunftssachen (im privaten und öffentlichen Bereich) sowie in Geheimhaltungs-, Richtigstellungs- und Löschungssachen (nur hinsichtlich des öffentlichen Bereichs) erhoben werden.

Graphische Übersicht des Arbeitsanfalls:



Die Graphik zeigt deutlich, dass im zweiten Halbjahr 2008 plötzlich deutlich mehr Beschwerden bei der Datenschutzkommission eingegangen sind. Dies musste im nächsten Halbjahr angesichts der Erledigungsfrist nach § 73 AVG durch eine entsprechende Erhöhung des Outputs abgefangen werden, was auch tatsächlich gelungen ist. Freilich konnte diese Output-Steigerung bei den Verfahren nach § 31 DSG 2000 nur dadurch erzielt werden, dass die Behandlung von Beschwerdeverfahren nach § 30 DSG, die ja keiner gesetzlichen Erledigungsfrist unterliegen, z.T. zurückgestellt wurde.

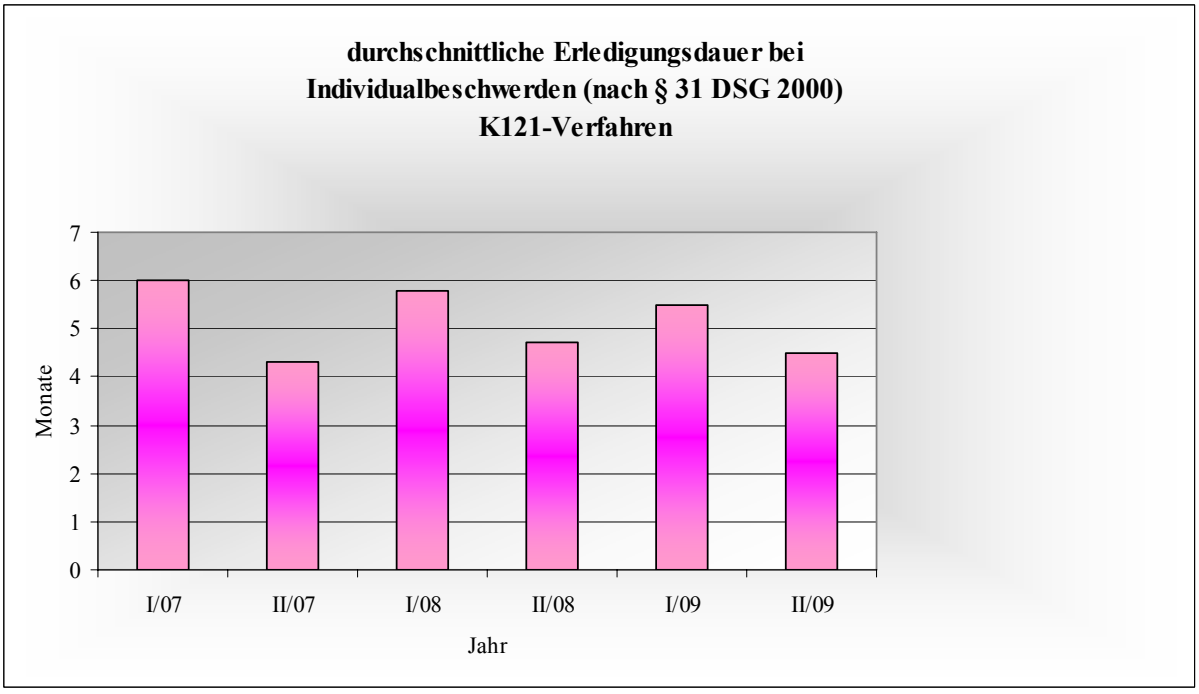
Wenn die Volksanwaltschaft – wie gegenüber der Datenschutzkommission angekündigt – die überlange Erledigungsdauer eines Verfahrens nach § 30 DSG 2000 in ihrem Bericht rügend erwähnen sollte, so ist hiezu Folgendes anzumerken: Die absolute Prioritätensetzung zugunsten der Behandlung von Beschwerden nach § 31 DSG 2000 ist deshalb erforderlich, weil nach der jüngsten Judikatur der Zivilgerichte im Falle von Säumnisbeschwerden an den Verwaltungsgerichtshof neben der Säumnis auch Amtshaftung geltend gemacht werden kann – mangelnde Personalausstattung kann demgegenüber nicht erfolgreich ins Treffen geführt werden.



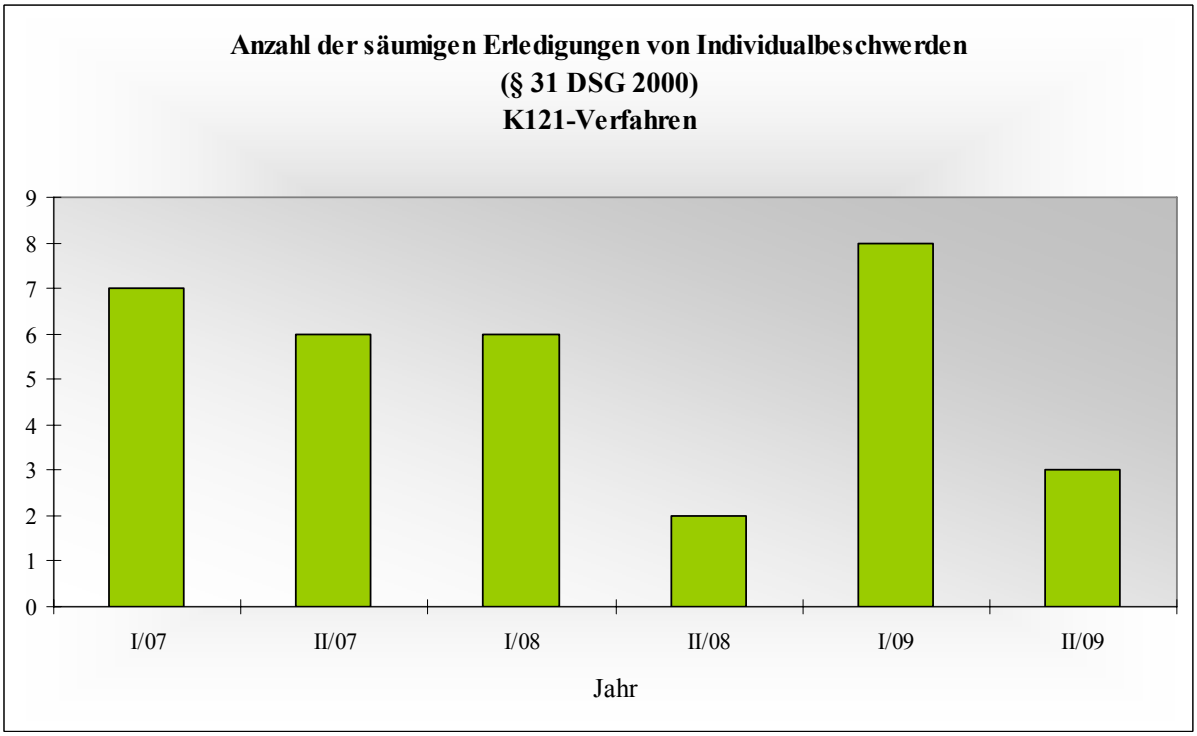
Die Individualbeschwerden nach § 31 DSG 2000 betreffen zu 52 % Auskunftsbeschwerdeverfahren, wovon der weit überwiegende Teil Auftraggeber des privaten Bereichs betrifft.

Graphische Übersichten über die Erledigungsdauer von Beschwerden nach § 31 DSG 2000:

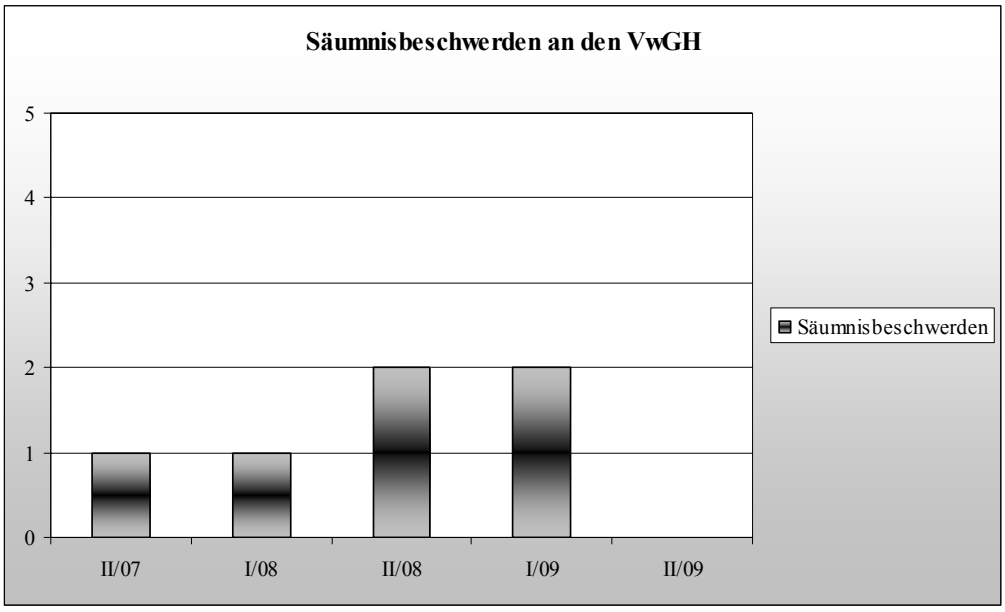
Aus dieser Graphik wird deutlich, wie sich die *durchschnittliche* Erledigungsdauer bei den Individualbeschwerden im Berichtszeitraum entwickelt hat: Trotz des extremen Anstiegs des Eingangs im zweiten Halbjahr 2008 betrug die durchschnittliche Erledigungsdauer im gesamten Berichtszeitraum jeweils weniger als sechs Monate.



Freilich konnte die 6-monatige Erledigungsfrist nicht in jedem Einzelfall eingehalten werden. Die folgende Graphik zeigt, dass die Zahl der länger dauernden Verfahren von fast 0 im zweiten Halbjahr 2008 infolge des außergewöhnlichen Anfalls doch wieder auf 8 anstieg und erst dann Ende 2009 wieder auf 3 Fälle gesenkt werden konnte:

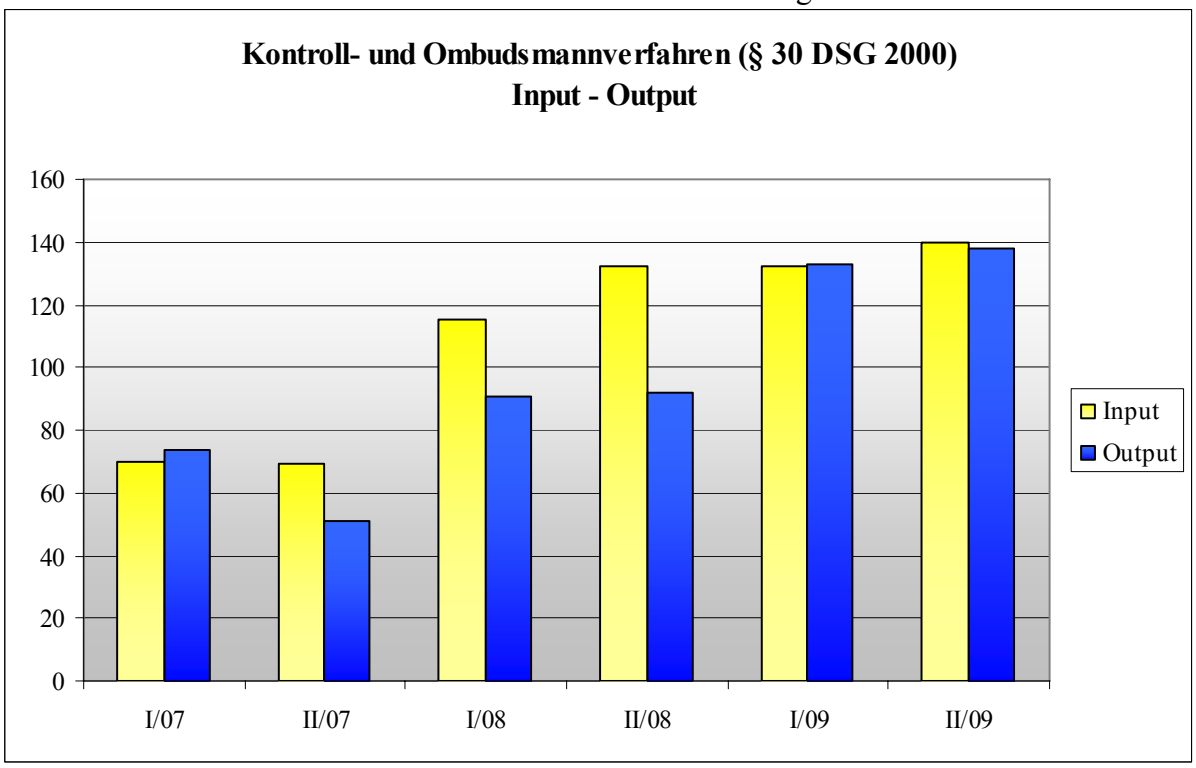


Die Erhebung von Säumnisbeschwerden vor dem Verwaltungsgerichtshof konnte im Berichtzeitraum trotz allem jedoch in engen Grenzen gehalten werden:



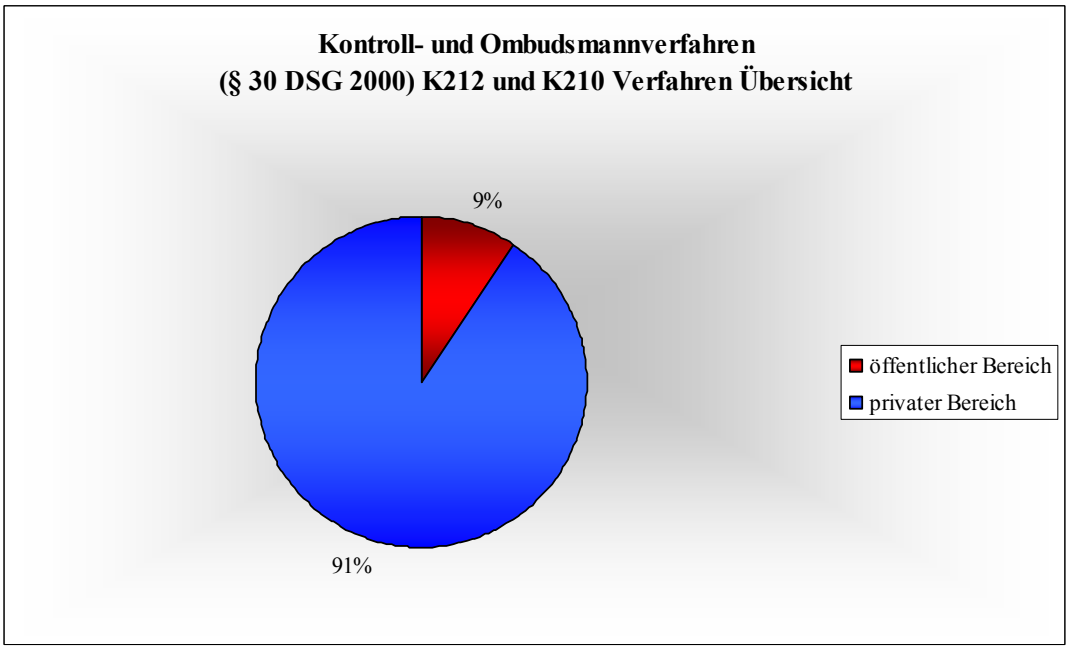
4.2.2 Ombudsmannverfahren (§ 30 DSG 2000)

Hier ist ein stetig steigender Arbeitsanfall zu verzeichnen:



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

Wie wichtig die Ombudsmann-Verfahren zur Herstellung des rechtmäßigen Zustands im privaten Bereich geworden sind, ist aus der obenstehenden Graphik deutlich zu entnehmen: Etwa 90 % aller Eingaben betreffen den privaten Bereich. Bei einem durchschnittlichen jährlichen Eingang von etwa 300 Eingaben, ergibt dies etwa 270

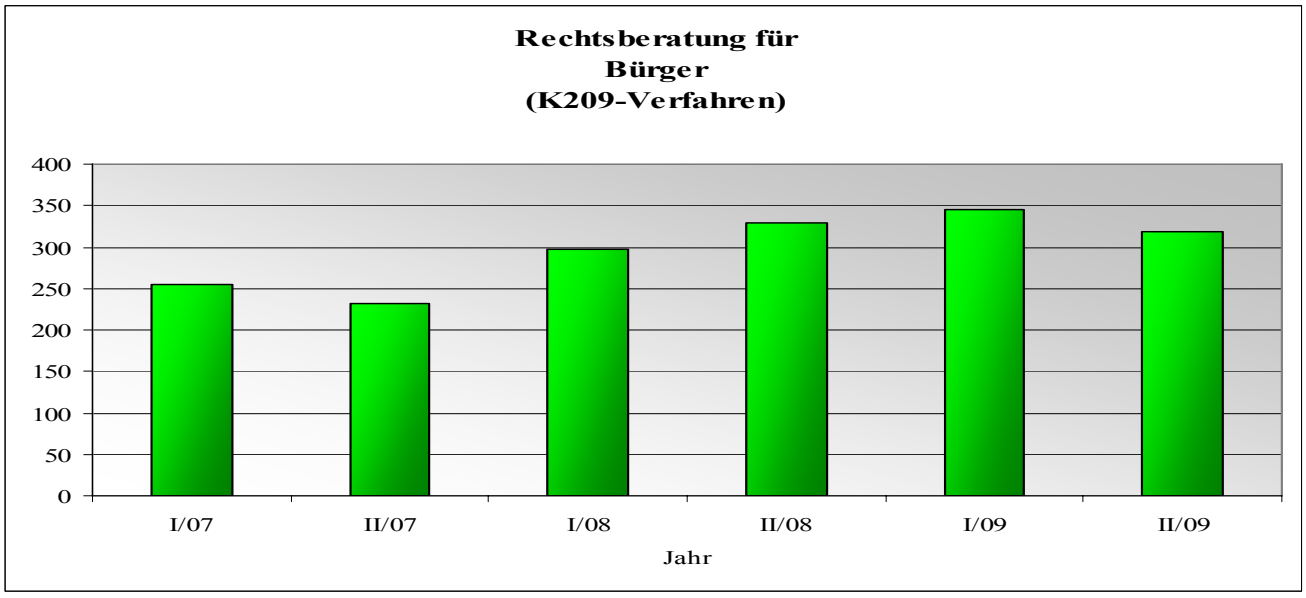


Verfahren gegen Auftraggeber des privaten Bereichs.

Demgegenüber dürfte die Zahl der vor den ordentlichen Gerichten durchgeführten Verfahren in Datenschutzsachen schon wegen des damit verbundenen Kostenrisikos gering sein. Auch wenn die Datenschutzkommission keine erschöpfenden Informationen über die Zahl der gerichtlichen Datenschutzfälle besitzt, scheint es angesichts der veröffentlichten Judikatur gerechtfertigt, von einer geringen Zahl auszugehen. Der Datenschutzkommission sind im Berichtszeitraum 4 konkrete Fälle – im Wege des Ersuchens um Nebenintervention – aus dem Bereich der Datenverwendung in Bonitätsdatenbanken und in Videoüberwachungssystemen bekannt geworden.

4.2.3 Rechtsauskünfte an Bürger (K 209-Verfahren)

Wie wichtig diese vom Büro der Datenschutzkommission wahrgenommene Funktion geworden ist, ergibt sich anschaulich aus der untenstehenden Graphik, die die schriftlich – hauptsächlich in Form von E-Mails – erteilten Rechtsauskünfte umfasst.



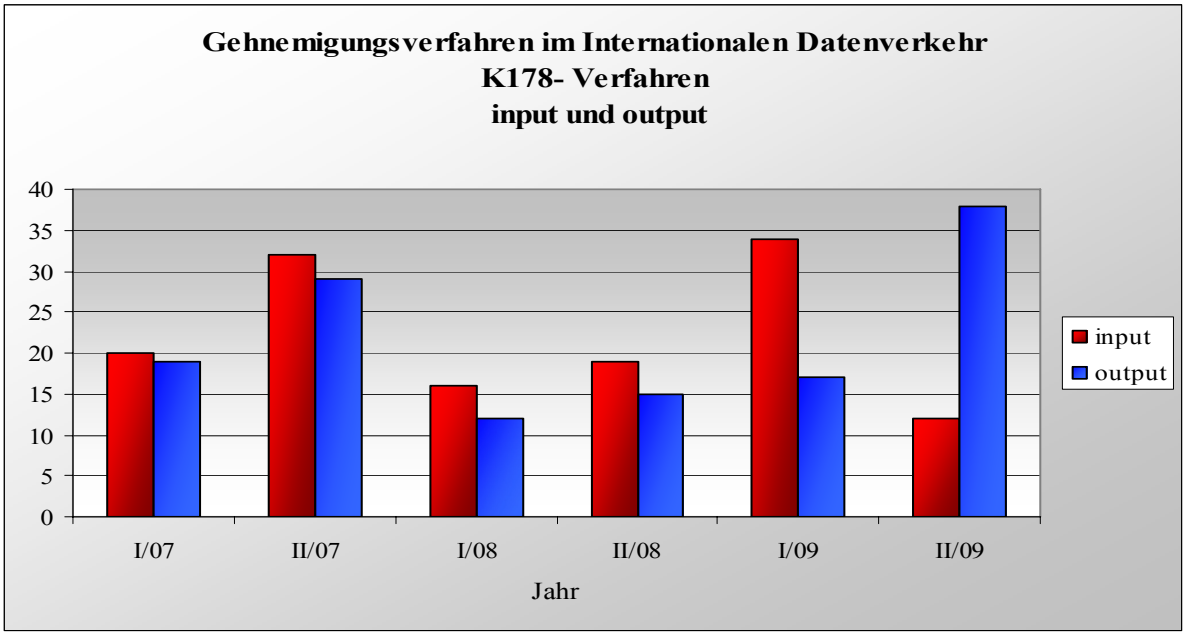
[9]

[9] Da die Erledigung dieser Anbringen meist durch sofortige Beantwortung von E-Mails erfolgt, wird keine eigene Statistik über Output und Erledigungsdauer geführt

Hinzu kommen zahlreiche telefonische Rechtsauskünfte; diesbezüglich wird jedoch keine eigene Statistik geführt.

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

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



In diesem Bereich konnte im Berichtszeitraum eine entscheidende Beschleunigung der Genehmigungsverfahren erreicht werden, nachdem die beträchtlichen Unklarheiten dieses Bereichs durch die Entscheidungspraxis der Datenschutzkommission mehr und mehr beseitigt werden konnten. Diese Entwicklung kann auch aus der unmittelbar vorstehenden Graphik abgelesen werden.

Dass Genehmigungsverfahren dennoch auch derzeit gelegentlich mehr als sechs Monate in Anspruch nehmen, liegt daran, dass das Genehmigungsverfahren eine registrierungsfähige Meldung jener Datenanwendung voraussetzt, aus der die Daten übermittelt bzw. überlassen werden sollen.

Wenn Auftraggeber bei der Ausarbeitung einer solchen Meldung nur mit größeren Verzögerungen handeln, kann auch das Genehmigungsverfahren für den Datentransfer ins Ausland nicht zügig abgeschlossen werden.

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

Auch im vorliegenden Berichtszeitraum war es nur ganz ausnahmsweise erforderlich, die Registrierung von Meldungen mit Bescheid abzulehnen, da die meldenden Auftraggeber letztlich die vom DVR verlangten Verbesserungen in aller Regel vornehmen, wenn auch manchmal erst nach geraumer Weile.

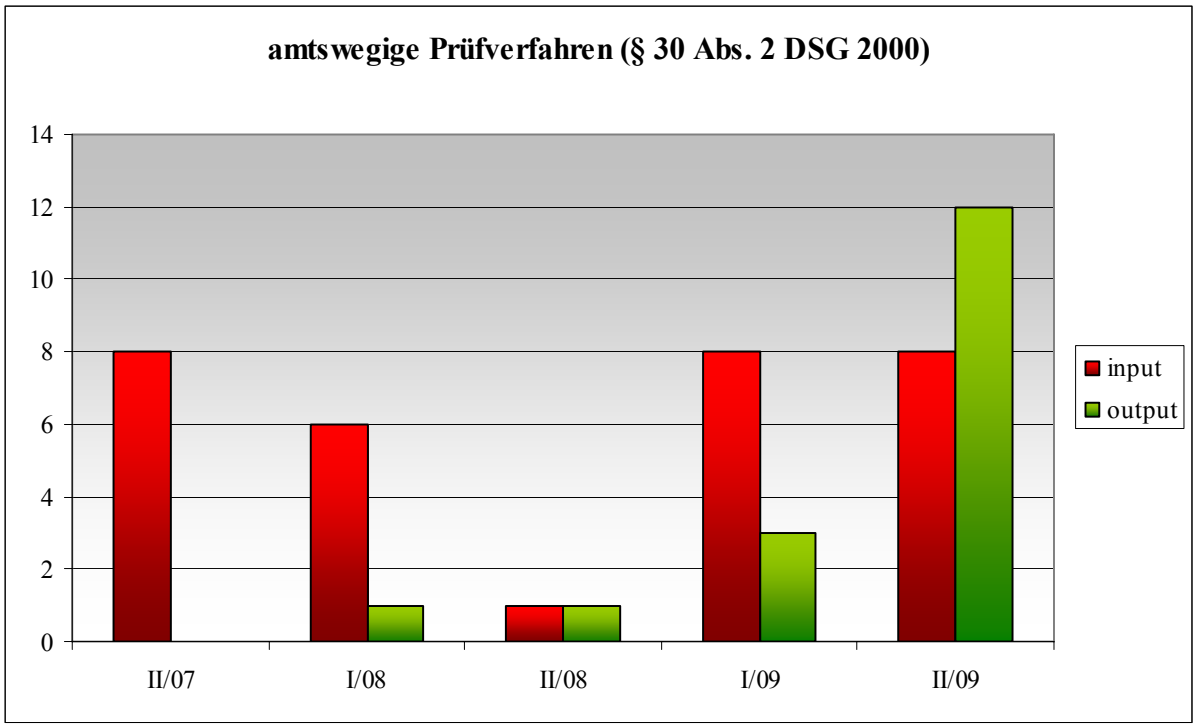
Auflagenbescheide wurden im Berichtszeitraum in größerer Zahl für die Teilnahme am Informationsverbundsystem „Konsumentenkreditevidenz (KKE)“ erteilt.

4.2.6 Amtswegige Prüfverfahren

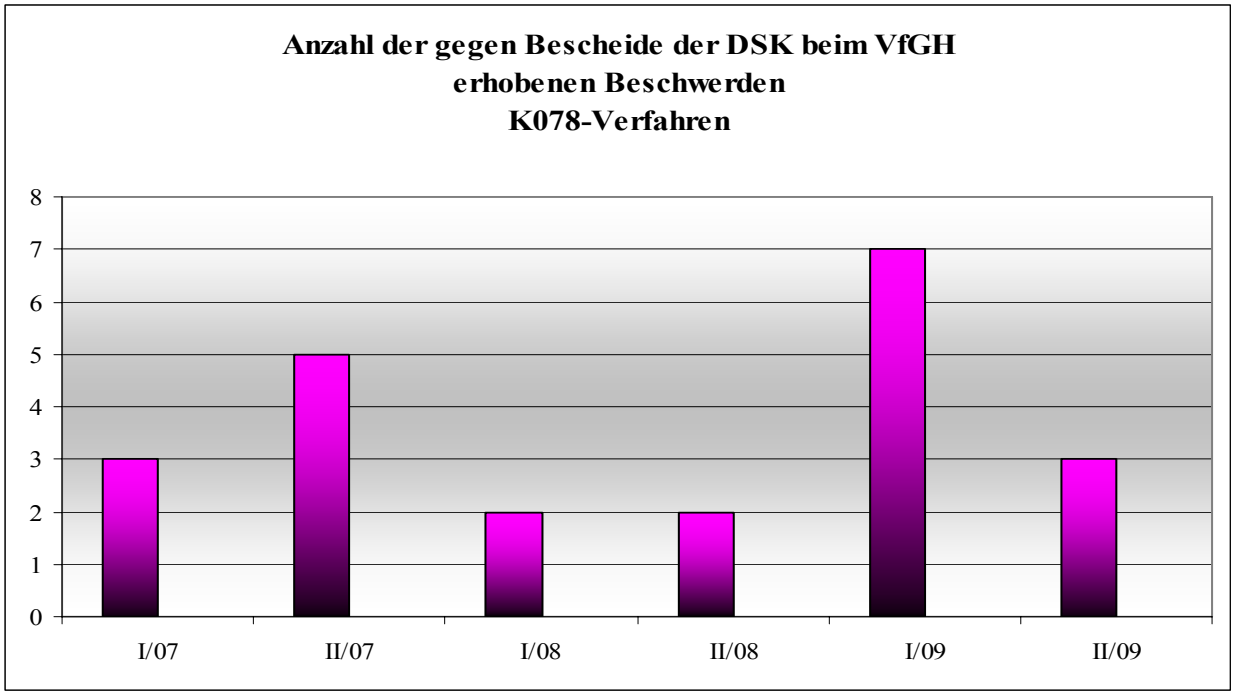
Im Berichtszeitraum sind insgesamt 31 amtswegige Prüfverfahren eingeleitet worden.

Dass die Tätigkeit der Datenschutzkommission in Form amtswegiger Prüfverfahren nicht die wünschenswerte Dichte erreicht, ist der Datenschutzkommission bewusst und wird außerordentlich bedauert, doch ist nicht absehbar, dass sich dieser Zustand bei der gegebenen Personalsituation verbessern ließe.

Zum Gegenstand dieser amtswegigen Prüfverfahren vgl. die Ausführungen im Kapitel 6.



4.2.7 Beschwerdeverfahren vor dem Verfassungsgerichtshof



Im Berichtszeitraum 1. Juli 2007 bis 31. Dezember 2009 wurde beim VfGH in 22 Fällen Beschwerde gegen Bescheide der Datenschutzkommission erhoben (gegenüber 23 Beschwerden im vorigen Berichtszeitraum).

In 5 Fällen wurde der Beschwerde stattgegeben,

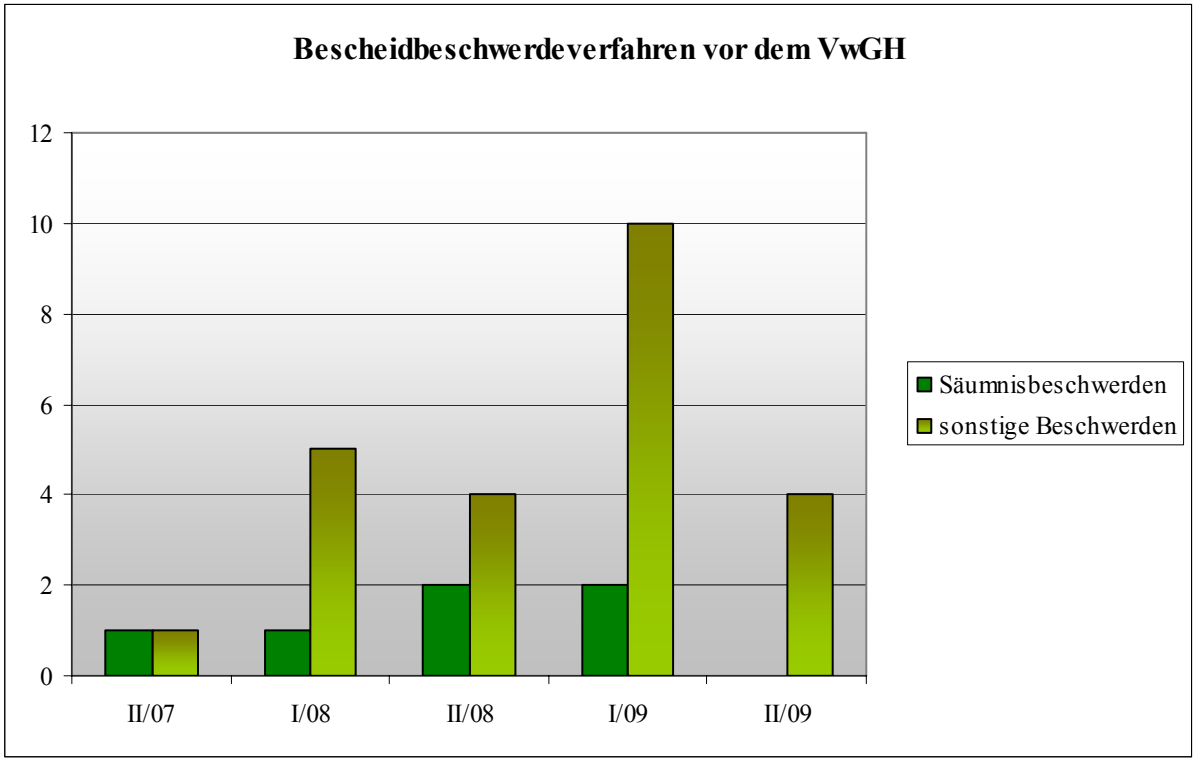
in 9 Fällen wurde die Behandlung der Beschwerde abgelehnt,

in 4 Fällen wurde die Beschwerde abgewiesen.

Über 4 Beschwerdefälle wurden noch nicht entschieden.

Zum Gegenstand jener Beschwerden, welchen stattgegeben wurde, vgl. die Ausführungen im Kapitel 6.

4.2.8 Beschwerdeverfahren vor dem Verwaltungsgerichtshof



Der ungewöhnliche Anstieg von VwGH-Beschwerden im zweiten Halbjahr 2007 und dann wiederum im ersten Halbjahr 2009 ist zur Gänze auf eine einzige Kategorie von Beschwerdeverfahren vor der Datenschutzkommission zurückzuführen, nämlich auf Beschwerdeverfahren betreffend die Löschung von Daten aus Kanzleiindices und Akten der Sicherheitsbehörden über Strafverfahren bzw. kriminalpolizeiliche Erhebungen .

Im Berichtszeitraum 1. Juli 2007 bis 31. Dezember 2009 wurde beim VwGH in 24 Fällen Beschwerde gegen einen Bescheid der Datenschutzkommission erhoben (gegenüber 27 Beschwerden im vorigen Berichtszeitraum).

In 4 Fällen wurde der Beschwerde stattgegeben,

in 7 Fällen wurde die Beschwerde abgewiesen bzw. zurückgewiesen.

Über die restlichen 13 Beschwerden wurde noch nicht entschieden.

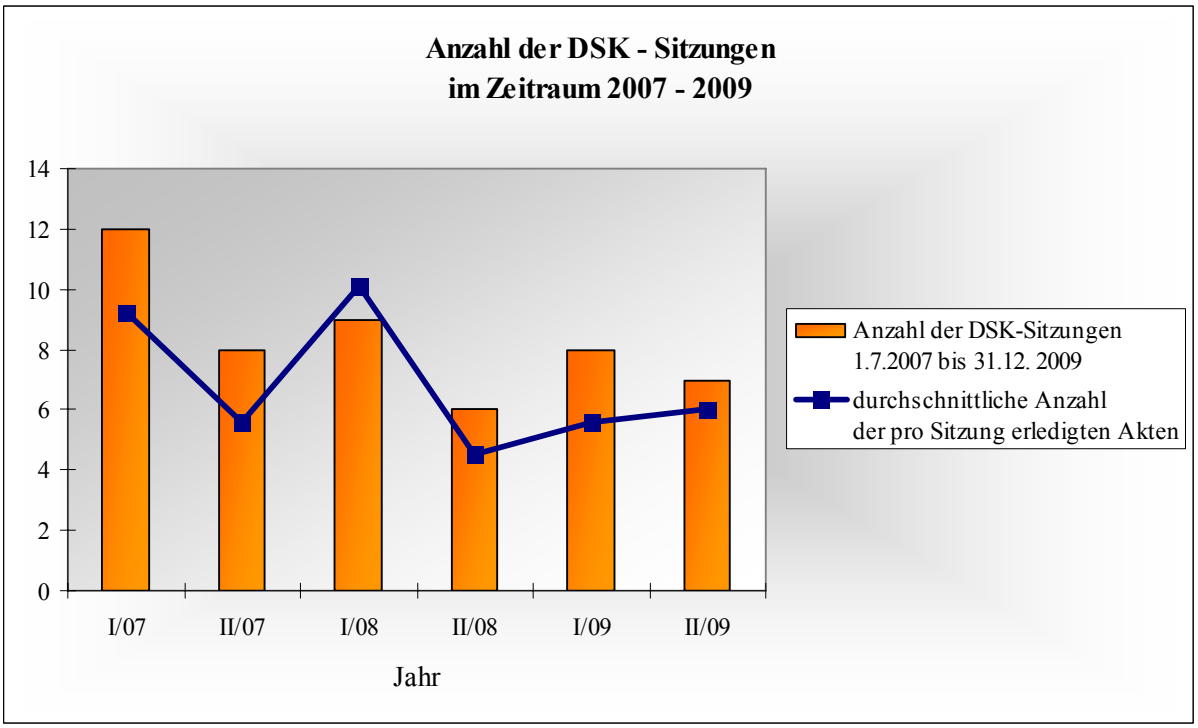
Zum Gegenstand jener Beschwerden, welchen stattgegeben wurde, vgl. auch die Ausführungen im Kapitel 6.

Was die Erhebung von Säumnisbeschwerden betrifft, ist die Datenschutzkommission äußerst bemüht, Anlässe für Säumnisbeschwerden zu vermeiden. Dass dies nicht immer - wenn auch immer besser - gelingt, ist dadurch begründet, dass die Datenschutzkommission in erster Instanz entscheidet und daher zunächst der Sachverhalt festgestellt werden muss, was manchmal zu unvorhergesehenen Verzögerungen führt; weiters liegt es in der Natur einer Kollegialbehörde, dass Entscheidungen nicht immer bei der erstmaligen Beratung eines Falles getroffen werden können und auch dadurch Verzögerungen eintreten.

4.3 Sitzungen der Datenschutzkommission

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

Graphische Darstellung der Sitzungshäufigkeit und Anzahl der behandelten Akten:



5. Kritische Anmerkungen zur Personal- und Organisationssituation der Datenschutzkommission

5.1 Zu den Aufgaben der Datenschutzkommission und ihrer Personalausstattung

5.1.1 Grundsätzliches zur Personalausstattung

An dem Umstand, dass die Datenschutzkommission – gemessen an der Einwohnerzahl - nur rund halb so viel Personal besitzt wie die meisten anderen Datenschutz-Kontrollstellen der Mitgliedsstaaten der Europäischen Union, hat sich nichts geändert.

Die DSG-Novelle 2010 versucht Umschichtungen im Personaleinsatz allenfalls dadurch zu ermöglichen, dass künftig weniger Ressourcen für die Registrierung von Meldungen an das Datenverarbeitungsregister eingesetzt werden müssen: Dies soll dadurch erreicht werden, dass nur mehr vorabkontrollpflichtige Datenanwendungen inhaltlich geprüft werden müssen.

Erfahrungsgemäß sind etwa 50 % der gemeldeten Datenanwendungen nicht vorabkontrollpflichtig. Die künftige Rechtslage könnte daher eine beträchtliche Erleichterung im Arbeitsanfall des Datenverarbeitungsregisters mit sich bringen. Ob es allerdings tatsächlich möglich sein wird, nennenswerte Personalumschichtungen vorzunehmen, scheint fraglich – es muss nämlich in Rechnung gestellt werden, dass derzeit eine erhebliche Diskrepanz zwischen Input und Output im DVR besteht, sodass zu befürchten ist, dass mit der Einführung des neuen Systems nur gerade das Gleichgewicht zwischen Arbeitsanfall und Erledigungskapazität hergestellt, nicht aber Personal freigesetzt werden kann für andere Aufgaben einer Datenschutz-Kontrollstelle.

5.1.2 Beschwerden von Bürgern

Mit dem derzeitigen Personalstand des Büros der Datenschutzkommission lassen sich, wie die statistischen Auswertungen im Abschnitt „Geschäftsgang“ gezeigt haben, die Beschwerdeverfahren einigermaßen bewältigen; bei entsprechend starker Anspannung ist es möglich, jene Verfahren, für die die gesetzliche Entscheidungspflicht des § 73 AVG gilt, innerhalb von 6 Monaten durchzuführen.

Bei den Ombudsmannverfahren ist es im Berichtszeitraum allerdings nicht immer gelungen, eine Erledigungsdauer von weniger als 6 Monaten zu erreichen, insbesondere bei extremen Anfallspitzen betreffend Verfahren nach § 31 DSG 2000 (wie etwa im 2. Halbjahr 2008), da dann die Verfahren nach § 30 DSG 2000 zurückstehen müssen. Die Zahl dieser Verfahren nimmt bei gleichbleibender Personalkapazität stetig zu und kann daher auch durch Überstundenleistung nur bis zu einem gewissen Grad ausgeglichen werden. Ein zusätzlicher Referent/Referentin wäre in diesem Bereich erforderlich.

5.1.3 Zusammenarbeit auf EU-Ebene

Diesbezüglich hat sich die Situation gegenüber dem letzten Datenschutzbericht in keiner Weise geändert. Im letzten Bericht wurde Folgendes ausgeführt:

„Weiters ist es durch besondere Anstrengungen gerade noch möglich, einigermaßen (wenn auch oft nur sehr oberflächlich) an den wichtigsten Aktivitäten der Art. 29 Gruppe und einiger ihrer Unterarbeitsgruppen sowie an den Sitzungen der Gemeinsamen Kontrollinstanzen der Dritten

Säule (vgl. dazu Abschnitt 7) teilzunehmen.

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

Für diesen Tätigkeitsbereich gibt es nach wie vor keinen Referenten in der Geschäftsstelle der Datenschutzkommission, seitdem diese Planstelle mit 1. Juli 2006 verloren gegangen ist. Angesichts der unvermeidlichen Rückwirkungen der im Rahmen der Art. 29 Gruppe erarbeiteten Lösungen auf den Datenschutz in Österreich wird versucht, nach Möglichkeit Personalressourcen für die Teilnahme an wichtigen Initiativen dennoch frei zu machen – an eine kontinuierliche und strategische ausgerichtete Einflussnahme auf die Arbeit auf europäischer Ebene ist unter diesen Voraussetzungen jedoch nicht zu denken, was umso bedauerlicher ist, als Vertreter der österr. Datenschutzkommission wiederholt zur Übernahme besonderer Verantwortung in der Art. 29 Gruppe eingeladen wurden, dies jedoch mangels personeller Ausstattung des Geschäftsapparats der Datenschutzkommission immer ablehnen mussten.

5.1.4 Prüfung von Datenanwendungen

Was beim gegebenen Personalstand weiters nicht ausreichend wahrgenommen werden kann, ist die regelmäßige und planvolle Prüfung von Datenanwendungen vor Ort (vgl. § 30 Abs. 2 und 3 DSG 2000). In diesem Punkt weist die Tätigkeit der Datenschutzkommission bei einem europäischen Vergleich das größte Defizit im Verhältnis zur Tätigkeit anderer nationaler Kontrollstellen auf.

Wie bereits im letzten Bericht festgestellt wurde, nimmt nach dem bei den Datenschutzkontrollstellen iSd Art. 28 der RL 95/46/EG im Europäischen Wirtschaftsraum (EWR) vorherrschenden Standard die Kontrolltätigkeit in Form der Vorort-Prüfung von Datenanwendungen (- vgl. auch Art. 28 Abs. 3, erster Anstrich -) einen ganz besonders hohen Stellenwert ein. Die Art. 29 Gruppe widmet sich diesem Thema in einer eigenen Unterarbeitsgruppe „Enforcement", die sich mit der koordinierten europaweiten datenschutzrechtlichen Überprüfung zB einer gesamten Branche durch die nationalen Kontrollstellen beschäftigt.

Es scheint daher dringend geboten, die Datenschutzkommission durch Zurverfügungstellung der nötigen Ressourcen in die Lage zu versetzen, ihre Prüfkompetenz in umfangreicherem Maße wahrzunehmen.

5.1.5 Öffentlichkeitsarbeit

a) Information der Öffentlichkeit in Datenschutzfragen

Die Datenschutzkommission und ihr Geschäftsapparat sind trotz dauerndem Zeitmangel bemüht, so viel als möglich zu objektiver und sachgerechter Information der Öffentlichkeit in Datenschutzbelangen beizutragen.

Das GfM hat zu aktuellen Datenschutzfragen zahlreiche Interviews für die Medien gegeben.

Es wurden Vorträge in Schulen, Fachhochschulen, Universitätsveranstaltungen, Seminaren, Konferenzen und Kongressen verschiedenster Fachrichtung gehalten, um den Stellenwert von Datenschutz in den

unterschiedlichsten Bereichen zu verdeutlichen.

Die Datenschutzkommission hat im Berichtszeitpunkt auch besondere Anstrengungen unternommen, um ihren Web-Auftritt möglichst informativ und aktuell zu gestalten.

b) Zur Einbeziehung der Datenschutzkommission in das Begutachtungsverfahren für Gesetzentwürfe:

Das Bestehen einer entsprechenden Kompetenz der Datenschutzkommission wurde in der Vergangenheit gelegentlich bestritten, doch hat sich diesbezüglich die Situation in der Berichtsperiode in dem Sinn normalisiert, dass für den Datenschutz wesentliche Gesetzes- und Verordnungsentwürfe regelmäßig auch der Datenschutzkommission zur Stellungnahme im Begutachtungsverfahren zugeleitet werden.

Die Datenschutzkommission macht von der Möglichkeit zur Stellungnahme bei besonders wichtigen Entwürfen auch regelmäßig Gebrauch, und zwar auch dann, wenn sie zur Teilnahme im Begutachtungsverfahren nicht ausdrücklich aufgefordert worden sein sollte.

Als nicht ausreichend hat sich die Einbindung der Datenschutzkommission allerdings in die Gesetzwerdung der DSG-Novelle 2010 erwiesen: Eine eingehende Diskussion mit der Datenschutzkommission hat nicht im erforderlichen Ausmaß stattgefunden. Die vorgenommenen Novellierungsänderungen stimmen daher in manchen Punkten mit den Vorstellungen der Datenschutzkommission über optimale Lösungen nicht überein. Dies gilt insbesondere im Bereich der neuen Bestimmungen über die Videoüberwachung in den §§ 50a ff DSG 2000 idF der DSG-Novelle 2010.

5.1.6 Zusammenfassung

In den nach Auffassung der Datenschutzkommission von ihr wahrzunehmenden Bereichen „Kontrollverfahren“ und „Zusammenarbeit auf EU-Ebene“ besteht nach wie vor dringender Handlungsbedarf hinsichtlich der Personalausstattung der Geschäftsstelle der Datenschutzkommission.

5.2 Zur räumlichen Unterbringung des Geschäftsapparates der Datenschutzkommission

Diesbezüglich ist es in der Berichtsperiode endlich gelungen, eine sinnvolle Lösung zu finden, indem nunmehr der gesamte Geschäftsapparat der Datenschutzkommission gemeinsam am Standort Hohenstaufengasse untergebracht ist.

Dies hat zu einer wesentlichen Erleichterung der Koordination der Arbeit zwischen den einzelnen Organisationseinheiten des Geschäftsapparats geführt.

5.3 Zur organisatorischen Stellung der Datenschutzkommission und ihres Geschäftsapparates

5.3.1 Die Kommission und ihre Mitglieder

a) Die Mitglieder der Datenschutzkommission „üben diese Funktion neben ihnen sonst obliegenden beruflichen Tätigkeiten aus“ – dies wurde durch die DSG-Novelle 2010 im neuen § 36 Abs. 3a ausdrücklich festgelegt. Damit ist klargestellt, dass vor allem auch die Funktion des GfM der Datenschutzkommission keine hauptberufliche Tätigkeit ist, sondern nur neben einem Hauptberuf – derzeit neben der Leitung der Geschäftsstelle der Datenschutzkommission – ausgeübt werden kann. Die Geschäftsstelle ist als Abteilung im Bundeskanzleramt eingerichtet.

b) Durch die Änderung des Bundes-Verfassunggesetzes mit der Novelle BGBl I Nr. 2/2008, wurde eine neue generelle verfassungsrechtliche Grundlage für die

Einrichtung weisungsfreier Verwaltungsbehörden geschaffen (Art. 20 Abs. 2 B-VG neu) . Gleichzeitig wurde die bisherige spezielle verfassungsrechtliche Grundlage der Weisungsfreiheit der Mitglieder der Datenschutzkommission im § 37 DSG 2000 durch Aufhebung des Verfassungsrangs dieser Bestimmung beseitigt und die Datenschutzkommission dem generellen Regime des Art. 20 Abs. 2 B-VG für weisungsfreie Verwaltungsbehörden unterstellt. Art. 20 Abs. 2 B-VG (neu) enthält nunmehr ein ausdrückliches Unterrichtungsrecht des zuständigen Bundesministers gegenüber weisungsfreien Verwaltungsbehörden in seinem Ressortbereich.

In der DSG-Novelle 2010 hat diese neue Rechtslage auch insofern Niederschlag gefunden, als ein Unterrichtungsrecht des Bundeskanzlers nunmehr ausdrücklich in § 38 Abs. 2 DSG 2000 festgeschrieben ist: „Der Bundeskanzler hat das Recht, sich jederzeit über alle Gegenstände der Geschäftsführung der Datenschutzkommission beim Vorsitzenden und dem geschäftsführenden Mitglied zu unterrichten."

Darüber hinaus sieht die DSG-Novelle 2010 allerdings die Einrichtung eines weiteren Unterrichtungs- und Einsichtsrechts des Datenschutzrates vor: Gemäß § 41 Abs. 2 Z 4 wird dem Datenschutzrat nunmehr das Recht eingeräumt, „von der Datenschutzkommission Auskünfte und Berichte sowie die Einsicht in Unterlagen zu verlangen". Ohne auf die unionsrechtliche Dimension dieser Bestimmung eingehen zu wollen, scheint sie jedenfalls im Hinblick auf Art. 20 Abs. 2 B-VG als verfassungsrechtlich bedenklich.

5.3.2 Der Geschäftsapparat

Gemäß § 38 Abs. 2 DSG 2000 hat der Bundeskanzler zur Unterstützung der Geschäftsführung der Datenschutzkommission die notwendige Sach- und Personalausstattung bereitzustellen. Diese Verpflichtung ist so umgesetzt, dass der Bundeskanzler der Datenschutzkommission eine Abteilung im BKA als Geschäftsapparat zur Verfügung gestellt hat. Der Bundeskanzler ist Dienstvorgesetzter der Bediensteten dieser Geschäftsstelle (vgl. § 37 Abs. 2 DSG 2000).

5.3.3 Ausblick

Das zwischenzeitig ergangene Urteil des EuGH C-518/07, in dem die rechtliche Stellung bestimmter deutscher Länder-Datenschutz-Kontrollstellen in Prüfung gezogen wurde, hat eine strenge Auslegung des Begriffs der „Tätigkeit in völliger Unabhängigkeit" ergeben, wonach zB die aus der organisatorischen Einordnung dieser Kontrollstellen in den Länder-Innenministerien erwachsende Aufsicht der Länder als unionsrechtswidrig befunden wurde. Generell wird in diesem Urteil die durch die Verordnung 2001/45 geschaffene Institution des EDPS (Europäischer Datenschutzbeauftragter) als Maßstab für die adäquate Einrichtung einer Datenschutz-Kontrollbehörde bezeichnet.

Die Antwort auf die Frage, welche Konsequenzen sich aus diesem Urteil für die österreichische Rechtslage ergeben, wird voraussichtlich im nächsten Berichtszeitraum gefunden werden müssen.

5.4 Zum Entwurf einer Verwaltungsgerichtsbarkeits-Novelle 2010

Zu dem unter Zl BKA-601.999/0001-V/1/2010 kürzlich in Begutachtung versendeten Entwurf einer Verwaltungsgerichtsbarkeits-Novelle 2010, als deren Folge die Datenschutzkommission aufgelöst werden soll, hat die Datenschutzkommission folgende Stellungnahme abgegeben: „Durch Z 25 des Teils A der in Z 36 des Novellenentwurfes vorgesehenen „Anlage" soll die Datenschutzkommission aufgelöst werden.

Die Datenschutzkommission übt die Funktion einer nationalen Datenschutz-Kontrollstelle im Sinne des Art. 28 der RL

95/46 aus. In jedem Mitgliedsstaat der EU müssen eine oder mehrere solche Kontrollstelle(n) eingerichtet sein. Für Kontrollstellen nach Art. 28 besteht somit eine unionsrechtliche Bestandsgarantie. Da die österreichische Datenschutzkommission die einzige nationale Kontrollstelle im Sinne des Art. 28 ist, kann eine Auflösung der Datenschutzkommission nur stattfinden, wenn gleichzeitig dafür Vorsorge getroffen ist, dass die Aufgaben nach Art. 28 der RL von anderen Organen der Republik Österreich wahrgenommen werden. Dies wird in dem vorliegenden Novellenentwurf jedoch verabsäumt.

Keine der Kompetenzen der Datenschutzkommission kann unmittelbar aufgrund des vorliegenden Gesetzestextes auf die Verwaltungsgerichte übergehen, da die Fälle des Art. 130 Abs. 1 zur Gänze auf die Aufgaben der Datenschutzkommission unanwendbar sind: In keinem Fall entscheidet die Datenschutzkommission über die in Art. 130 Abs. 1 genannten Fälle, insbesondere auch nicht über „den Bescheid einer Verwaltungsbehörde“ (Art. 130 Abs. 1 Z 1) oder „die Ausübung von unmittelbarer Befehls- oder Zwangsgewalt“ (Art. 130 Abs. 1 Z 2). Allein der Umstand, dass sich die Aufgaben, für die die Verwaltungsgerichte eigentlich geschaffen werden sollen, in keinem einzigen Fall mit jenen der Datenschutzkommission decken, ist ein wesentliches Indiz dafür, dass der intendierte Kompetenzübergang offenbar nicht auf ideale Voraussetzungen beim Kompetenzempfänger trifft, da dieser vorrangig für andere Tätigkeiten eingerichtet ist.

Selbst wenn die Absicht bestehen sollte, diese Vorsorge durch entsprechende spätere einfachgesetzliche Regelungen (Art. 130 Abs. 2) noch zu treffen, stehen einer derartigen Übertragung der Kompetenzen der Datenschutzkommission auf die Verwaltungsgerichte grundsätzliche und unüberwindliche Hindernisse entgegen: Die Novelle geht davon aus, dass durch die Schaffung von Verwaltungsgerichten für bestehende Rechtsschutzkompetenzen von Verwaltungsorganen eine zweckmäßigere – und zumindest aufkommensneutrale – Gesamtlösung gefunden wird und gleichzeitig keine Lücken im Rechtsschutzsystem entstehen. Diese Wirkung kann im Falle des Übergangs der Kompetenzen der Datenschutzkommission auf Verwaltungsgerichte nicht erreicht werden, weil der weit überwiegende Teil der Kompetenzen der Datenschutzkommission nicht „gerichtsfähig“ ist, handelt es sich doch großteils um informellen (kurativen) Rechtsschutz oder vorbeugenden Rechtsschutz durch Kontrolle von Datenanwendungen unabhängig vom Vorliegen von Beschwerden: Die Durchführung von Ombudsmann-Verfahren nach § 30 DSG 2000 ist ihrer Natur nach am ehesten mit der Tätigkeit der Volksanwaltschaft – ausgedehnt auf den gesamten privaten Bereich – zu vergleichen; die Kontrolle der Rechts- und Ordnungsmäßigkeit von Datenanwendungen gleicht am ehesten der Rechtmäßigkeitskontrolle durch den Rechnungshof, freilich eingeschränkt auf Fragen des Datenschutzes, aber ausgedehnt auf den gesamten privaten Bereich; dem vorbeugenden Rechtsschutz dient auch das Registrierungsverfahren im Datenverarbeitungsregister.

„Gerichtsfähig“ sind nur die förmlichen Entscheidungen der Datenschutzkommission in Verfahren nach § 31 DSG 2000, die in ihrem Gesamtaufwand jedoch bestenfalls 25 % des Gesamt-Arbeitsaufwands der Behörde „Datenschutzkommission“ darstellen. Von diesen „gerichtsfähigen“ Aufgaben ist der überwiegende Teil dennoch nicht an Verwaltungsgerichte übertragbar, da es sich nicht um Beschwerdefälle handelt, die ein Verhalten „in Vollziehung der Gesetze“ (Art. 130 Abs. 2 Z 1) zum Gegenstand haben: Die Behandlung der Beschwerden wegen Verletzung im Recht auf Auskunft durch Auftraggeber des privaten Bereichs – die zahlenmäßig den weitaus größten Teil der Verfahren nach § 31 DSG 2000 ausmachen – ist nach dem vorliegenden Novellentext nicht auf Verwaltungsgerichte übertragbar, sodass

im Endeffekt bestenfalls 10 % der Tätigkeit der Datenschutzkommission überhaupt für eine Übertragung (durch besonderes einfaches Gesetz) auf die Verwaltungsgerichte in Frage kämen. (Ein Eingehen auf die Frage, ob die Übertragung an das Bundesverwaltungsgericht oder teilweise an die Landesverwaltungsgerichte erfolgen müsste, scheint angesichts der Schwierigkeit der Einordnung des – derzeit noch geltenden – § 2 Abs. 2 DSG 2000 in den neuen Art. 131 im derzeitigen Stadium der Diskussion entbehrlich).

Daraus folgt, dass bei Auflösung der Datenschutzkommission eine neue Behörde geschaffen werden müsste, der der Löwenanteil der bisherigen Kompetenzen der Datenschutzkommission übertragen wird. Daraus folgt weiters, dass die Auflösung der Datenschutzkommission in keiner Weise zweckmäßig sein kann:

1. Zusätzlich zu den Verwaltungsgerichten müsste nach wie vor eine eigene Behörde als Datenschutz-Kontrollstelle mit umfangreichen Kompetenzen eingerichtet sein. Dies kann nicht aufkommensneutral oder gar einsparend wirken, da sich zumindest eine zusätzliche Behörde und damit zusätzliches Personal mit Fragen des Datenschutzes intensiv auseinandersetzen müsste. Auch würde dadurch die Einheitlichkeit der Rechtsprechung reduziert. Für die Wirtschaft ist aber jede Kompetenzzersplitterung ein zusätzlicher Kostenfaktor, da damit die Entscheidungen inhaltlich schwerer vorhersehbar werden.

2. Wenn die Beschwerden nach § 31 DSG 2000 über Auftraggeber des öffentlichen Bereichs tatsächlich an die Verwaltungsgerichte übertragen werden, weil die Datenschutz-Kontrollstelle keine gerichtsähnliche Tätigkeit entfalten soll, müssten parallel dazu die Beschwerden über Auskunftsverletzungen durch Auftraggeber des privaten Bereichs wieder an die ordentlichen Gerichte zurückfallen, die vor dem DSG 2000 hiefür zuständig waren. Dies würde eine entscheidende Einbuße für die Betroffenen im Rechtsschutzsystem zur Folge haben, da erfahrungsgemäß in Datenschutzsachen vom Rechtsschutz vor den ordentlichen Gerichten infolge des Prozessrisikos kaum Gebrauch gemacht wird. Es käme daher zu einer Verschlechterung der Gesamtsituation aus dem Blickwinkel eines effektiven Rechtsschutzes.

3. Der Verwaltungsgerichtshof würde durch den Übergang von Datenschutzkompetenzen auf die Verwaltungsgerichte in keiner Weise entlastet, da diese in erster Instanz entscheiden würden und daher der Rechtszug zum VwGH so wie bisher offenstehen muss.

4. Die Verwaltungsgerichte sind ihrer Natur nach nicht für Entscheidung in erster Instanz und für die dafür notwendigen Sachverhaltsermittlungen gedacht, sodass übertragene Datenschutzkommission-Kompetenzen zur Entscheidung in Beschwerdesachen jedenfalls einen Fremdkörper bei den Verwaltungsgerichten darstellen würden. Auch aus diesem Grund scheint die „Ersetzung“ der Datenschutzkommission durch Verwaltungsgerichte zweckwidrig und völlig ungeeignet, in irgendeiner Weise Mehrwert zu erzeugen.

5. Im Übrigen darf darauf hingewiesen werden, dass die wiederholte öffentliche Ankündigung der Auflösung der nationalen Datenschutz-Kontrollstelle – ohne die geringste Erwähnung einer brauchbaren Alternativlösung – geeignet ist, im europäischen Kontext Befremden hervorzurufen und überdies die Arbeit der österreichischen Datenschutzkommission im nationalen wie im europäischen Zusammenhang zu behindern.“

Abschließend ist noch in Erinnerung zu rufen, dass sich die Prüfungsaufgabe der Datenschutzkommission über alle Bereiche des Verwaltungs- und Zivilrechts erstreckt und durch die derzeit vorgesehene Zusammensetzung der Datenschutzkommission auch gewährleistet ist, dass die Erfahrungen aus diesen Bereichen in die Entscheidungen der Datenschutzkommission einfließen können.

6. Zu Entscheidungsart und Inhalt der im Berichtszeitraum durchgeführten Verfahren

Die Entscheidungen der Datenschutzkommission werden in ihrem gesamten Wortlaut in anonymisierter Form im Rechtsinformationssystem des Bundes (RIS, www.ris.bka.gv.at) veröffentlicht. Im Folgenden werden daher nur einzelne Aspekte von Entscheidungen – in stark verkürzter Form – aus dem Berichtszeitraum vorgestellt, die zu wichtigen **rechtsdogmatischen oder rechtspolitischen Fragen** Stellung nehmen bzw. wesentliche Tendenzen aufzeigen.

6.1 Beschwerdeverfahren nach § 31 DSG 2000

Beschwerdeverfahren nach § 31 DSG 2000 führen zu Entscheidungen (Bescheiden), die für die dadurch Verpflichteten rechtlich verbindlich sind. Solche verbindlichen Entscheidungen können wegen Verletzung der Rechte auf Geheimhaltung, Auskunft, Richtigstellung oder Löschung gegen Auftraggeber des öffentlichen Bereichs gefällt werden – gegen Auftraggeber des privaten Bereichs jedoch nur hinsichtlich der Verletzung der Pflicht zur Auskunftserteilung. Als Folge der umfassenden Zuständigkeit der Datenschutzkommission zur Entscheidung über Beschwerden zum Auskunftsrecht machen Verfahren wegen Verletzung dieses Rechts den weitaus größten Teil der Beschwerdefälle aus.

6.1.1 Anmerkungen zum Inhalt der Entscheidungen

6.1.1.1 Zu möglichen Grenzen des Auskunftsrechts

a) Als grundsätzliches Problem muss der Umstand angesprochen werden, dass moderne Datenanwendungen durch einen hohen Grad an Komplexität und Dezentralisierung (zB E-Mails auf den note books der Mitarbeiter des Auftraggebers) gekennzeichnet sind, sodass die **Vollständigkeit einer Auskunft** immer schwieriger garantiert – und überprüft (!) – werden kann. Die Volltextsuche ist hier keine verlässliche Abhilfe, da selbst dann, wenn die Textdokumente alle verfügbar sind, die Bezugnahme auf Personen in Dokumenten ja nicht allein durch die Verwendung ihres Namens erfolgt (zB „der Kläger“, „der Beschuldigte“). Eine praktikable, automationsunterstützte Umsetzung des Auskunftsrechts betreffend unstrukturierte Fließtexte würde in vielen Fällen einer umfassenden Indizierung von Dokumenteninhalten nach personenbezogenen Merkmalen bedürfen; das aber kann aus datenschutzrechtlichen Gründen nicht wünschenswert sein, da dadurch die gezielte Auffindbarkeit personenbezogener Daten wesentlich erleichtert würde. Die Datenschutzkommission hat daher in ihrer Rechtsprechung des Öfteren die Mitwirkungsobliegenheit des Betroffenen (nähere Angaben zu möglichen Datenfundstellen auf Aufforderung durch den Auftraggeber) betont.

b) In diesem Zusammenhang hat sich auch mehrfach die Frage gestellt, ob für Zwecke der **Auskunftserteilung** nur jene **Suchmethoden** angewendet werden müssen, die beim Auftraggeber auch sonst bei der Datenverarbeitung eingesetzt werden oder ob für die Beantwortung einer Auskunft zusätzliche Suchmethoden entwickelt und eingesetzt werden müssen, damit Daten des Auskunftswerbers auch dann gefunden

werden, wenn sie mit Hilfe der vom Auftraggeber sonst angewendeten Suchhilfen nicht gefunden werden können. Dahinter steht das datenschutzrechtliche Problem, dass die datenschutzrelevante Gefahr der leichten Auffindbarkeit von Daten des Auskunftswerbers in diesem Fall erst durch die Auskunft erzeugt würde, wenn man von der Verpflichtung zum Einsatz außergewöhnlicher Suchhilfen ausginge. Eine Entscheidung über diese Fragestellung ist von dem derzeit beim Verwaltungsgerichtshof anhängigen Verfahren Zl. 2010/17/0051-2 zu erhoffen.

c) Eine im Grunde ähnliche Problematik lag einer Entscheidung über das Bestehen eines **Auskunftsrechts betreffend *nicht ausgewertete* Videoüberwachungsdaten** zugrunde (K121.385/0007-DSK/2008 u.a.m.): Ein Auskunftsverlangen im Hinblick auf nicht ausgewertete Videoüberwachungsdaten hat den – aus datenschutzrechtlicher Sicht – absurden Effekt, dass Daten, die dem Auftraggeber (angesichts der relativ kurzen zulässigen Speicherdauer und des Verbots der anlasslosen Auswertung) gegenüber „geheim“ geblieben wären, ihm infolge des Auskunftsverlangens nun zur Kenntnis gelangen müssen, und zwar unter gleichzeitiger voller Identifikation des Betroffenen, die dem Auftraggeber sonst bei der Auswertung meist gar nicht gelingen würde. Dieser Negativeffekt wird noch ausgeweitet, wenn Datenschutzrechte Dritter im Spiel sind, weil deren Bilddaten, die sonst geheim geblieben wären, infolge des Auskunftsbegehrens eines anderen nunmehr dem Auftraggeber der Videoüberwachung zur Kenntnis gelangen.

Die Datenschutzkommission hat in dieser Situation unter Wertung der Datenschutzinteressen aller Beteiligten die einzig angemessene Lösung darin gesehen, dass das Bestehen eines Auskunftsrechts aus nicht ausgewerteten Videoüberwachungsaufzeichnungen verneint wurde. Leider hat es der Gesetzgeber unterlassen, in der DSG-Novelle 2010 die Gelegenheit zu einer das Auskunftsrecht ausdrücklich einschränkenden gesetzlichen Regelung zu ergreifen, obwohl Art. 13 der Datenschutz-RL 95/46 ihm dazu jede Möglichkeit geboten hätte.

6.1.1.2 Zur Zulässigkeit der Datenermittlung

a) Eine größere Anzahl von Beschwerden wurden im Berichtszeitraum gegen **erkennungsdienstliche Behandlungen** nach § 65 Abs. 1 SPG erhoben. In diesem Bereich war zunächst die Zuständigkeitsabgrenzung zwischen den UVS und der Datenschutzkommission strittig bis der VwGH mit Erk. vom 19.9. 2006 klargestellt hatte, dass die Datenschutzkommission zuständig ist, wenn bei der erkennungsdienstlichen Behandlung Zwang weder angewendet noch angedroht wurde. Zur materiellen Frage, ob die Ermittlung personenbezogener Daten durch eine erkennungsdienstliche Behandlung in einem konkreten Fall zulässig ist, hat die Datenschutzkommission in Umsetzung der Judikatur des VwGH nunmehr jeweils geprüft, ob eine fallbezogene Prognose unter Berücksichtigung der Persönlichkeit des Täters und der Art des Delikts ergibt, dass der Betroffene auch in Zukunft wahrscheinlich gefährliche Angriffe begehen werde, sodass eine Vorbeugung durch eine erkennungsdienstliche Behandlung erforderlich erscheint (K121.383/0010-DSK/2008, K121.454/0005-DSK/2009 u.a.m.).

b) Bedenken hinsichtlich der Zulässigkeit der Datenermittlung sind auch im Zusammenhang mit der Eintragung von Daten in die **Zentrale Informationssammlung (ZIS) der Versicherungswirtschaft** entstanden (K121.278/0018-DSK/2007). In diesem Informationsverbundsystem werden Angaben u.a. darüber gespeichert, dass der Antrag auf Vertragsabschluss bei einer bestimmten Person von einem der teilnehmenden Unternehmen abgelehnt wurde. Auch wenn eingeräumt wird, dass keine sensiblen Daten wie etwa Gesundheitsdaten in diesem Informationsverbundsystem geführt werden, ist doch insgesamt unklar,

auf welches überwiegende berechtigte Interesse die Versicherungswirtschaft die Führung dieses Informationsverbundsystem stützen will. Die Datenschutzkommission hat daher erst unlängst im Begutachtungsverfahren über einen Entwurf einer Novelle zum Versicherungsvertragsgesetz gefordert, dass der Gesetzgeber hier eine ausdrückliche Regelung trifft, ob und inwieweit ein derartiges Informationsverbundsystem der Versicherungswirtschaft über Fälle der Ablehnung eines Vertragsabschlusses oder Abschluss mit erhöhtem Risiko geführt werden darf.

c) Immer wieder wird die Datenschutzkommission mit Beschwerden befasst, die die Unzulässigkeit der Ermittlung von Daten im Rahmen eines Ermittlungsverfahrens einer anderen Behörde behaupten, so zB im Berichtszeitraum hinsichtlich der Ermittlung von Sozialversicherungsdaten über Beschäftigungsverhältnisse im Zusammenhang mit der Frage, ob bei Zeugengebühren auch die Kosten einer Vertretung im Gewerbebetrieb zu berücksichtigen gewesen wären (121.372/0008-DSK/2008). In ständiger Rechtsprechung beurteilt die Datenschutzkommission in solchen Konstellationen nur, ob das Übermaßverbot verletzt wurde: wenn es **denkmöglich** ist, dass die ermittelten Daten nach Art und Inhalt für die Feststellung des relevanten Sachverhalts geeignet waren, ist die Zulässigkeit der Ermittlung aus datenschutzrechtlicher Sicht gegeben. Eine tiefer gehende Prüfung würde in eine Rechtmäßigkeitsprüfung des Verfahrens anderer Verwaltungsbehörden münden und damit in eine „Allzuständigkeit" der Datenschutzkommission, die dem verfassungsrechtlich verankerten Grundsatz der festen Zuständigkeitsverteilung (Verfahren vor dem gesetzlichen Richter) widerspräche (vgl. auch ausführlich K121.277/0016-DSK/2007).

d) Im Fall der Baseline-Schülertestung hatten Eltern die Datenschutzkommission angerufen, weil sie die Anonymität der getesteten Schüler und auch ihrer Familien angesichts der tief in die Privatsphäre eingreifenden Fragestellungen nicht garantiert sahen (K121.526).

Die Teilnahme der Schüler an der vom Bundesinstitut für Bildungsforschung, Innovation und Entwicklung des österreichischen Bildungswesens (BIFIE) Anfang 2009 durchgeführte Baseline-Testung war verpflichtend. Mit der Baseline-Testung führt das BIFIE in Erfüllung seines gesetzlichen Auftrags eine wissenschaftliche Erhebung in erster Linie des Wissenstandes und des Bildungsniveaus an österreichischen Schulen durch, allerdings wurde bei der gewählten Testmethode den Schülern zusätzlich zu den eigentlichen Wissensfragen ein umfangreicher Fragenbogen zur Erhebung ihrer sozialen, schulischen und familiären Situation zur Beantwortung vorgelegt. Auf diesen Fragebogen schien zwar nirgends der Name des ausfüllenden Schülers auf, doch waren sie mit einer zehnstelligen Kennnummer versehen, die einen Rückschluss auf die Schule (erste sechs Stellen), die Klasse oder Lerngruppe (siebte und achte Stelle) und die (Katalog)Nummer des ausfüllenden Schülers innerhalb der Klasse (neunte und zehnte Stelle) ermöglichte. Weiters war vom Schüler auf dem Deckblatt seines Fragebogens bei der Abgabe sein Geburtsdatum und Geschlecht einzutragen, um später dem Schüler – und nur diesem – das Ergebnis der Testung im Internet zugänglich zu machen.
Die Schule verfügte über eine Entsprechungstabelle zwischen den zehnstelligen Kennnummern und den zugehörigen Namen ihrer Schüler, um kontrollieren zu können, ob alle Schüler ihrer Teilnahmepflicht entsprochen hätten. Diese Entsprechungstabelle war von der Einsicht durch das BIFIE ausgeschlossen. Den Schulen war der Einblick in die ausgefüllten Fragebogen an sich nicht gestattet.

Diese Form der Kennzeichnung der einzelnen Schülerfragebögen hatte bei den Eltern, wie eingangs geschildert, Zweifel an der angesichts der gestellten Fragen not-

wendigen Anonymität der Fragebeantwortung erregt. Weiters wurde ins Treffen geführt, dass die Ermittlung sensibler personenbezogener Daten mit Hilfe des Fragebogens über die soziale und familiäre Situation der Schüler in Überschreitung des gesetzlichen Auftrags zur Bildungsstanderhebung gemäß § 17a SchUG, also ohne ausreichende Rechtsgrundlage geschehe. Dem hielt das BIFIE entgegen, dass das Verfahren der Baseline-Testung so ausgelegt gewesen sei, dass ausschließlich indirekt personenbezogene Daten für Zwecke einer wissenschaftlichen Untersuchung ermittelt worden wären, sodass sich die Zulässigkeit dieser Datenverwendung schon aus § 46 Abs. 1 DSG 2000 ergebe.

Die Datenschutzkommission hatte sich daher ganz grundsätzlich mit dem Begriff der „indirekt personenbezogenen Daten" auseinander zu setzen und hat hiezu Folgendes erwogen:

„Mit Hilfe der in einem konkreten Fall vorhandenen Identifikatoren soll der Verwender indirekt personenbezogener Daten „die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen" können. Es genügt hierbei nicht, dass der Datenverwender die Identität der Betroffenen nicht bestimmen darf, sondern dass er sie auch tatsächlich nicht bestimmen kann, ohne rechtlich verpönte Mittel anzuwenden, wie etwa Einbruch, Diebstahl, Zwang oder Bestechung, um den Re-Identifikationsschlüssel zu erlangen. Dass die Definition des § 4 Z 1 DSG 2000 im Sinne des Erfordernisses einer ausreichenden faktischen (technisch-organisatorischen) Absicherung der Daten gegen die Möglichkeit missbräuchlicher Re-Identifikation verstanden werden muss, wird auch aus dem Zweck der Schaffung dieses Begriffs klar: Die Verwendung „indirekt personenbezogener Daten" ist im DSG 2000 vielfach privilegiert (vgl. die §§ 8 Abs. 2, 9 Z. 2, 12 Abs. 3 Z 2, 17 Abs. 2 Z 3 usw.) – dies ist nur dadurch gerechtfertigt, dass ein datenschutzrechtliches Risiko für die Betroffenen dadurch weitestgehend ausgeschaltet ist, dass missbräuchliche Re-Identifikation für den Verwender angesichts der konkret angewendeten Pseudonymisierungsmethode praktisch nicht möglich ist."

Die Datenschutzkommission sah im vorliegenden Fall eine Verletzung im Recht auf Geheimhaltung deshalb gegeben, weil die zur Individualisierung innerhalb der Gruppe verwendeten Daten ‚Katalognummer', ‚Geburtsdatum' und ‚Geschlecht' bei einer Befragung der Gruppenmitglieder (Schulklasse, Lerngruppe) mit hoher Wahrscheinlichkeit zur eindeutigen Identifikation der jeweils Betroffenen führen würden: Die Gruppe umfasste maximal 30 Personen, die durch das Merkmal „Geschlecht" regelmäßig wesentlich verkleinert – im Durchschnittsfall halbiert – wird, wobei das Geburtsdatum im Klassenverband vielfach bekannt ist und die Katalognummer, die regelmäßig die Stellung des Namens im Alphabet wieder spiegelt, in Zweifelsfällen zusätzlich zur Identifikation beiträgt. Damit kann nicht vom Ermitteln bloß indirekt personenbezogener Daten ausgegangen werden, da die Möglichkeit der missbräuchlichen Identifikation von Betroffenen mit Hilfe der ermittelten Identifikationskriterien keineswegs faktisch unmöglich ist. Damit kann aber auch § 46 Abs. Z 3 DSG 2000 nicht als Rechtsgrundlage für die Verwendung der Daten herangezogen werden, womit es überhaupt an einer tauglichen Rechtsgrundlage fehlt (§ 9 DSG 2000 sieht keinen Rechtfertigungsgrund vor). Wiewohl dem BIFIE die Fragebögen niemals zugingen, war die Verletzung im Recht auf Geheimhaltung schon durch die rechtswidrige Ermittlung von personenbezogenen Daten verwirklicht.

6.1.1.3 Zum Umfang des Löschungsrechts

a) Mehrere Beschwerden wurden mit dem Begehren erhoben, dass im Falle der Einstellung eines Strafverfahrens oder der Verfahrensbeendigung durch **Freispruch** alle darauf Bezug habenden **Akten** bei den Strafverfolgungsbehörden **zur Absicherung der Unschuldsvermutung gelöscht** werden müssten.

Tatsächlich gibt es keine ausdrückliche gesetzliche Bestimmung darüber, wie lan-

ge kriminalpolizeiliche Akten über Ermittlungen im Dienste der Strafjustiz aufzubewahren sind. Es gibt vielmehr nur die allgemeine Bestimmung des § 6 Abs. 1 Z 5 DSG 2000, wonach Daten zu löschen sind, sobald sie für die Erreichung der Zwecke, für die sie ermittelt wurden, nicht mehr benötigt werden.

Die Datenschutzkommission hat dem Löschungsbegehren nicht stattgegeben, da mit Abschluss eines (Straf)Verfahrens die Notwendigkeit zur Aufbewahrung von Verfahrensdaten in aller Regel nicht erschöpft ist: Zum einen ist es im Interesse des Betroffenen selbst notwendig, dass die Einstellung oder der Freispruch dokumentiert und damit nachweisbar ist. Zum anderen muss die Rechtmäßigkeit staatlichen Handelns nachprüfbar sein, was die Aufbewahrung von Akten für einen gewissen Zeitraum über den Abschluss eines Verfahrens hinaus erfordert. Das von den Beschwerdeführern eigentlich verfolgte Ziel, die Heranziehung von alten Verfahrensakten für neuerliche Verdachtsfälle gegenüber derselben Person zu unterbinden, müsste auf andere Weise als durch Aktenvernichtung gewährleistet werden, nämlich durch entsprechende Weiterverwendungsbeschränkungen für Verfahrensdaten. (vgl. zB K121.407/0001-DSK/2009 oder K121.390/0001-DDSK/2009). Der VfGH hat diese Auffassung in der Zwischenzeit bestätigt (vgl. etwa B 298/09-13). Der VwGH ist der Ansicht des VfGH gefolgt (VwGH in 2009/17/0064). Die im Zusammenhang mit dem außergewöhnlichen Fall des wegen Grundrechtswidrigkeit aufgehobenen Straftatbestands des § 209 StGB vom VfGH bejahte grundsätzliche Löschungsverpflichtung für Ermittlungsdaten kann somit nicht generalisierend angewendet werden.

b) Ein überwiegendes berechtigtes **Dokumentationsinteresse** hat die Datenschutzkommission im Übrigen auch den kirchlichen Matrikelbüchern gegenüber dem Begehren eines ausgetretenen Kirchenmitglieds auf Löschung aller Daten über seine Taufe zuerkannt (K121.309/0010-DSK/2007).

6.1.1.4 Zur Bestimmung des (rechtmäßigen) Auftraggebers

a) Im Zusammenhang mit der Bonitätsprüfung in Form der Errechnung sogenannter „Scoring-Werte“ hat sich mehrfach die Frage gestellt, wer hier als Auftraggeber zur Auskunft verpflichtet wäre. Einige Unternehmen, für deren Zwecke die Bonitätsprüfung stattgefunden hat, haben eine Auskunftserteilung mit der Begründung abgelehnt, sie hätten keine Daten, insbesondere keine Scoring-Werte gespeichert, sondern bekämen den Scoring-Wert jeweils von einer Kreditauskunftei, deren Kunde sie selbst seien, geliefert.

Unabhängig davon, bei wem die **Scoring-Werte** gespeichert sind bzw. errechnet werden – dies kann auch bei einem Dienstleister geschehen -, ist ein Unternehmen zB der warenkreditgebenden Branche oder der Telekom-Branche dann als **Auftraggeber des Systems** für die Errechnung von Scoring-Werten für seine präsumtiven Vertragspartner anzusehen, wenn die Parameter der Bonitätsbeurteilung, also die Kriterien und ihre Wertigkeit, von diesem Unternehmen selbst festgelegt wurden. Hinsichtlich der Bedeutung eines Scoring-Wertes muss der Auftraggeber des Scoring-Systems Auskunft geben. Diese Sichtweise wurde in der Zwischenzeit auch höchstgerichtlich bestätigt.

Falls in einem Scoring-System auch Informationen verwendet werden, die von einer Kreditauskunftei übermittelt wurden, hat der Auftraggeber des Scoring-Systems dies in der Auskunft über die Herkunft der Daten offen zu legen.

b) Ob **Gemeinden** als **Auftraggeber** einer Datenermittlung in Form der **Videoüberwachung zwecks Geschwindigkeitskontrolle im Straßenverkehr** auftreten dürfen, war Gegenstand der unter K121.359/0016-DSK/2008 ergangenen

Entscheidung: Gemeinden haben für sich die Berechtigung zur Vornahme solcher Überwachungen in Anspruch genommen. Gestützt wurde dies unter anderem auch auf das Argument, dass sie hiebei nur indirekt personenbezogene Daten ermitteln würden, da sie keinen Zugang zum Kraftfahrzeugregister zwecks Identifizierung der Kraftfahrzeughalter hätten. Diese werde jeweils erst von der Bezirkshauptmannschaft aufgrund der Anzeigen der Gemeinde vorgenommen.

Die Datenschutzkommission hat hinsichtlich der Frage, ob nur indirekt personenbezogene Daten ermittelt würden, darauf verwiesen, dass nach dem Zweck der Datenermittlung – Bestrafung von „Schnellfahrern" – zweifellos Daten über Personen mit der Intention ihrer Identifizierung ermittelt würden; es würden daher Daten über identifizierbare Personen ermittelt, wofür alle Verwendungsbeschränkungen des DSG 2000 zu beachten wären. Davon ausgehend sei festzustellen, dass es einer Gemeinde an einer gesetzlichen Zuständigkeit für die Datenermittlung im Wege der Verkehrsüberwachung mangle, da Verkehrsüberwachung die gesetzliche Aufgabe der Bezirksverwaltungsbehörden sei (- eine ausnahmsweise Betrauung der Gemeinde nach der StVO lag im Anlassfall nicht vor).

Gegen diesen Bescheid hat die beschwerdegegnerische Gemeinde Beschwerde an den Verwaltungsgerichtshof erhoben, was zur Aufhebung des Bescheids der Datenschutzkommission führte (VwGH Zl 2008/17/0152-4) und zwar deshalb, weil die Datenschutzkommission nicht geprüft hätte, ob die Radarmessungen nicht im Rahmen der Privatwirtschaftsverwaltung der Gemeinde erfolgt seien. In dem (im Juni 2010 ergangenen) Ersatzbescheid der Datenschutzkommission (K121.359/0007-DSK/2010) wird dieser Frage breiter Raum gewidmet und zu dem Schluss gelangt, dass die Zuständigkeit zur Vornahme einer Tätigkeit („punktuelle Radarmessungen"), die durch § 98b StVO ausdrücklich der Bezirksverwaltungsbehörde übertragen wird, nicht von einer anderen Behörde im Rahmen der Privatwirtschaftsverwaltung beansprucht werden kann.

c) Von grundsätzlicher Bedeutung scheint auch die in K121.446/006-DSK/2009 geäußerte Rechtsansicht der Datenschutzkommission, dass die **Ausübung des Weisungsrechts** einer übergeordneten Behörde gegenüber der untergeordneten Behörde nicht den **Übergang der datenschutzrechtlichen Auftraggebereigenschaft** bewirkt: Auch die aufgrund einer Weisung tätige Behörde handelt im eigenen Namen und nimmt dadurch die Auftraggebereigenschaft in Anspruch. Das Problem, wer von zwei durch einen Weisungszusammenhang verbundenen Behörden rechtmäßiger Auftraggeber ist, war auch im Fall K121.533 zu behandeln: Ein Bundesministerium darf nicht als Auftraggeber einer Datenanwendung auftreten, wenn das Gesetz diese Rolle ausdrücklich einer dem BMium weisungsunterstellten Behörde zuschreibt.

6.1.2 Bereiche, in welchen Beschwerden gehäuft vorgebracht wurden

6.1.2.1 Bonitätsdatenbanken

Ein erheblicher Teil von Beschwerden im Berichtszeitraum hat sich wiederum auf den Sektor der Anbieter von Kreditinformation (Kreditauskunfteien gemäß § 152 GewO 1994) bezogen.

Vielfach handelte es sich um Beschwerden über die **Verletzung des Auskunftsrechts.** Dabei waren auch durchaus kuriose Fälle zu behandeln, wie zB, dass das Recht auf eine kostenlose Auskunftserteilung pro Jahr auch das Recht mitumfasst, dass die Auskunft frei von Portokosten zugesendet wird (K121.521/0007-DSK2009), oder dass ein Verstoß gegen den Grundsatz von Treu und Glauben (§ 6 Abs. 1 Z1 DSG 2000) vorliegt, wenn der Auftraggeber einer Bonitätsdatenbank Daten sofort

löscht, nachdem ihm sein Dienstleister mitgeteilt hat, dass ein Auskunftsbegehren irrtümlich beim Dienstleister gestellt worden sei und dieser den Auskunftswerber an den Auftraggeber verwiesen habe (K.121.524/0011-DSK/2009). Gegen den Grundsatz von Treu und Glauben verstößt der Auftraggeber einer Bonitätsdatenbank auch dann, wenn er – ohne dem Auskunftswerber die Möglichkeit einer Nachbesserung zu geben - keine Auskunft erteilt, weil der Identitätsnachweis nicht lesbar sei, oder wenn er argumentiert, dass er keine Daten über den Auskunftswerber verarbeite, weil zwar eine Person mit demselben Vor- und Nachnamen in seiner Datenbank enthalten sei, für diese aber eine andere Adresse angegeben sei als beim Auskunftswerber (K121.344).

Zahlreiche Beschwerden im Bereich der Bonitätsdatenbanken betrafen auch eine behauptete **Verletzung des Rechts auf Widerspruch nach § 28 Abs. 2 DSG 2000**: Diese Bestimmung sieht vor, dass jedermann, dessen Daten in einer öffentlich zugänglichen Datei dargeboten werden, ohne dass hiezu eine gesetzliche Duldungspflicht besteht, dagegen Widerspruch erheben kann, der nicht weiter begründet werden muss und die Pflicht des Auftraggebers zur Löschung der Daten aus der öffentlichen Datei zur Folge hat. Nachdem diese Möglichkeit publik geworden ist und der OGH auch ausgesprochen hat, dass die allfällige Entgeltlichkeit des Zugangs zu einer Bonitätsdatenbank ihre „Öffentlichkeit“ nicht verhindert, solange nur jedermann, der bereit ist, das Entgelt zu bezahlen, Zugang hat, haben viele Personen Widerspruch nach § 28 Abs. 2 DSG 2000 gegen die Führung ihrer Daten in einer Bonitätsdatenbank erhoben und haben eine Prüfung bei der Datenschutzkommission nach § 30 DSG 2000 angeregt, wenn diesem Widerspruch nicht innerhalb von 8 Wochen durch Löschung entsprochen wurde.

Freilich muss eingeräumt werden, dass diese rechtliche Möglichkeit des Widerspruchs das Problem der Verfügbarkeit verlässlicher Bonitätsinformation nicht löst – notwendig wäre vielmehr eine spezialgesetzliche Regelung des datenschutzrechtlichen Rechtsrahmens für die Ermittlung und Darbietung von Bonitätsinformation, wie dies die Datenschutzkommission bereits in ihrem vorigen 12. Bericht 2007 gefordert hat.

6.1.2.2 Sicherheits- und Kriminalpolizei

Ein merkbarer Prozentsatz der Datenschutzbeschwerden richtet sich erfahrungsgemäß immer gegen Sicherheitsbehörden, was angesichts des besonderen Nachteilpotentials der von diesen Behörden verarbeiteten Daten nicht verwundert. Im hier gegenständlichen Berichtszeitraum 2007-2009 hat sich der Erfahrungstrend ohne zahlenmäßige Besonderheiten fortgesetzt.

Am häufigsten wurden Beschwerden zu dem bereits weiter oben (6.1.1.3) erörterten Thema der **Löschung von Akten und Aktenindizierungsbehelfen** erhoben sowie Beschwerden gegen die **Zulässigkeit von erkennungsdienstlicher Behandlung** nach dem SPG (siehe 6.1.1.2).

Seit Inkrafttreten der StPO-Novelle mit 1.1.2008 muss hinsichtlich des datenschutzrechtlichen **Rechtsschutzweges** zwischen **sicherheitspolizeilicher und kriminalpolizeilicher Tätigkeit der Organe der Sicherheitsbehörden klar unterschieden** werden. So war im Fall K121.476 die Beschwerde gegen die Datenermittlung durch Photographieren einer Beschuldigten von der Datenschutzkommission mangels Zuständigkeit zurückzuweisen, da diese Handlung unter den Tatbestand der kriminalpolizeilichen Identitätsfeststellung gemäß §§ 117 ff StPO zu subsumieren war. Der dafür vorgesehene Rechtsschutzweg wäre der Einspruch an das Gericht gegen eine Ermittlungsmaßnahme gemäß § 106 Abs. 1 Z 2 StPO gewesen. Die datenschutzrechtliche Beschwerde gemäß § 90 SPG war daher nicht

zulässig, da keine Daten „in Angelegenheiten der Sicherheitsverwaltung“ verwendet wurden.

In einem anderen Fall (K121.279/0017-DSK/2007) hat die Datenschutzkommission eine **überschießende Datenermittlung im Internet** durch eine Sicherheitsbehörde festgestellt: Zum einen sei der Betreiber eines Chatrooms nicht als „Betreiber eines öffentlichen Telekommunikationsdienstes“ anzusehen, weshalb er auch nicht zur Auskunft darüber verpflichtet werden könne, welche IP-Adresse einem im Chatroom verwendeten „nickname“ zu einem bestimmten Zeitpunkt zugeordnet gewesen sei; zum anderen könne die (dynamische) IP-Adresse als Verkehrsdatum selbst bei äußerster Ausdehnung des Wortlauts der Eingriffsnorm des § 53 Abs. 3a SPG (alte Fassung) nicht unter „Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses“ subsumiert werden. Die gegen diesen Bescheid erhobene Amtsbeschwerde des BMI wurde vom Verwaltungsgerichtshof abgewiesen (Erkenntnis des VwGH vom 27. 5. 2009, 2007/05/0280). Daraufhin wurden die Datenermittlungsbefugnisse der Sicherheitsbehörden im Internet durch BGBl. I Nr. 114/2007 deutlich erweitert.

6.1.2.3 Parlamentarische Anfragen

Diesbezüglich sind die eingegangenen Beschwerden zwar nicht besonders zahlreich, doch scheinen sie erwähnenswert, weil dadurch eine Rechtsschutzlücke aufgezeigt wird:

Datenschutzrechtliche Verstöße innerhalb der drei Staatsgewalten Verwaltung, Gerichtsbarkeit und Gesetzgebung sind noch immer nicht gleichermaßen ahndbar: Während die Verwaltung unter der datenschutzrechtlichen Kontrolle der Datenschutzkommission steht und für die Gerichtsbarkeit ein eigenes datenschutzrechtliches Kontrollregime durch die §§ 83 ff GOG geschaffen wurde, fehlen entsprechende Rechtsschutzmechanismen für den Bereich behaupteter Datenschutzverletzungen durch Gesetzgebungsorgane. Beschwerdeführer haben sich daher mehrfach auch an die Datenschutzkommission gewendet, die jedoch immer nur ihre Unzuständigkeit feststellen konnte und derartige Beschwerden daher zurückweisen musste. (Vgl. etwa K121.535/0004-DSK/2009 und VfGH B1048/09-6.

6.1.3 Anmerkungen zum Beschwerdeerfolg

a) Eine Sichtung der formalen Verfahrensergebnisse bei Beschwerden nach § 31 DSG 2000 zeigt einen weit überwiegenden Anteil von abweisenden oder zurückweisenden Entscheidungen der Datenschutzkommission. Dies darf jedoch aus folgenden Gründen nicht täuschen:

Das Ziel eines Verfahrens nach § 31 DSG 2000 ist die Herstellung des vom Beschwerdeführer verlangten Zustands, soweit sein Begehren berechtigt war. Wenn dieser Zustand im Zeitpunkt der Entscheidung der Datenschutzkommission (Bescheiderlassung) noch nicht erreicht ist, wird daher bei Auftraggebern des privaten Bereichs ein Leistungsauftrag zu erteilen sein, bei Auftraggebern des öffentlichen Bereichs hingegen die Feststellung genügen, dass der festgestellte Zustand rechtswidrig ist – gemäß § 40 Abs. 4 DSG 2000 hat die belangte Behörde die Rechtsansicht des Datenschutzkommission umgehend umzusetzen.

Sehr oft kommt es jedoch dazu, dass der Beschwerdegegner durch das Verfahren sich des rechtswidrigen Zustands erst bewusst wird und sodann – noch während laufenden Verfahrens – den vom Beschwerdeführer gewünschten Zustand herstellt, indem er zB nun Auskunft erteilt. Damit ist aber der Verfahrenszweck erreicht, dem Beschwerdeführer fehlt in der Folge ein weiteres Rechtsschutzinteresse und das Verfahren könnte beendet werden.

Nach der im Berichtszeitraum geltenden Rechtslage konnte eine Einstellung des Verfahrens jedoch nur erfolgen, wenn der Beschwerdeführer vorher seine Beschwerde zurückzog. In allen Fällen, in welchen der Beschwerdeführer dazu nicht bereit war (vielfach auch aus mangelndem Interesse, sobald er seinen Zweck erreicht hatte), hatte die Datenschutzkommission entsprechend der einschlägigen Judikatur des VwGH die – aufrechte – Beschwerde wegen nunmehr mangelndem Rechtsschutzinteresse mit Bescheid zurückzuweisen. D. h. dass Auskunftsbeschwerden in der weit überwiegenden Zahl zum Erfolg führen, auch wenn dies aus der formalen Art der Verfahrensbeendigung (früher: Zurückweisung, seit 1.1.2010: Einstellung) nicht erkennbar hervorgeht.

§ 31 DSG 2000 ermächtigt jedenfalls – entgegen dem häufig erkennbaren Wunsch der Beschwerdeführer – die Datenschutzkommission *nicht* zur bescheidmäßigen Feststellung, dass ein Verhalten rechtswidrig *war*, wenn es rechtzeitig vor Schluss des Verfahrens beendet und damit die Sachlage saniert wurde.

b) Häufige Gründe dafür, dass Beschwerden tatsächlich nicht zum Erfolg führen, ist bei Auskunfts-, Richtigstellungs- oder Löschungsbeschwerden etwa das Fehlen eines vorherigen Begehrens an den Auftraggeber oder eines tauglichen Identitätsnachweises.
Kein Erfolg ist einer Beschwerde auch dann beschieden, wenn sie sich auf nicht speziell strukturierte Datensammlungen in Papier bezieht (- so war etwa die Auskunftserteilung aus einer Maturaarbeit abzulehnen, K121.427/0003-DSK/2009).

Oft wird unter Berufung auf § 26 DSG 2000 auch Auskunft über Dinge verlangt, die in § 26 Abs. 1 nicht erwähnt sind und deren Offenlegung daher vom datenschutzrechtlichen Auskunftsrecht nicht erfasst ist.

Bei Löschungs- und Richtigstellungbegehren wird oft vergessen, dass die Datenschutzkommission diesbezüglich im privaten Bereich keine Zuständigkeit zur Durchführung förmlicher Beschwerdeverfahren nach § 31 DSG 2000 besitzt.

Generell besitzt die Datenschutzkommission keine Zuständigkeit für die Behandlung behaupteter Datenschutzverstöße durch Organe der Gesetzgebung oder der Gerichtsbarkeit; dies betrifft zB auch kriminalpolizeiliche Handlungen, da sie den Strafgerichten zuzurechnen sind.

6.2 Kontrollverfahren nach § 30 DSG 2000

6.2.1 Vorbemerkungen

Über die nach § 31 DSG 2000 zur Verfügung stehenden förmlichen Rechtsmittel hinaus bietet § 30 Abs. 1 DSG 2000 jedermann die Möglichkeit, sich wegen einer – ihn selbst betreffenden – behaupteten Verletzung von Rechten oder Pflichten nach dem DSG 2000 auch in einem sogenannten „Ombudsmann-Verfahren“ an die Datenschutzkommission zu wenden: Damit können zwar keine vollstreckbaren Entscheidungen erlangt werden, doch gelingt es der Datenschutzkommission meist, ein für den einschreitenden Bürger zufriedenstellendes Ergebnis im Konsensweg zu erzielen. Diese Verfahrensart ist auch im gesamten privaten Bereich anwendbar und ersetzt in der Praxis oft die Durchsetzung von Datenschutzrechten gegenüber Auftraggebern des privaten Bereichs vor den ordentlichen Gerichten.

Die Datenschutzkommission kann jedoch auch ohne Vorliegen einer Eingabe eines Betroffenen von sich aus Datenanwendungen auf ihre Rechtmäßigkeit überprüfen - bei vorabkontrollpflichtigen Datenanwendungen sogar ohne dass ein konkreter Verdacht auf Mängel der zu prüfenden Datenanwendung bei der Datenschutzkommission schon vorhanden sein müsste. In derar-

tigen Kontrollverfahren stehen die Mittel des Augenscheins, der Anforderung von Auskünften oder Unterlagen und die testweise Inbetriebnahme von Datenverarbeitungsanlagen zur Verfügung.
Ziel des Verfahrens nach § 30 DSG 2000 ist die Herbeiführung eines rechtmäßigen Zustands. Dazu können vielfache Mittel angewendet werden, u.a. die Wiedereröffnung des Registrierungsverfahrens, nötigenfalls auch eine Anzeige an die zuständige Strafbehörde. Es kann auch eine Empfehlung ausgesprochen werden. Empfehlungen sind – wie schon der Name sagt, zwar nicht unmittelbar verbindlich, doch wäre im öffentlichen Bereich die Durchsetzung einer solchen Empfehlung letztlich doch im Umweg über die politische Verantwortung des obersten zuständigen Organs erzielbar. Im privaten Bereich hat die Datenschutzkommission die Möglichkeit der Klageerhebung vor dem zuständigen ordentlichen Gericht, wodurch ein exekutierbares Urteil erwirkt werden kann. Unter bestimmten Voraussetzungen kann bei Gefahr im Verzug die Führung einer gemeldeten Datenanwendung vorläufig untersagt werden (§ 20 Abs. 2 DSG 2000 in der derzeit noch anwendbaren Fassung).

6.2.2 Zu einzelnen Kontrollverfahren

Im Berichtszeitraum sind berichtenswerte Empfehlungen u.a. betreffend den Sektor der Arbeitsmarktverwaltung und der Schulverwaltung ergangen.

6.2.2.1 Arbeitsmarktservice

In diesem Bereich kommt es erfahrungsgemäß häufig zu Datenschutzbeschwerden. Dies deshalb, weil zwischen dem Arbeitsuchenden und den Vermittlern des Öfteren sehr unterschiedliche Auffassungen über die Richtigkeit und die Maßgeblichkeit der Vermittlungsdaten bestehen: Die Beschwerden aus diesem Bereich bestreiten häufig die Richtigkeit der von den Betreuern gemachten Aufzeichnungen über die Arbeitssuchenden.

Beschwerdeverfahren betreffend das AMS haben mehrfach auch zu Empfehlungen der Datenschutzkommission geführt:
Diese Empfehlungen betrafen die **Art der Kommunikation** zwischen Betreuer und Arbeitssuchendem (vgl. etwa die Empfehlung K210.579/0004-DSK/2008 über die Führung von Beratungsgesprächen in akustisch abgeschirmten Bereichen) aber auch die Weitergabe von Daten über Arbeitssuchende an die zwecks Schulung herangezogenen privaten Institutionen. Diese privaten Institutionen sind als **Dienstleister des AMS** zu sehen, weshalb an sich ein Datenaustausch zwischen AMS und Schulungsinstitution zulässig ist, doch muss sich der Umfang des Datenaustausches an dem Schulungsgegenstand einschränkend orientieren (vgl. hiezu auch die Empfehlung K210.583/0009-DSK/2008).

6.2.2.2 Schulverwaltung

a) Ein Fall von generellem Interesse betraf die Weitergabe von Gesundheitsdaten der Schüler und Eltern vom Schularzt an den Magistrat der Stadt Wien (K210.633):

Im Rahmen der schulärztlichen Untersuchungen haben die Eltern neben dem Gesundheitsblatt für den Schüler auch einen ‚Elternfragebogen' mit einigen Frage zur Gesundheit der Eltern auszufüllen. Dieser enthielt zum Zeitpunkt der Beschwerdeerhebung eingangs folgende Erklärung: „Ihre Angaben sind nur für die Schulärztin/den Schularzt bestimmt. Sie werden **streng vertraulich** behandelt und sollten in Ihrem eigenen Interesse in einem **Kuvert verschlossen der Schulärztin/dem Schularzt** übermittelt werden….". Am Ende des Formulars waren das „Bundesministerium für Gesundheit und Frauen" und das „Bundesministerium für Bildung, Wissenschaft und Kultur", jeweils mit einer DVR-Nummer genannt. Ein Hinweis auf andere Behörden als allenfalls

Verantwortliche für die Datenerhebung fanden sich im Formular nicht.

Im April 2009 richtete die Leiterin des Schulärztlichen Dienstes, der eine Organisationseinheit der MA 15 darstellt, ein Ersuchen an alle städtischen SchulärztInnen, die Gesundheitsblätter sowie die Elternfragebögen sämtlicher Schüler bestimmter Schulstufen in einem verschlossenem Kuvert an sie zu übermitteln zwecks Erstellung des Wiener Kindergesundheitsberichts, für den die MA 15 als Bezirksverwaltungsbehörde (Gesundheitsamt) verantwortlich ist.

Kern der Beschwerde war, dass diese Weitergabe der Elternfragebögen im Widerspruch zu den eingangs zitierten Angaben auf dem Fragebogen über die Zweckbestimmung und Vertraulichkeit der ermittelten Daten stehe.

In der Sache untersuchte die Datenschutzkommission das Vorliegen einer Rechtsgrundlage für die gegenständliche Weitergabe, da § 1 Abs. 2 DSG 2000 für Eingriffe in das Grundrecht auf Datenschutz durch eine staatliche Behörde stets eine Rechtsgrundlage in Form eines Gesetzes im formellen Sinn fordert. Zunächst musste dazu geprüft werden, ob überhaupt ein Eingriff in das Grundrecht in Form einer „Übermittlung“ (§ 4 Z 12 DSG 2000) vorliege.

Die Datenschutzkommission kam zu dem Schluss, dass keine Übermittlung von Daten vorlag: Erstens ist der schulärztliche Dienst von den bei den Bezirksverwaltungsbehörden eingerichteten Gesundheitsämtern (hier: die MA 15) zu besorgen (§ 3 Abs. 1 Z I lit. d des Gesetzes über die Vereinheitlichung des Gesundheitswesens), die gleichzeitig für die Ausarbeitung des Kindergesundheitsberichts zuständig sind; es handelte sich also um eine Datenverwendung innerhalb derselben Behörde. Zweitens geschah die Verwendung der Gesundheitsdaten aus den schulärztlichen Untersuchungen für den Kindergesundheitsbericht, stellte also auch keinen Zweckwechsel dar, dem die rechtliche Qualität einer „Verwendung für ein anderes Aufgabengebiet“ iSd des § 4 Z 12 DSG 2000 zukäme, vielmehr sind beide Aktivitäten gleichermaßen dem Teilaufgabengebiet „(gesundheitliche) Vorsorge für Kinder und Jugendliche“ zuzurechnen. Eine Übermittlung iSd § 4 Z 12 DSG 2000 war damit nicht gegeben, sodass die in der Beschwerde gerügte Datenweitergabe auch keiner besonderen Rechtsgrundlage bedurfte – sie war vielmehr als zulässig zu werten, da die Ermittlung bestimmter gesundheitlicher Grunddaten der Eltern als wesentlich für die – auch prognostische – Beurteilung der gesundheitlichen Situation des Kindes ist: Die Frage nach familiären gesundheitlichen Vorprägungen gehört nach dem Stand der medizinischen Wissenschaft zum unverzichtbaren Teil eines Anamnese, wie sie bei den Reihenuntersuchungen der Schüler zu erfolgen hat, und ist damit schon durch § 9 Z 12 DSG 2000 iVm § 58 und § 66 SchUG gedeckt.

Die Beschwerde selbst war daher abzuweisen. Anzuerkennen war jedoch, dass die auf dem Elternfragebogen enthaltenen Informationen insbesondere zur Frage des Auftraggebers oder zu allfälligen die ärztliche Vertraulichkeit durchbrechenden weiteren Datenverwendungen irreführend sind, weshalb die Datenschutzkommission sich veranlasst sah, in einem nachfolgenden amtswegigen Verfahren nach § 30 Abs. 2 DSG 2000 die Empfehlung an die MA 15 auszusprechen, sie möge in den bei den schulärztlichen Untersuchungen verwendeten Elternfragebögen eine den §§ 24 und 25 DSG 2000 genügende Information erteilen (Empfehlung der Datenschutzkommission vom 16. 12. 2009, GZ K210.633/0007-DSK/2009). Diese Information müsse a) jedenfalls den Auftraggeber der Datenermittlung samt seiner DVR-Nummer nennen (dies war durch die Nennung von Ministerien auf dem in Verwendung gestandenen Frageboden nicht erfüllt) und b) jedenfalls alle Zwecke der Verwendung der ermittelten Daten aufzählen. Auf die Weiterverwendung der Daten für Zwecke des Kindergesundheitsberichts sei hinzuweisen und die Formulierung des

Einleitungssatzes („Ihre Angaben sind nur für die Schulärztin/den Schularzt bestimmt. Sie werden streng vertraulich behandelt“) entsprechend anzupassen.

b) Zur Frage einer künftigen datenschutzrechtlich adäquaten Vorgangsweise der Kennzeichnung der getesteten Schüler im Rahmen der Baseline – Studien hat die Datenschutzkommission dem BIFIE Empfehlungen erteilt (K213.031): Jener Teil des Codes, der es dem getesteten Schüler ermöglichen soll, das Ergebnis seiner Testung im Internet einzusehen, sollte nach dem Zufallsprinzip, am besten vom Schüler selbst erzeugt (zB durch Ziehen eines Zettels mit einer Zahl aus einer Urne) und auf dem Fragebogen aufgebracht werden. Hiebei wären die Schüler in altersgerechter Form darüber zu belehren, dass dieser Code(teil) geheim gehalten und sicher aufbewahrt werden muss, damit nur die Schüler selbst (und ihre Eltern) vom Ergebnis des Tests Kenntnis erhalten können. Der Ablauf der Datenverwendung für Zwecke der Erhebung von Bildungsstandards (Schülerbefragung und „Baseline-Testung“) ist allen Betroffenen außerdem vorab oder aus Anlass der Datenerhebung umfassend und in verständlicher Weise schriftlich darzulegen. Dies betrifft auch die Art und Weise der Bildung der Kennzahlen und Codes und ihre Bedeutung.

6.2.2.3 Private Personenversicherungen

Die Datenschutzkommission setzte 2008 auch einen Schwerpunkt durch Prüfung des Umgangs mit personenbezogenen Daten in der Personenversicherung (Lebens-, Kranken- und Unfallversicherung). Dabei wurden drei Versicherungsunternehmen, die nach bestimmten Kriterien (Größe des Unternehmens, Unternehmenssitz) ausgewählt wurden, vor Ort geprüft. Schon im Vorfeld der Prüfung vor Ort konnte sich die Datenschutzkommission ein Bild von der Tätigkeit und dem Umgang mit personenbezogenen Daten machen. Sowohl während der Prüfung als auch in der nachfolgenden Korrespondenz ist es – auch aufgrund der Bereitschaft zur Zusammenarbeit – der Datenschutzkommission gelungen, einige mit dem Datenschutzrecht nicht vereinbare Praktiken aufzuzeigen und die Herstellung des rechtmäßigen Zustandes zu bewirken bzw. einzuleiten. In einigen wesentlichen Punkten wäre allerdings eine Verbesserung der gesetzlichen Rechtslage notwendig.

Neben Unzulänglichkeiten im Bereich der organisatorischen Abwicklung, des Zugangs zu und der Protokollierung von Zugriffen auf personenbezogene Gesundheitsdaten, der Löschung von Daten (und damit verbunden entsprechender Löschungsregelungen), die umgehend behoben wurden, wurden Probleme bei der Gültigkeit von Zustimmungserklärungen der Versicherungsnehmer zur Einholung von Gesundheitsdaten von Dritten (Ärzten, Krankenhäusern) sowie bei Meldungen an das Datenverarbeitungsregister iSd §§ 17ff DSG 2000 festgestellt.

Besonderes Augenmerk wurde auch auf das Zentrale Informationssystem (ZIS) der Versicherungsgesellschaften gelegt, in welchem Personenversicherungsanträge, die ua. abgelehnt oder nur zu erschwerten Bedingungen angenommen wurden, eingetragen werden, um Versicherungsshopping zu vermeiden. Nähere Details des Versicherungsantrags oder -verhältnisses finden sich im ZIS nicht.

Soweit die getroffenen Feststellungen nicht nur die geprüften Unternehmen, sondern die gesamte Branche betrafen, wurde auch der Verband der Versicherungsunternehmen Österreichs in die Diskussionen eingebunden. Insbesondere zur Frage des Umgangs mit dem ZIS sowie zur Verbesserung des § 11a VersVG als Rechtsgrundlage für Übermittlungen von Gesundheitsdaten von behandelnden Gesundheitsdienstanbietern an die Versicherer fanden Beratungen statt, deren Ergebnis dem zuständigen Bundesministerium für Justiz zur Verfügung gestellt wurde. Hiezu ist in der Zwischenzeit vom BMJ der Entwurf einer Novelle zum Versicherungsvertragsgesetz

im Begutachtungsverfahren vorgelegt worden.

6.3 Genehmigungsverfahren für internationalen Datenverkehr nach § 13 DSG 2000

Im Berichtszeitraum hatte die Datenschutzkommission zahlreiche Anträge zur Erteilung von Genehmigungen für den Internationalen Datenverkehr (§ 13 DSG 2000) zu bearbeiten, die im Übrigen fast ausschließlich österreichische Tochterunternehmen internationaler Konzerne betrafen.

Bei den Anträgen waren zwei große Gruppen zu unterscheiden: Anträge auf Weitergabe von Daten an Dienstleister im Ausland und Anträge auf Übermittlung an andere Auftraggeber (meist Konzernfirmen) im Ausland.

6.3.1 Anträge auf Genehmigung der Überlassung von Daten ins Ausland

Viele Konzerne setzen Dienstleister zur effizienten Führung ihrer Datenanwendungen, zur Softwareerstellung und -wartung sowie zur Datenerfassung ein. Die häufigsten Empfängerländer sind die USA (oft am Sitz des Konzerns), Indien, Malaysia und andere Staaten in Asien. Manche Konzerne betreiben komplexe Systeme mit Dienstleistern in verschiedenen Ländern.

Die meisten Überlassungen sind gemäß § 13 DSG 2000 genehmigungspflichtig. Die in § 12 Abs. 3 DSG 2000 vorgesehenen Fälle der Genehmigungsfreiheit sind auf Dienstleistungen kaum anwendbar.

Die Probleme bei Genehmigungsverfahren für Dienstleistungen im Ausland lagen sehr oft an mangelden Meldungen jener Datenanwendungen, aus welchen Daten überlassen werden sollen, und nicht so sehr in der Heranziehung eines Dienstleisters außerhalb des EWR. Die Voraussetzung für die Zulässigkeit jeder Überlassung in das Ausland ist die Rechtmäßigkeit der zugrunde liegenden Datenanwendung im Inland (§ 12 Abs. 5 DSG 2000). Die Zulässigkeit dieser Datenanwendung wird im Meldeverfahren gemäß §§ 17ff DSG 2000 geprüft. Die Meldung ist daher Voraussetzung der Genehmigung. Viele Auftraggeber melden ihre neuen Datenanwendungen zeitgleich mit dem Antrag auf Genehmigung einer Überlassung oder sogar erst, wenn die Datenschutzkommission sie auf die Notwendigkeit einer Meldung aufmerksam gemacht hat. Erfolg und Dauer eines Verfahrens zur Genehmigung von Überlassungen hängt daher sehr oft von einem parallel laufenden Meldeverfahren ab.

Die Antragsteller verwenden als Mittel, um ein angemessenes Schutzniveau beim Empfänger der Daten im Ausland zu belegen, fast ausschließlich die Standardvertragsklauseln der Europäischen Union für Überlassungen („Entscheidung der Kommission 2002/16/EG vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung[10] personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG “, kurz „Standardvertragsklauseln 2002/16/EG“[11]). Sofern die oben geschilderten Hindernisse betreffend die Registrierung der Datenanwendung, aus der Daten ins Ausland überlassen werden sollen, überwunden werden konnten, ermöglichen die Standardvertragsklauseln 2002/16/EG eine rasche und problemlose Genehmigung der beantragten Überlassungen.

Des Öfteren ergeben sich Komplikationen

[10] Die RL 95/46 kennt keine Terminologie zur Unterscheidung von Übermittlungen und Überlassungen, weshalb in den deutschen Fassungen der Entscheidungen der EU-Kommission betr. Standardvertragsklauseln das Wort ‚Übermittlung’ für beide Formen des internationalen Datenverkehrs verwendet wird.

[11] siehe http://www.Datenschutzkommission.gv.at/site/6208/default.aspx

in Genehmigungsverfahren auch aus dem Umstand, dass fast alle Antragsteller Konzernunternehmen, also Teil größerer und international agierender Unternehmenskonglomerate sind. Oftmals rollen Konzerne weltweit neue Datenanwendungen aus, ohne die nationale Rechtssituation vorher einer entsprechenden Prüfung zu unterziehen und ohne ihre Tochterunternehmen über die datenschutzrechtlich relevanten Parameter solcher Datenanwendungen eingehend genug zu informieren, was in den Melde- und Genehmigungsverfahren für Missverständnisse und Verzögerungen sorgen kann.

6.3.2 Anträge auf Genehmigung der Übermittlung von Daten ins Ausland

Neben den zahlreichen Anträgen auf Überlassung hatte die Datenschutzkommission auch über eine größere Anzahl von Anträgen auf Übermittlung von Daten an andere Auftraggeber im Ausland zu entscheiden. Diese Anträge gestalteten sich rechtlich sehr viel komplexer als Anträge auch Überlassung, da hier nicht nur das angemessene Datenschutzniveau im Ausland, sondern v.a. auch das Bestehen einer ausreichenden Rechtsgrundlage für die Übermittlung zu prüfen ist. Auch hier stellt sich zunächst allerdings häufig das Problem des Vorhandenseins einer registrierungsfähigen Meldung an das Datenverarbeitungsregister.

Wie bei den Anträgen auf Überlassung betrafen auch die Anträge auf Übermittlung zum überwiegenden Teil Konzernunternehmen. Angesichts des Umstandes, dass die RL 95/46/EG und daher auch das österr. Datenschutzgesetz kein Konzernprivileg kennt, besteht das Problem, dass die einzelnen Konzernunternehmen als unterschiedliche Auftraggeber zu sehen sind, weshalb der Datenverkehr zwischen den Konzernunternehmen einer besonderen Rechtsgrundlage bedarf. Dies ist internationalen Konzernen angesichts ihrer wirtschaftlichen Einheit oft nicht ohne weiteres einsichtig. Die vielfach anzutreffende Verarbeitung von Personal- oder Kundendaten in konzernweiten Informationsverbundsystemen ist datenschutzrechtlich nicht ohne weiteres zulässig: Der zivilrechtliche Eigentümer eines Konzernunternehmens ist nicht Arbeitgeber der Mitarbeiter oder Vertragspartner der Kunden und kann daher auf die Daten dieser Personengruppen nicht ohne besondere rechtliche Befugnis zugreifen.

6.3.3 Whistleblower-Hotlines

Rechtliches Neuland hatte die Datenschutzkommission im Berichtszeitraum im Hinblick auf ein neuartiges Instrument der Korruptionsbekämpfung zu betreten: Mehrere internationale Konzerne legten Anträge auf Genehmigung sogenannter „Whistleblower-Hotlines“ vor. Dabei handelt es sich um Systeme zur – u.U. auch anonymen – Meldung von Missständen in einem Konzernunternehmen an die Konzernspitze unter Umgehung des normalen Dienstweges. Mit diesen Systemen sollen Malversationen im Bereich der Finanzen und der Buchführung sowie Fälle von Bestechung im Unternehmen entdeckt werden. Die „Whistleblower-Hotlines“ wurden in den USA ua. durch die Anti-Korruptionsbestimmungen des „Sarbanes–Oxley Act of 2002“ als Antwort auf den Enron-Korruptionsskandal vorgesehen.

Die rechtlichen Probleme, die sich im Zusammenhang mit Whistleblower-Hotlines stellen, sind mannigfaltig. Die Hotlines dienen zur Meldung des Verdachts der Begehung strafbarer Handlungen. Derartige Daten sind gemäß § 8 Abs. 4 DSG 2000 besonders geschützt. Weiters sollen die Daten an die jeweilige Konzernmutter in Übersee weitergeleitet werden, was mit den Arbeitgeberrechten und -pflichten eines österreichischen Konzernunternehmens unter Umständen kollidiert. Meist sollen im Übrigen auch besondere Dienstleister als spezialisierte Betreiber der Hotline zwischengeschaltet werden.

Die Datenschutzkommission hat in mehre-

ren Bescheiden[12] die Grundlagen der Zulässigkeit für Whistleblower – Hotlines wie folgt dargestellt:

1. Als Auftraggeber jener Datenanwendung, in der die durch whistleblowing an die Hotline gemeldeten Daten aufgezeichnet werden, gilt der österreichische Arbeitgeber.
2. Der Betreiber der Hotline ist daher in erster Linie Dienstleister des österreichischen Auftraggebers.
3. Die Übermittlung von Verdachtsdaten an die Konzernspitze (bzw. an die von ihr beauftragte Stelle) darf nur in solchen Fällen stattfinden, in welchen ein leitender Angestellter des österr. Auftraggebers beschuldigt wird, da nur dann die Gefahr einer „Vertuschung“ denkbar ist, sodass sich in solchen Fällen ein überwiegendes berechtigtes Interesse zur Übermittlung an die Konzernspitze erkennen lässt.
4. Anonyme Meldungen an die Hotline dürfen zwar zugelassen werden, sie werden aber vom österreichischen Auftraggeber bei seinen Mitarbeitern nicht eigens gefördert. Den Meldern wäre vielmehr volle Vertraulichkeit hinsichtlich ihrer Identität zuzusichern, wenn sie diese angeben.
5. Die mit der Bearbeitung von Meldungen betrauten Stellen (sowohl beim österr. Auftraggeber als auch im Konzern im Ausland) sind von den anderen Konzernstellen strikt getrennt zu organisieren und dürfen nur Personen als Mitarbeiter haben, die besonders geschult und ausdrücklich verantwortlich für die Vertraulichkeit der gemeldeten Daten sind.
6. Die Beschuldigten haben grundsätzlich Zugang zu Anschuldigungen.
7. Die Identität des Meldenden wird nur dann offengelegt, wenn sich nachträglich herausstellt, dass die Anschuldigung bewusst falsch erhoben wurde.
8. Die gemeldeten Daten werden spätestens 2 Monate nach Beendigung der Untersuchung gelöscht.

[12] Die letzte Entscheidung ist Zahl K178.305/0004-DSK/2009 vom 24. Juli 2009.

7. Internationale Zusammenarbeit der Unabhängigen Datenschutzbehörden

7.1 Globalisierung des Datenschutzes

Die Internationalen Datenschutzkonferenzen der letzten Jahre in Montreal (2007), in Straßburg (2008) und in Madrid (2009) haben vor allem die Globalisierung der Grundgedanken des Datenschutzes vorangetrieben. Die zahllosen Zusammenhänge, in welchen in einer globalisierten Wirtschaft personenbezogene Daten aus den EU-Ländern ins Ausland transferiert werden, machen deutlich, dass auf Dauer Schutz durch Genehmigungsverfahren nicht praktikabel ist. Es muss vielmehr versucht werden, die Grundsätze des Datenschutzes zu so allgemeiner Anerkennung zu bringen, dass internationaler Datentransfer genehmigungsfrei stattfinden kann, weil er grundsätzlich immer auf ein akzeptables Datenschutzniveau im Empfängerland trifft. Falls einige Staaten an dieser Entwicklung nicht teilhaben wollen, so könnten doch die genehmigungspflichtigen Transfers wenigstens in Zukunft zur Ausnahme werden und nicht mehr die Regel darstellen wie bisher bei global agierenden Unternehmen.

Auch in die Arbeit der internationalen Standardisierungsgremien hat das Thema „Datenschutz“ Einzug gehalten: Die ISO Normen ISO 29100 (Definition von Datenschutzanforderungen bei der Verarbeitung persönlicher Daten in den Informationssystemen aller Länder); und ISO 24760 – Ein Rahmen für Identitätsmanagement (Rahmen für das sichere, zuverlässige Datenschutzkonformitäts- Management der Identitätsinformationen) sind in Ausarbeitung und es ist der Art. 29 Gruppe gelungen, unter der Schirmherrschaft der EU-Kommission aktiv an diesen neuen Standards mitzuarbeiten, damit die europäische Sichtweise von Datenschutz entsprechende Berücksichtigung findet.

7.2 Zusammenarbeit im Rahmen der Art. 29 Gruppe

Die aus den Vertretern der nationalen Datenschutz-Kontrollstellen (iSd Art. 28 der RL 95/46) zusammengesetzte Art. 29 Gruppe hat ihre Bedeutung für die Weiterentwicklung des europäischen Datenschutzes im Berichtszeitraum nachhaltig unter Beweis gestellt. Technologische Neuheiten ebenso wie neue Business-Konzepte werden dort zuerst auf ihre datenschutzrechtlichen Implikationen hin untersucht und beurteilt.

Neuerdings kommt als Feld rechtlicher Analyse auch die Frage nach den Auswirkungen des Vertrags von Lissabon auf den EG-Rechtsbestand hinzu und eine 2009 gestartete Initiative der EU-Kommission, wonach die RL 95/46 daraufhin geprüft wird, ob sie noch zur Gänze den heutigen Bedürfnissen entspricht.

Es wäre im dringenden nationalen Interesse Österreichs, der Datenschutzkommission jenes Personal zur Verfügung zu stellen, das notwendig ist, um an den zahlreichen Aufgaben der Art. 29 Gruppe mitzuarbeiten und dadurch den österreichischen Standpunkt in die erarbeiteten Lösungsvorschläge für neuartige Probleme einfließen zu lassen. Auch wenn die Art. 29 Gruppe keine bindenden Entscheidungen erlassen kann, kommt ihren Äußerungen doch wesentliche Bedeutung zu, da diese – auch global – als maßgebliche Interpretationen des europäischen Datenschutzrechtes angesehen werden, an welchen sich nationale Lösungen messen lassen müssen. Als Beispiel hiefür kann etwa der Bereich „Whistleblowing“ genannt werden, in dem

die Datenschutzkommission in ihren Genehmigungsentscheidungen im internationalen Datenverkehr der Opinion WP 117 zwar weitgehend aber nicht vollständig gefolgt ist, was einen erheblichen Erklärungsbedarf gegenüber der internationalen Business community verursacht hat. [13]

Im Berichtszeitraum hat sich die Art. 29 Gruppe insbesondere mit folgenden Themen auseinander gesetzt und ihre Meinung dazu in Form einer Opinion beschlossen:

a) Fluggastdaten (WP 138, WP 145, WP 151, WP 167)
b) Kooperationssystem für Verbraucherschutz der EU (WP 139)
c) Binnenmarktinformationssystem der EU (WP 140)
d) Schutz der personenbezogenen Daten von Kindern (WP 147, WP 160)
e) Suchmaschinen (WP 148)
f) Verbindliche unternehmensinterne Datenschutzregelungen (BCRs) (WP 154, WP 155)
g) Welt-Anti-Doping-Code (WP 156, WP 162)
h) Soziale Online Netzwerke (WP 163)
i) Zukunft des Datenschutzes (WP 168)

Sämtliche zitierten Arbeitspapiere können auf der Homepage der EU-Kommission nachgelesen werden. [14]

Darüber hinaus wurde zB auch das Thema ‚Geolokalisation' und in diesem Zusammenhang Datenanwendungen wie Google StreetView mehrfach diskutiert, ohne allerdings diesbezüglich zu einer einheitlichen Rechtsauffassung in den Details zu finden.

In den Unter-Arbeitsgruppen wurden im Berichtszeitraum auch Vorarbeiten geleistet für einige wichtige Fragen, die erst 2010 – oder später – zum Abschluss gebracht werden konnten bzw. können, wie die Haltung der Art. 29 Gruppe zu dem in Ausarbeitung befindlichen Grundsatzabkommen EU-USA über Datenschutz beim Datenaustausch – dies wäre für Swift- oder PNR-Daten von grundsätzlicher Bedeutung, oder die Interpretation der Begriffe „Auftraggeber" und „Dienstleister" in der RL 94/46, oder die Auslotung der Frage des „anwendbaren Rechts" im Sinne des Art. 4 der RL 95/46; auch ein Entwurf für eine Opinion zu Datenschutz bei der neuesten Form des Marketing, nämlich „behaviourial advertising" , wurde 2009 ausgearbeitet.

7.2.1 Zu einzelnen Themen von generellem Interesse

7.2.1.1 Proaktive Übermittlung von Daten von Reisenden an den Ankunftsstaat (PNR-Daten)

Seit 2002 verlangen die US-Einwanderungsbehörden von allen Fluglinien, die in den USA landen wollen (aber auch von solchen, die die USA nur überfliegen), Daten über ihre Passagiere, die zum Zweck der Reiseabwicklung gespeichert werden. Dieses Beispiel hat zwischenzeitig umfangreich Schule gemacht und wird nunmehr auch im Hinblick auf Personen diskutiert, die in die EU einreisen wollen. Zu Ende des Berichtszeitraums wurde im Rahmen des britischen „e-borders Projekts" ein solches Verlangen – wenn auch nur beschränkt auf einen kleineren Kreis von Datenarten – sogar innerhalb der Europäischen Union gestellt.

Angesichts der zahlreichen und in immer neuen Varianten auftretenden Datenschutzprobleme in diesem Bereich hat die

[13] Die Datenschutzkommission hat nur die Übermittlung von Verdachtsdaten betreffend leitende Angestellte und Organe von österr. Tochterunternehmen an die ausländische Konzernzentrale als zulässig erachtet: Nur hinsichtlich dieses Personenkreises sei ein überwiegendes berechtigtes Interesse an der Übermittlung erkennbar, da hier die Gefahr bestehe, dass solche Personen angesichts ihres erheblichem Einflusses im Unternehmen die Untersuchung von ihnen selbst zugeschriebenen Verstößen verhindern könnten.

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

Art. 29 Gruppe eine eigene „Traveller data subgroup“ eingerichtet, die sich mit den in diesem Zusammenhang auftretenden Datenschutzproblemen eingehend auseinandersetzt.

Welche Haltung die seit einem halben Jahr im Amt befindliche EU-Kommission letztlich dazu einnehmen wird, ist derzeit noch nicht eindeutig erkennbar. Inwieweit bei der Umsetzung des Stockholmer Programms über einen „Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger“ in Europa dem Datenschutz im Detail mehr Einfluss zugestanden werden wird als bisher, bleibt abzuwarten.

7.2.1.2 Bodyscanners

Im Zusammenhang mit Flugreisen hat ein weiteres Thema für heftige datenschutzrechtliche Reaktionen gesorgt, nämlich der Plan sogenannte Bodyscanner einzusetzen, um das verborgene Mitführen von unerlaubten Substanzen am Körper zu erkennen.

Im Februar 2009 hat die EU Kommission die Art. 29 Gruppe zu diesem Thema im Rahmen einer öffentlichen Konsultation befragt. Die Ergebnisse dieser Konsultation wurden von der EU Kommission am 15.6.2010 publiziert [15].

7.2.1.3 Mobilitätsdaten

Im Rahmen der Unterarbeitsgruppe ‚Internet Taskforce’ werden die jeweils neuesten Trends der Informationstechnologie im Hinblick auf die datenschutzrechtlichen Implikationen diskutiert. Ein Thema mit großer zukünftiger Bedeutung dürfte die Speicherung von Mobilitätsdaten in den unterschiedlichsten Zusammenhängen sein wie zB. Bahnkartendaten, Schiffskartendaten, Road-Pricing-Daten, Verkehrssteuerungsdaten, Fahrzeug-Unfall-Daten etc.

Auch für das Anbieten von vielen Mehrwertdiensten (zB Auskunft durch SMS auf dem Mobil-Telefon, wo die nächste Pizzeria, die nächste Bushaltestelle, Apotheke etc. ist) ist die Geolokalisation des Betroffenen Voraussetzung. Mobilitätsdaten von Einzelpersonen werden demnächst auch im Wege der Vorratsdatenspeicherung von Funkzellenstandortdaten erfasst sein.

Aus datenschutzrechtlicher Sicht muss rechtzeitig darauf aufmerksam gemacht werden, welche Gefahren sich für die Freiheit des Einzelnen ergeben können, wenn nicht von vornherein klare Regeln dafür aufgestellt werden, welche Grenzen für eine Auswertung dieser Daten eingehalten werden müssen. Schon im Design solcher Dienste muss Datenschutz vorgesorgt werden – dies ist eine der wichtigsten und stets wiederholten Forderungen der Unabhängigen Datenschutzbehörden an die Industrie für die Konfigurierung von IT-Applikationen.

7.2.1.4 Verbindliche Konzern-Richtlinien (Binding Corporate Rules, BCRs)

Zu diesem Punkt wurde im Berichtszeitraum ein Durchbruch erzielt, indem es gelang, ein Konzept für ein gemeinsames Evaluierungsverfahren zu verabschieden. Voraussetzung dafür war die Ausarbeitung genauer inhaltlicher Vorgaben für BCRs, deren Einhaltung nunmehr jeweils von drei Datenschutzbehörden gemeinsam geprüft wird. Schon während des Verfahrens sind auch alle anderen betroffenen Datenschutzbehörden eingebunden – das sind jene, in deren Land der die BCRs vorlegende Konzern ein Tochterunternehmen unterhält. Das Ergebnis des Verfahrens wird allen Datenschutzbehörden mitgeteilt und soll im positiven Fall für alle Datenschutzbehörden, die sich bereit erklärt haben, an diesem gemeinsamen Verfahren teilnehmen zu wollen, als Nachweis des angemessenen Datenschutzniveaus bei den betreffenden Konzernfirmen gelten. Auch Österreich hat sich jenen – bisher 20 – EU-Mitgliedstaaten angeschlossen, die an diesem neuen Verfahren grundsätzlich teilnehmen.

[15] COM(2010) 311/4

7.2.1.5 Global Privacy enforcing network

Eine weitere Initiative der Art. 29 Gruppe, die gemeinsam mit dem Europäischen Datenschutzbeauftragten verfolgt wird, besteht darin zu explorieren, inwieweit staatliche Aufsichtsbehörden aus anderen Rechtskreisen – etwa in den USA – dafür gewonnen werden könnten, bei transatlantischen oder sonstigen globalen Datenschutz-Rechtsdurchsetzungsproblemen gemeinsam oder zumindest koordiniert vorzugehen. Diese noch im Anfangsstadium befindliche Initiative könnte eine informelle, aber deshalb nicht minder interessante vorläufige Antwort auf die grenzüberschreitende und insbesondere Kontinente überschreitende Verwendung personenbezogener Daten sein, solange es kein globales Datenschutzübereinkommen – etwa der Vereinten Nationen – gibt.

7.2.1.6 Die Zukunft des europäischen Datenschutzes

Im Mai 2009 hat die EU-Kommission eine Konferenz der maßgeblichen Stakeholder nach Brüssel einberufen, um in Erfahrung zu bringen, wie die Situation des europäischen Datenschutzes von diesen Stakeholdern beurteilt wird. Angesichts der vielfach kritischen Stimmen hat die Art. 29 Gruppe beschlossen, noch vor Ende des Jahres 2009 ihre Sichtweise betreffend den Sachstand und allfällige Korrekturwünsche in einem eigenen Papier niederzulegen und der EU-Kommission zur Verfügung zu stellen. Dieses Vorhaben wurde rechtzeitig verwirklicht (WP 168) und hat damit Eingang in die derzeit stattfindende Diskussion über eine Änderung des europäischen Datenschutzrechtes – auch im Hinblick auf den Wegfall der Säulenteilung durch den Vertrag von Lissabon – gefunden.

Die wesentliche Botschaft dieses Papiers gilt dem sogenannten „accountability principle“, worunter eine Verschiebung der Hauptverantwortung für die Einhaltung von Datenschutz zu verstehen ist: Bisher wurde in fast allen EU-Mitgliedstaaten versucht, die Einhaltung von Datenschutz vornehmlich durch proaktive administrative Maßnahmen wie Registrierung oder Genehmigungsverfahren oder reaktive Maßnahmen wie Beschwerdeverfahren und Vorort-Kontrollen zu gewährleisten. Als Garant dieser Gewährleistung wird die Datenschutzkontrollstelle angesehen. In dieser Situation muss zugegeben werden, dass in einem Umfeld, in dem elektronische Datenverarbeitung nicht mehr die Ausnahme sondern die absolute Regel ist, diese Maßnahmen nicht mehr die notwendige Effizienz aufweisen. Es sollten somit auch andere Regulierungsinstrumente angedacht werden, die es in höherem Maße den Auftraggebern auferlegen, durch eigene Initiativen nachzuweisen, dass sie datenschutzkonform agieren, dass sie also Verantwortlichkeit („accountability“) bei sich verwirklichen. Regelmäßige Datenschutz-Audits, unternehmensinterne Datenschutzregeln, Gütesiegel, Zertifizierungen etc. könnten hiezu beitragen. Wie immer eine kontinentaleuropäische Haltung zu diesen vor allem aus dem anglosächsischen Bereich stammenden Ideen aussehen mag, lässt sich jedoch die Notwendigkeit nicht leugnen, dass darüber nachgedacht werden muss, wie der Wirkungsgrad der nationalen Datenschutzkontrollstellen bei steigender Ressourcenknappheit effektiver gestaltet werden kann.

7.3 Zusammenarbeit im Rahmen der Gemeinsamen Kontrollinstanzen der Dritten Säule

7.3.1 Die Gemeinsame Kontrollinstanz (GKI) für Europol

Europol ist eine EU-weit operierende Polizeiorganisation mit dem Ziel, die Mitgliedstaaten bei der Prävention und der Bekämpfung schwerwiegender Formen internationaler Kriminalität zu unterstützen. Dies bezieht sich nur auf solche Fälle, in denen es sich um organisierte Kriminalität handelt und zwei oder mehr Mitgliedstaaten betroffen sind.

Die Hauptaufgabe der 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 führt die GKI jährlich eine Inspektion bei Europol durch.

Die österreichischen Mitglieder der GKI werden von der Datenschutzkommission entsandt. Überdies stellt die Datenschutzkommission ein Mitglied der Europol-Inspektionsgruppe, welche im März 2008 und im März 2009 Inspektionen bei Europol durchgeführt hat. Die Schwerpunkte dieser beiden Kontrollen lagen im Wesentlichen bei der Überprüfung der Funktionsweise des Europol-Informationssystems und der Rechtskonformität der Datenverwendung in Analytical Workfiles (AWF). Weiters beschäftigte sich das Inspektionsteam mit der Funktionsweise des Informationsportals „Check the Web“ und der OASIS-Projekte sowie mit der Umsetzung von Empfehlungen, die Europol als Ergebnis vorangehender Inspektionen erteilt wurden.

Eine besondere Aufgabe, die der gemeinsamen Kontrollinstanz durch das Europol Übereinkommen übertragen wurde, ist die Entscheidung über Beschwerden von Einzelpersonen, die sich gegen eine Antwort von Europol auf ein Auskunfts- Richtigstellungs- oder Löschungsbegehren richtet. Zu diesem Zweck hat die GKI am 23. November 1998 einen Beschwerdeausschuss eingerichtet. Die Arbeit dieses gerichtsähnlichen Gremiums stellt ein Rechtsbehelfsverfahren für Einzelpersonen dar, die im Zusammenhang mit der Verarbeitung und Nutzung ihrer personenbezogenen Daten durch Europol ihre Rechte und Freiheiten einfordern. Zwischen Juli 2007 und Jänner 2010 wurden zwei Beschwerdefälle erledigt.

7.3.2 Die Gemeinsame Kontrollinstanz (GKI) für Schengen

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

Das Bundesministerium für Inneres (BMI) ist für die Führung des nationalen Teils des Schengener Informationssystems (N.SIS) als Auftraggeber zuständig. Die Pflicht zur Auskunftserteilung über das N.SIS gemäß §§ 1 und 26 DSG 2000 an Betroffene trifft daher das BMI. Fälschlicherweise an die Datenschutzkommission gerichtete Auskunftsbegehren werden daher an das BMI weitergeleitet. Außerdem lässt sich auf der Website der Datenschutzkommission schon seit Jahren ein Formular (mit englischer Übersetzung) für die Auskunft aus dem N.SIS abrufen (http://www.Datenschutzkommission.gv.at/DocView.axd?CobId=30578), das auch vielfach benützt wird.

Schon seit 2003 wird über eine neue rechtliche Basis für das SIS diskutiert, da die Technik von ‚SIS I Plus’ angesichts des rasant angestiegenen Datenumfangs durch

den erweiterten Teilnehmerkreis an seine Grenzen stößt. Die neuen Rechtsgrundlagen für das SIS II sind mittlerweile veröffentlicht[16], finden aber erst dann Anwendung, wenn das SIS II in Echtbetrieb – möglicherweise noch 2010[17] – geht. Die GKI wurde in die Vorbereitung zur Implementierung von SIS II eingebunden. Sie hat sich zu verschiedenen Fragen der Migration von Daten aus SIS I Plus in SIS II geäußert. Vor allem ging es um datenschutzrechtliche Anforderungen, die an einen derartigen Testlauf gestellt werden, insbesondere die Sicherstellung der Anonymisierung der dabei verwendeten Daten.

Im Jahr 2004 hatte die GKI eine europaweit koordinierte Prüfung von Ausschreibungen zur Einreiseverweigerung nach Art. 96 SDÜ sowie von Ausschreibungen in Bezug auf Vermisste und Minderjährige gemäß Art. 97 SDÜ initiiert. Im März 2008 wurde ein follow-up-check der damaligen Feststellungen beschlossen, um zu überprüfen, ob die seinerzeit festgestellten Defizite weiterhin bestehen. Die Nachprüfungen haben ergeben, dass die Ausschreibungen dazu in den einzelnen Mitgliedsländern nach wie vor sehr unterschiedlich gehandhabt werden und dies auch der Grund dafür ist, dass die Zahl der Ausschreibungen in den einzelnen Mitgliedsstaaten stark voneinander abweichen. Die GKI sprach sich daher in ihrem Abschlussbericht und den darin erlassenen Empfehlungen für einheitliche Ausschreibungsverfahren aus, die schriftlich festgehalten und für die ausschreibenden Stellen immer greifbar sein sollen.

7.3.3 Die gemeinsame Kontrollinstanz (GKI) für das ZIS

Auf der Basis der Verordnung (EG) 515/97 des Rates über die gegenseitige Amtshilfe zwischen Verwaltungsbehörden der Mitgliedstaaten und die Zusammenarbeit dieser Behörden mit der Kommission im Hinblick auf die ordnungsgemäße Anwendung der Zoll- und Agrarregelung vom 13. März 1997 (ABl. L 82 vom 22. März 1997, S. 1) sowie des Übereinkommens aufgrund von Artikel K.3 des Vertrages über die Europäische Union über den Einsatz der Informationstechnologie im Zollbereich vom 26. Juli 1995 (ABl. C 316 vom 27. November 1995, S. 34) (Zollübereinkommen) wurde ein gemeinsames Zollinformationssystem (ZIS) eingerichtet. Dieses erlaubt es, sowohl in einer Datenbank für den Bereich der gemeinschaftsrechtlichen Zuständigkeiten wie auch in einer Datenbank, die den nicht harmonisierten Bereich betrifft, Daten über Waren oder Transportmittel sowie über natürliche und juristische Personen zu speichern, für die es tatsächliche Anhaltspunkte gibt, dass sie im Zusammenhang mit Handlungen stehen, die der Zoll- oder der Agrarregelung zuwiderlaufen. Das ZIS ist als Ausschreibungsdatei im Rahmen der Betrugsbekämpfung konstruiert und ermöglicht es jenem Mitgliedstaat, der die Daten in das System eingegeben hat, einen ZIS-Partner in einem anderen Mitgliedstaat um die Durchführung u.a. gezielter Kontrollen zu ersuchen.

Um eine adäquate datenschutzrechtliche Kontrolle zu gewährleisten, wurde durch das vorstehend zitierte Übereinkommen vom 26. Juli 1995 eine gemeinsame Aufsichtsbehörde (Gemeinsame Kontrollinstanz für das ZIS) eingerichtet, für die jedes EU-Mitgliedsland zwei Vertreter namhaft macht, die von der jeweiligen nationa-

[16] Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABlEG 2006/L 381/4); Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über den Zugang von für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständigen Dienststellen der Mitgliedstaaten zum Schengener Informationssystem der zweiten Generation (SIS II) (ABlEG 2006/L 381/1); Beschluss des Rates vom 12. Juni 2007 über die Einrichtung, Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABlEG 2007/L 205/63).

[17] Der Start hat sich bisher aufgrund technischer Probleme immer wieder verzögert.

len unabhängigen Datenschutzbehörde nominiert werden. Die GKI hält regelmäßig Sitzungen in Brüssel ab.

Derzeit wird darüber diskutiert, das bestehende Zollübereinkommen durch einen Ratsbeschluss zu ersetzen.

7.3.4 Die datenschutzrechtliche Kontrolle von Eurodac

Das „Eurodac"-System ermöglicht den Mitgliedstaaten, Asylbewerber sowie Personen zu identifizieren, die nach illegalem Überschreiten einer EU-Außengrenze aufgegriffen wurden. Anhand des Vergleichs der Fingerabdrücke kann ein Mitgliedstaat feststellen, ob ein Asylwerber oder ein Ausländer, der sich illegal in seinem Hoheitsgebiet aufhält, bereits in einem anderen Mitgliedstaat Asyl beantragt hat oder ob ein Asylbewerber illegal in die EU eingereist ist.

„Eurodac" besteht aus einer von der EU-Kommission verwalteten Zentraleinheit – der computergestützten Datenbank für Fingerabdrücke – und elektronischen Einrichtungen für die Datenübertragung zwischen den Mitgliedstaaten und der zentralen Datenbank. Neben den Fingerabdrücken umfassen die von den Mitgliedstaaten übermittelten Daten u. a. den Herkunftsmitgliedstaat, Ort und Zeitpunkt der Antragstellung, das Geschlecht sowie die Kennnummer (Namen werden in diesem System nicht gespeichert, es handelt sich daher um eine Sammlung von „indirekt personenbezogenen Daten" im Sinne des öDSG).

Im Berichtszeitraum hat sich die Koordinierungsgruppe, bestehend aus dem Europäischen Datenschutzbeauftragten und den nationalen Kontrollinstanzen, damit auseinandergesetzt, inwieweit die Mitgliedstaaten der in Art. 18 EURODAC-Verordnung enthaltenen Unterrichtungspflicht nachkommen.[18] Weiters wurde die Speicherung von Daten Minderjähriger, insbesondere, ob – anders als in der EURODAC-Verordnung vorgesehen – auch schon Daten von unter 14-Jährigen gespeichert werden, die unterschiedlichen von den Mitgliedstaaten angewandten Methoden zur Feststellung des Alters des minderjährigen Asylbewerbers sowie die Anwendung von Dubli-Net[19] untersucht.

7.4 Die „Working Party Police and Justice (WPPJ)"

Bei der Frühjahrskonferenz der Unabhängigen Datenschutzbehörden 2007 auf Zypern (Larnaka) wurde die Working Party Police and Justice (WPPJ) neu konstituiert als Nachfolgeorganisation der früheren Police Working Party (PWP), die als ständige Untergruppe der Frühjahrskonferenzen der Europäischen Datenschutzbehörden eingerichtet worden war. Die WPPJ hat die Aufgabe, die wichtigsten datenschutzrechtlichen Fragen der ehemaligen 3. Säule der EU (polizeiliche und justizielle Zusammenarbeit) zu beraten, die der Zuständigkeit der Art. 29 Gruppe – nach wie vor – entzogen sind. Sie fungiert damit auch als Pendant und/oder auch als Bindeglied zur Art. 29 Datenschutzgruppe.

Im Berichtszeitraum hatte sich die WPPJ mit der Implementierung des Prümer Vertrages sowie mit einem Rahmenbeschluss über den Datenschutz in der 3. Säule auseinander zu setzen. Außerdem hat sich die WPPJ jüngst kritisch zu der Entscheidung der Europäischen Kommission, den Voll-

[18] Art. 18 EURODAC-Verordnung lautet:

„(1) Der Herkunftsmitgliedstaat unterrichtet die Personen, die unter diese Verordnung fallen, über a) die Identität des für die Verarbeitung Verantwortlichen und ggf. seines Vertreters, b) die Zwecke der Verarbeitung der Daten im Rahmen von Eurodac, c) die Empfänger der Daten, d) die Verpflichtung zur Fingerabdrucknahme bei Personen im Sinne des Artikels 4 oder Artikels 8, e) die Auskunfts- und Berichtigungsrechte bezüglich sie betreffender Daten."

[19] Das ist ein Netz, über das die Daten zur Bestimmung der zuständigen Asylbehörde zwischen den Mitgliedstaaten ausgetauscht werden.

zugsbehörden Zugang zu Eurodac zu gewähren, geäußert.

8. Das Datenverarbeitungsregister

8.1 Statistische Aufgliederung des Arbeitsanfalls und der Erledigungen

8.1.1 Vorbemerkungen:

Entsprechend der Gliederung des sonstigen Geschäftsgangs der Datenschutzkommission nach Halbjahren, werden auch Eingänge und Erledigungen im Datenverarbeitungsregister nach Halbjahren gegliedert dargestellt. Was den Berichtszeitraum betrifft, hat sich jedoch herausgestellt, dass es angesichts der in diesem Zeitraum angewendeten unterschiedlichen technischen Protokollierungssysteme nicht möglich ist, Zahlen über unterschiedliche Dokumenttypen, wie Auftraggebermeldungen, Erstmeldungen für Datenanwendungen etc. auszuweisen. Es kann im wesentlichen nur mit ‚Jobs' gerechnet werden unabhängig davon, welches ihr Inhalt war.

Wesentlich ist es auch vorauszuschicken, dass für die technische Infrastruktur des Datenverarbeitungsregisters das Bundeskanzleramt verantwortlich zeichnet. Bis zum 1. Jänner 2009 waren mehrere (bis zu drei) verschiedene Systeme der Bearbeitung von Meldungen nebeneinander im Einsatz. Auswertungen mussten daher für den Zeitraum vor 2009 in unterschiedlicher Form vorgenommen werden, so konnten zB vor dem 1. Jänner 2009 statistische Auswertungen nur unter Mithilfe der EDV-Abteilung des Bundeskanzleramtes vorgenommen werden. Erst seit dem 1.Jänner 2009 können statistische Auswertungen vom Datenverarbeitungsregister selbst direkt aus dem System erstellt werden.

8.1.2 Arbeitsanfall und Erledigungen 2008

Was das Jahr 2008 betrifft, beziehen sich die Auswertungsergebnisse auf die sog. „DVR-Applikation" (-Vorgängersystem zu „DVR-Online"-) und auf „ELAK"-Erledigungen – dies sind zwei der drei Protokollierungssysteme, die vor dem 1.1.2009 im Einsatz waren.

Im ersten Halbjahr 2008 betrug der Eingang (Neuzugang) 2441 Jobs (in der „DVR-Applikation"), sowie 1464 Meldungen, welche im ELAK protokolliert wurden (gesamt: über 3900).
Die Zahl der Erledigungen ergibt sich in der DVR-Applikation mit 2164; hinzu kommt die Erledigung von 566 Eingangsstücken aus dem Bereich der ELAK-Datenbank (gesamt: 2750)

Erstes Halbjahr 2008

	Eingang	Erledigungen
Jobs	2441	2164
ELAKs	1464	586
Gesamt	3905	2750
Monatsschnitt	650	458

Für das zweite Halbjahr 2008 liegen exakte Zahlen nur bis Oktober vor. Eine Schätzung auf Grundlage des von der EDV-Abteilung des BKA für 2008 errechneten Monatsschnitts ergibt als Eingang etwas mehr als 5900 Eingangsstücke. Diese hohe Zahl ergibt sich vor allem dadurch, dass in diesem Zeitraum hunderte Meldungen von Banken zur Videoüberwachung, weiters hunderte Meldungen von Banken, Versicherungen und Leasinggesellschaften zur Kleinkredit-Evidenz (KKE) und zahlreiche

Meldungen von Judovereinen (JAMA) eingelangt sind.

Was die Erledigungen betrifft, wurde für das zweite Halbjahr 2008 ein Monatsdurchschnitt für die Monate bis November von 458 Registrierungen errechnet, was – hochgerechnet – für dieses Halbjahr insgesamt etwa 2750 Erledigungen ergibt.

Zweites Halbjahr 2008

	Eingang	Erledigungen
Jobs	5550(*)(**)	2574(*)
ELAKs	382	175
Gesamt	5932	2749
Monatsschnitt	988	458

(*)… hochgerechnet
(**)…jeweils hunderte Meldungen KKE, Videoüberwachung - Banken, JAMA

8.1.3 Arbeitsanfall und Erledigungen 2009

Eine verlässliche Angabe der Anzahl von noch zu erledigenden Jobs gibt es seit Jänner 2009, zu welchem Zeitpunkt das gesamte Arbeitsaufkommen in das neue System „DVR-Online“ migriert wurde. Einschließlich der Rückstände waren zu diesem Zeitpunkt insgesamt etwa 8700 Jobs zur Bearbeitung offen.

Im ersten Halbjahr 2009 betrug der Eingang (Neuzugang) in der neuen DVR-Applikation 3393. 107 Meldungen wurden nach wie vor im ELAK protokolliert (gesamt somit: 3500).

Die Zahl der Erledigungen in der DVR-Applikation betrug 2000. Hinzu kommt die Erledigung von 82 Eingangsstücken aus dem Bereich der ELAK-Datenbank (gesamt: 2082).

Erstes Halbjahr 2009

	Eingang	Erledigungen
DVR-Applikation	3393	2000
ELAKs	107	82
Gesamt	3500	2082
Monatsschnitt	583	347

Für das zweite Halbjahr 2009 beträgt die Gesamtanzahl der Eingangsstücke etwa 3600 (Monatschnitt 600). Die Zahl der Erledigungen in diesem Zeitraum beträgt 3465, was einen Monatschnitt von 588 Erledigungen ergibt.

Zweites Halbjahr 2009 (***)

	Eingang	Erledigungen
DVR-Applikation	3470	3367
ELAKs	129	98
Gesamt	3599	3465
Monatsschnitt	600	578

(***)… hochgerechnet (01.07.-31.10.09 /4 x6)

In diesem Halbjahr gelang es zum ersten Mal, Eingänge und Erledigungen ins Gleichgewicht zu bringen. Dies darf freilich nicht darüber hinweg täuschen, dass noch mehrere tausend Anträge als Rückstände einer Erledigung harren, falls nicht durch entsprechende Übergangsbestim-

mungen nach Anwendbarkeit der neuen Registrierungsregeln der DSG Novelle 2010 Vorsoge getroffen wird.

8. 2 DVR-online

8.2.1 Darstellung der bereits operationalen Verbesserungen im Verfahrensablauf durch das neue System:

Im letzten Datenschutzbericht wurde für das Datenverarbeitungsregister ein neues System, welches den online-Zugang zum DVR von außen – sowohl für Bürger, die Information suchen, als auch für meldepflichtige Auftraggeber – ermöglichen soll, angesprochen. Durch die in den letzten Jahren eingetretene technische Entwicklung nahm die Anzahl der Meldungen von registrierungspflichtigen Datenanwendungen und deren Änderungen kontinuierlich zu. Es war daher erforderlich, die Mitarbeiterinnen und Mitarbeiter des Datenverarbeitungsregisters von den administrativen Routineaufgaben im Registrierungsverfahren so weit wie möglich durch eine geeignete elektronische Datenbankapplikation zu entlasten.

Von 2005 bis Ende 2008 war eine fachspezifische Web-Anwendung im Einsatz, die jedoch grundlegend adaptiert werden musste, um einen – zunächst nur internen - Online-Betrieb zu ermöglichen. Im Dezember 2008 wurden jene Daten, die im elektronischen Aktenverwaltungssystem der Bundesverwaltung ELAK verwaltet worden waren sowie die Registerinhalte der internen fachspezifischen Web-Anwendung zusammengeführt und in das neu programmierte System „DVR-Online“ übernommen. Anschließend musste die Qualität der übernommen Daten überprüft und eine Datenbereinigung vorgenommen werden. Der interne Echtbetrieb dieses neuen Systems wurde im Jänner 2009 aufgenommen.

Erleichterungen durch die neue Applikation ergaben sich vor allem in manipulativer Hinsicht im Arbeitsablauf für die DVR-Bediensteten:

So musste zB vor der Übernahme der ELAK-Akten und der Daten der alten Applikation jeweils in beiden Systemen gesucht werden (zB ob ein Auftraggeber bereits registriert ist). Die Suchmöglichkeit war eingeschränkt auf die Auftraggeberbezeichnung und/oder die DVR-Nummer. Die DVR-Recherche für DVR-Beschäftigte erstreckt sich nunmehr auf die registrierten Auftraggeber und auf alle im Arbeitsvorrat befindlichen Meldungen. Die Suchkriterien wurden wesentlich erweitert (zB auf die Bezeichnung von Datenanwendungen, Datenschutzkommission-Bescheidzahlen, Datenarten und Datenkategorien etc.).

Unter Protokoll-Statistik können statistische Auswertungen für einen definierten Zeitraum vorgenommen werden.

Besonders hervorzuheben als arbeitsbeschleunigend ist die automatisierte Zustellung von Erledigungsschreiben an Auftraggeber (Verbesserungsaufträge und Mitteilungen über die Registrierung). Die Erledigungsschreiben werden nach Genehmigung und Versendung auch automatisch in den Beilagen zum Auftraggeber bzw. den Datenanwendungen abgelegt.

8.2.2 Darstellung der noch nicht realisierten weiteren Ausbauschritte des Systems:

Eine wirklich messbare Reduzierung des Arbeitsanfalles für die Bediensteten des DVR wird es allerdings erst dann geben, wenn das System nicht nur intern genutzt werden kann sondern für Bürger und Auftrageber zwecks online-Information bzw. online-Meldung frei geschaltet ist. Derzeit ist das System nur intern operational.

Nach Freischaltung des Systems werden den Bürgern, Auftraggebern und Informationsverbundsystemen -Betreibern folgende Funktionalitäten zur Verfügung stehen:

1. Eingangstool:
- Über das Eingangstool können Bürger ohne Authentifizierung im öffentlichen Teil des Datenverarbeitungsregisters recherchieren;
- Auftraggeber haben mit der Bürgerkarte oder über das Stammportal des Bundeskanzleramtes Zugang zu ihrem Auftraggebertool;
- Betreiber von Informationsverbundsystemen (IVS) haben mit der Bürgerkarte oder über das Stammportal des Bundeskanzleramtes Zugang zu ihrem IVS-Betreibertool.

Für die Authentifizierung der Benutzer werden bei Verwendung der Bürgerkarte bestehende E-Government-Strukturen genutzt. Es wird allerdings auch weiterhin möglich sein, ohne Verwendung der Bürgerkarte eine Meldung einzubringen.

Die eingesetzten E-Government Strukturen sind der eigentlichen Anwendung vorgelagert und mussten nicht individuell implementiert werden. Die Prüfung der Berechtigung zur Verwendung der Bürgerkarte erfolgt nicht in DVR-Online, sondern vorgelagert mit bestehenden Technologien. Bei der erstmaligen Anmeldung eines Auftraggebers mit der Bürgerkarte im Eingangstool wird für den betreffenden Auftraggeber automatisiert das bereichsspezifische Personenkennzeichen (bPK) gebildet und mit den ihn betreffenden Daten, Meldungen und Beilagen zu den Meldungen im Datenverarbeitungsregister verknüpft und gespeichert.

2. Auftraggebertool:
Über das Auftraggebertool können Auftraggeber elektronisch DVR-Meldungen einbringen. Der betreffende Auftraggeber hat Einsicht in die von ihm eingebrachten Meldungen samt Beilagen. Nach Klick auf den Button „Versenden“ wird die Meldung an das DVR weitergeleitet, oder wenn die Voraussetzungen für eine automatische Registrierung vorliegen, automatisch registriert.

Der Auftraggeber kann für eine Änderungsmeldung seine registrierte Datenanwendung wieder aufsuchen und die entsprechenden Änderungen im Formular vornehmen, was wieder zur automatischen Registrierung führt.

3. IVS-Betreibertool:
Für Informationsverbundsysteme, die als gesamtes System vom Systembetreiber zu melden sind, steht ein eigenes IVS-Betreibertool zur Verfügung. Die am Informationsverbundsystem teilnehmenden Auftraggeber haben darüber hinaus eine Meldung mit Hilfe des Auftraggebertools zu erstatten. Der IVS-Gesamtmeldung ist eine Liste der teilnehmenden Auftraggeber angeschlossen.

Die Erfassung der Meldungen erfolgt in Hinkunft somit grundsätzlich nicht mehr durch DVR-Bedienstete sondern durch die Auftraggeber. Weiters ist vorgesehen, dass eine Registrierung von Verarbeitungen, die nicht vorabkontrollpflichtig sind, aufgrund einer Plausibilitätskontrolle voll automatisch möglich ist. Der Registerauszug wird diesfalls elektronisch zugestellt.

Bevor dieses System allgemein Online in Betrieb gehen soll, ist geplant, den Zugang für einige Auftraggeber, die regelmäßig Datenanwendungen melden, zu eröffnen, damit festgestellt werden kann, ob aus Sicht dieser Auftraggeber Verbesserungen der Funktionalitäten des Systems notwendig sind.

Als Zeithorizont für die allgemeine Nutzbarkeit von DVR-Online ist Mitte 2011 geplant.

8.3 Wichtige Registrierungen aus dem Berichtszeitraum:

8.3.1 Aus dem Bereich Banken, Versicherungen:

Klein-Kreditevidenz ("Konsumentenkreditevidenz") zum Zweck des Gläubigerschutzes und der Risikominimierung.

Die Kleinkreditevidenz zum Zweck des Gläubigerschutzes und der Risikominimierung (Konsumentenkreditevidenz, KKE) ist ein vom Kreditschutzverband von 1870 (KSV) betriebenes Informationsverbundsystem, welches Daten über Kreditverhältnisse, und zwar – im Unterschied zur Warnliste der Banken – auch sog. „Positivdaten“, nämlich Daten über Kreditverhältnisse ohne Zahlungsanstand, enthält.

Die KKE steht nur den Banken, kreditgebenden Versicherungen und Leasingunternehmen im EWR – in dem ein gleichmäßig hohes Datenschutzniveau aufgrund der gemeinschaftsrechtlichen Vorschriften gewährleistet ist – als Informationsmittel zur Verfügung. Im Zusammenhang mit den die Banken betreffenden Verpflichtungen zur umfassenden Risikobeurteilung von Kreditwerbern nach den Basel II-Richtlinien und auch nach der vor der Verabschiedung stehenden Verbraucherkredit-Richtlinie erhält eine Datensammlung wie die KKE besondere Bedeutung, und zwar als Mittel zur umfassenden Erkundung des Kreditrisikos, das mit der Kreditvergabe an Privatpersonen oder Klein- und Mittelbetriebe (KMUs) verbunden ist.

Hier erfolgte die Registrierung unter strengen Auflagen

8.3.2 Aus dem Gesundheitsbereich:

- Arzneimittel-Sicherheitsgurt mit e-card/E-Medikationsdatenbank
  Hierbei handelt es sich um ein von der Pharmazeutischen Gehaltskasse betriebenes Informationsvebundsystem, welches als Pilotprojekt im Bundesland Salzburg folgende Ziele umfasst:
- Vermeidung unerwünschter Interaktionen
- Vermeidung von Mehrfachverordnungen/Mehrfachbezug
- Unterstützung bei der compliance-Überwachung (Reichweite)(weitere Informationen unter: www.gehaltskasse.at)Die Registrierung erfolgte unter strengen Auflagen, insbesondere betreffend das Vorliegen einer Zustimmung der Betroffenen
- Mammografie-Screening
- Vorsorgeregister (z. B. Schlaganfall)
- Epidemiologisches Meldesystem (EMS)
- Klinische Studien

8.3.3 Aus dem Bereich Soziales:

- Missbrauchsopferdatenbank OÖ (zur Datenerfassung bei Verdacht einer Vernachlässigung, Misshandlung oder des sexuellen Missbrauchs von Minderjährigen aufgrund der §§ 5a und b OÖ Jugendwohlfahrtsgesetz)
- Informationsverbundsystem-Soziales NÖ

8.3.4 Aus dem Zuständigkeitsbereich des Bundesministeriums für Inneres:

- Meldungen der Verkehrsbehörden im Rahmen der 22. StVO-Novelle (hinsichtlich der neu geregelten Bestimmungen im Zusammenhang mit Radarmessungen, Abstandsmessungen, der Section Control, der Rotlicht-Überwachung im Kreuzungsbereich und der Überwachung aus den Fahrzeugen)
- Identitätsdokumentenregister (Ergänzung durch Fingerprints für Reisedokumente)
- (Zentrales/Lokales) Einsatzleitsystem BMI

8.3.5 für den Bereich des öffentlichen Notariats:

Folgende Informationsverbundsysteme wurden registriert:

- Österreichisches Zentrales Testamentsregister, (ÖZTR),
- Österreichisches Zentrales Vertretungsverzeichnis (ÖZVV),
- Patientenverfügungsregister des österreichischen Notariats,
- Privaturkundenarchiv des österreichischen Notariats,
- Treuhandregister des österreichischen Notariats (THR),
- Urkundenarchiv des österreichischen Notariats,
- Vorsorgevollmachtsregister des österreichischen Notariats (VVR)

9. Die Datenschutzkommission als Stammzahlenregisterbehörde

9.1 Die Funktionen der Stammzahlenregisterbehörde

Im österreichischen E-Government-System erfolgt die eindeutige Identifikation von natürlichen Personen durch eine geheime Stammzahl und davon abgeleitete bereichsspezifische Personenkennzeichen (bPK). Die Stammzahl darf nur auf der Bürgerkarte gespeichert werden. Sie wird aus der im zentralen Melderegister verwendeten ZMR-Zahl mit Hilfe eines geheimen Schlüssels gebildet. Der geheime Schlüssel wird von der Datenschutzkommission in ihrer Funktion als Stammzahlenregisterbehörde verwaltet.

Die Datenschutzkommission beaufsichtigt in ihrer Funktion als Stammzahlenregisterbehörde weiters die Erzeugung der bereichsspezifischen Personenkennzeichen und stellt sicher, dass diese richtig vergeben werden. Zu diesem Zweck müssen Auftraggeber des öffentlichen Bereichs einen Antrag bei der Datenschutzkommission auf Erlaubnis der Ausstattung einer Datenanwendung mit bPKs stellen. Anlässlich der Erlaubniserteilung wird von der Datenschutzkommission – die im Hinblick auf die Datenanwendung außerdem auch als Datenverarbeitungsregister tätig wird - festgelegt, welchem Bereich die Datenanwendung zuzurechnen ist und mit welcher Bereichskennung daher die bPKs für diese Datenanwendung zu bilden sind. Im Datenverarbeitungsregister wird dies dadurch sichtbar gemacht, dass in der Registrierung eine Datenart „bPK“ mit einem bestimmten Bereichskennzeichen eingetragen ist.

Dieses System der Identifikation stellt sicher, dass die eindeutig erzeugten Identifikatoren für ein- und dieselbe Person in unterschiedlichen Bereichen der öffentlichen Verwaltung unterschiedlich sind. Ein bereichsspezifisches Personenkennzeichen kann weder auf die Stammzahl zurückgerechnet werden, noch – ohne zusätzliche Angaben über die Person - in ein bereichsspezifisches Personenkennzeichen eines anderen Bereichs umgerechnet werden.

Die österreichische Datenschutzkommission betreibt in ihrer Funktion als Stammzahlenregisterbehörde weiters zwei Register, in die sich jene natürlichen Personen und sonstigen rechtlich erheblichen Entitäten (zB Behörden oder ARGEs) eintragen lassen können, die in keinem der Basisregister des e-Governmentsystems eingetragen sind und daher noch keine Identifikation für das e-Government-System besitzen: Es sind dies das Ergänzungsregister für natürliche Personen (die nicht im Melderegister enthalten sind) und das Ergänzungsregister für sonstige Betroffene (die nicht im Firmenbuch oder im Vereinsregister enthalten sind).

Im Jahr 2007 wurden unter der Aufsicht der Datenschutzkommission

17.750.000 bereichsspezifische Personenkennzeichen und

36.400.000 verschlüsselte bereichsspezifische Personenkennzeichen,

im Jahr 2008

1.580.000 bereichsspezifische Personenkennzeichen und

53.541.500 verschlüsselte bereichsspezifische Personenkennzeichen berechnet. Die verschlüsselten bPKs dienen dem Verkehr zwischen Behörden unterschiedlicher Verwaltungsbereiche.

9.2 Die Umsetzung der Novelle 2008 zum E-Government-Gesetz

Im Berichtszeitraum war von der Stammzahlenregisterbehörde auch die Umsetzung der Novelle zum E-Government-Gesetz (BGBl. I Nr. 7/2008) und der die Stammzahlenregisterbehörde betreffenden Verordnungen durchzuführen.

Die wichtigste Neuerung der Novelle besteht darin, dass Banken und Versicherungen unter gewissen Voraussetzungen bereichsspezifische Personenkennzeichen verwenden dürfen. Dadurch könnte einerseits die Qualität der Identitätsdaten der Kunden dieser Unternehmen erheblich verbessert werden, zum anderen wäre der Zugang zum Electronic Banking technisch wesentlich besser absicherbar als mit den derzeit üblichen PINs und TANs der TAC Systeme. Von diesem Angebot haben diese Unternehmen allerdings bisher keinen umfassenden Gebrauch gemacht.

Die Stammzahlenregisterbehördenverordnung 2009, BGBl. II Nr. 330/2009 und die Ergänzungsregisterverordnung 2009 BGBl. II Nr. 331/2009 haben die Kompetenzen und den Handlungsspielraum der Stammzahlenregisterbehörde zwar erweitert, gehen aber davon aus, dass die mit diesen Kompetenzen verknüpften E-Government-Funktionen selten genützt werden, weshalb diesbezüglich bis jetzt weitgehend auf die Einrichtung von Online-Applikationen verzichtet wurde. Dies bedeutet aber für die Stammzahlenregisterbehörde dass sie immer dann, wenn kein automatisiertes Verfahren oder kein Dienstleister für eine der von der Stammzahlenregisterbehörde verwalteten E-Government Applikationen vorgesehen sind, sie diese Anträge manuell zu behandeln hat, wofür ihre Personalausstattung nicht ausreicht. In diesem Bereich wird daher noch nachgerüstet werden müssen, möglicherweise auch durch Heranziehung weiterer Dienstleister für spezielle Funktionen.

9.3 Die Vorbereitung der Volkszählung neuen Stils (Registerzählung)

Im Berichtszeitraum war die Stammzahlenregisterbehörde neben der Führung und Überwachung des laufenden Betriebs der verschiedenen technischen Einrichtungen und der mit der Umsetzung beauftragten Dienstleister vor allem auch mit der Betreuung öffentlicher Auftraggeber im Zusammenhang mit der Ausstattung ihrer Datenanwendungen für die neue Registerzählung aufgrund des Registerzählungsgesetzes, BGBl. I Nr. 33/2006, beschäftigt.

Die Feuerprobe hatte die Stammzahlenregisterbehörde bereits im Rahmen der Registerprobezählung 2006[20] bestanden, wo ein beachtlicher Koordinationsaufwand unter hohem Zeitdruck entstand, weil parallel zum Einsatz der Anwendungen der Stammzahlenregisterbehörde für die Erstausstattung der größten österreichischen Register mit bereichsspezifischen Personenkennzeichen diese Anwendungen noch entwickelt oder weiterentwickelt werden mussten. Die damit verbundenen Arbeiten fanden schwerpunktmäßig im Zeitraum von Jänner 2007 bis Juni 2008 statt. Es wurden für die Probezählung ca. 100 Millionen bereichsspezifische Personenkennzeichen berechnet.

Mit dem Registerzählungsgesetz wurde eine völlig neue Methode der Volks-, Gebäude-, Wohnungs- und Arbeitsstättenzählungen in Österreich eingeführt. Seitdem werden die Informationen nicht mehr von den Bürgern eingeholt, sondern den vorliegenden Verwaltungsregistern entnommen. Das Zentrale Melderegister bildet das Rückgrat der Registerzählung. Die anderen Hauptregister sind das Gebäude- und Wohnungsregister, das Unternehmensregister und das Bildungsstandregister sowie

[20] http://www.statistik.at/web_de/static/bericht_ueber_die_probezaehlung_2006_036181.pdf

das Register des Hauptverbandes der österreichischen Sozialversicherungsträger, die Daten des Arbeitsmarktservice und die *Stamm*daten der Abgabenbehörden des Bundes (nicht jedoch die Einkommensdaten).

Bei der Registerzählung werden die Daten aus den teilnehmenden Registern nicht mit dem Namen der Betroffenen sondern *ausschließlich* mit seinem bereichsspezifischen Personenkennzeichen (bPK) an die Bundesanstalt Statistik Österreich geliefert. Die Zusammenführbarkeit von Daten aus den Registern, die unterschiedlichen Verwaltungsbereichen angehören und daher ein- und dieselbe Person unter verschiedenen bPKs führen, und die Überprüfbarkeit der Richtigkeit von Registerdaten durch die Bundesanstalt Statistik Österreich wird durch ein System von kreuzweise verschlüsselten bPKs erreicht: Die Register liefern ihre Daten an die Statistik Austria mit einem nur von der die Bundesanstalt Statistik Österreich entschlüsselbaren bPK für den Bereich „Amtliche Statistik" („AS")[21]. Um Rückfragen der Statistik Austria zu ermöglichen, übermitteln die Register zusammen mit diesem verschlüsselten bPK „AS" ein weiteres nur von ihnen selbst entschlüsselbares verschlüsseltes bereichsspezifisches Personenkennzeichen. Auf diese Weise kann die Bundesanstalt Statistik Österreich mithilfe des von allen Registern zur selben Person immer gleichen bPK „AS" die Daten zusammenführen und kann außerdem im Bedarfsfall mit Hilfe des besonderen von dem jeweiligen Register mitgelieferten verschlüsselten bPKs des Registers über die Richtigkeit gelieferter Daten beim entsprechenden Register Rückfrage halten .

Im Finanzausgleichsgesetz 2008, BGBl. I Nr. 103/2007, wird geregelt, dass ab dem Finanzjahr 2009 die Bundesanstalt Statistik Österreich nach § 9 Abs. 9 leg. cit. die Bevölkerungszahl für den Finanzausgleich jährlich für den 31.10. zu ermitteln hat. Auch bei dieser „Mini"-Registerzählung werden die oben genannten Register zusammengeführt, daher unterscheidet sie sich im Grunde nicht von der Probe- bzw. der eigentlichen Registerzählung. Es tritt lediglich an Stelle der Wohnsitzanalyse gemäß § 5 Abs. 5 des Registerzählungsgesetzes (Befragung der Personen bei unklarem Hauptwohnsitz) ein statistisches Verfahren, das auf den Erfahrungen der Probezählung basiert. Durch diesen Umstand ist die Stammzahlenregisterbehörde nunmehr ständig sowohl technisch als auch organisatorisch mit Anforderungen, die aufgrund von „Mini"-Registerzählungen entstehen, beschäftigt.

Mit Ausnahme der Schülerdaten des Bildungsstandregisters konnten alle großen öffentlichen Register mit bereichsspezifischen Personenkennzeichen ausgestattet werden, sodass mit einem problemlosen Ablauf der Registerzählung 2011 gerechnet werden kann. Hiermit ist auch die Verwendung der Sozialversicherungsnummer zur Identifizierung von Bevölkerungsgruppen nur mehr im Bereich der Schülerdaten gegeben. Aus Sicht der Datenschutzkommission ist es äußerst bedauerlich, dass im Bildungsbereich keine Anstrengungen unternommen wurden, auf die Sozialversicherungsnummer zugunsten des wesentlich datenschutzfreundlicheren bereichsspezifischen Personenkennzeichens zu verzichten.

Auch die Mehrheit der kleineren Register, die an der Registerzählung teilzunehmen haben, (wie zB die Bundeskammer d. Architekten u. Ingenieurkonsulenten) konnten mit bereichsspezifischen Kennzeichen ausgestattet werden. Hier konnte allerdings großteils keine automatische Aktualisierung der sich verändernden Datenbestände durch die Benutzung von online Services der Stammzahlenregisterbehörde realisiert werden, wodurch bei jeder Registerzählung von Neuem ein Arbeitsaufwand entsteht und sämtliche Daten neu abgeglichen werden müssen. Aufgrund der relativ geringen

[21] Siehe dazu die E-Government-Bereichsabgrenzungsverordnung, BGBl. II Nr. 289/2004

Größe dieser Register hielt sich der Mehraufwand bei der Stammzahlenregisterbehörde jedoch in Grenzen.

Insgesamt darf festgestellt werden, dass durch das neue System statistischer „Zählungen“ der Bevölkerung unter verschiedensten Gesichtspunkten (Fragestellungen) datenschutzrechtlich ein erheblicher Fortschritt erzielt wurde, da anstelle von identifizierten Bürgern nur mehr nicht-identifizierte Individuen gezählt werden. Die neue Form der Volkszählung ist somit ein zusätzlicher datenschutzfreundlicher Anwendungsfall des österreichischen e-Government-Systems.

ANHANG:

Erfahrungsbericht über Videoüberwachung

Die Datenschutzkommission hatte sich im Berichtszeitraum auch ausführlich mit der (datenschutz)rechtlichen Einordnung von Videoüberwachung auseinander zu setzen. Schon im Datenschutzbericht 2007 veröffentliche die Datenschutzkommission FAQs und Leitlinien für das Registrierungsverfahren, anhand derer praktisch relevante Fälle zu prüfen waren. Mit 1. Jänner 2010 sehen sich sowohl die datenschutzrechtlichen Auftraggeber wie auch die Betroffenen (und auch die Datenschutzbehörden) mit einer neuen Rechtslage betreffend Videoüberwachung gegenüber. Diese Rechtslage spiegelt dem Grunde nach die Rechtsprechung der Datenschutzkommission in den letzten Jahren, ua. daher auch im Berichtszeitraum, wieder. Dennoch ergeben sich aus den gesetzlichen Entwicklungen auch einige Änderungen und Widersprüchlichkeiten zur entwickelten Rechtssprechung. Diese Punkte sowie die wichtigsten Entscheidungen der Datenschutzkommission im Berichtszeitraum behandelt dieser Abschnitt:

1. Was ist „Videoüberwachung“?

Im Gegensatz zum Konzept, von dem die Datenschutzkommission ausging, nämlich unter „Videoüberwachung“ die Beobachtung, einer Örtlichkeit mit Hilfe von Videokameras zu verstehen[22], definiert der Gesetzgeber „Videoüberwachung“ nunmehr am Beginn des 9a. Abschnitts ua mit Bezug auf [23] „die systematische, fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt oder eine bestimmte Person betreffen“. Dabei macht es keinen Unterschied, ob die Aufnahme durchgehend erfolgt, oder etwa nur zu den Nachtstunden oder nur am Wochenende, ob der Aufnahmefall von einem äußeren Ereignis abhängig ist (zB Bewegungsmelder, Taster) oder ob etwa nur ein Foto alle 10 Minuten angefertigt wird. Aufnahmen zu rein persönlichen bzw. familiären Zwecken (durch eine natürlichen Person), wie zB das Babyfon, oder touristische/künstlerische Aufnahmen sind nicht erfasst (§ 45 DSG 2000). Die Veröffentlichung (also Übermittlung) dieser Daten stellt aber einen rechtlich zu beurteilenden Eingriff in das Grundrecht auf Datenschutz dar.

Daneben gibt es noch Anwendungen, die keinen Kontrollzweck verfolgen, und dementsprechend nicht nach den Bestimmungen des 9a. Abschnitts zu beurteilen sind, sondern an allgemeinen datenschutzrechtlichen Regelungen zu messen sind. So können etwa Bildaufnahmen oder -übertragungen zu wissenschaftlichen oder statistischen Zwecken im Rahmen der Bestimmungen des § 46 DSG 2000 zulässig sein.[24]

Während die Datenschutzkommission in ihrer Judikatur als Zweck für Videoüberwachung zwischen Eigenschutz[25] (insbesondere Eigentumsschutz), Verantwortungsschutz[26] und Fremdschutz[27] unter-

[22] Siehe Datenschutzbericht 2007, 64.
[23] § 50a Abs. 1 DSG 2000.

[24] Datenschutzkommission, 24.7.2009, K202.084/0004-DSK/2009; 12.5.2010, K202.094/0004-DSK/2010.
[25] „**Eigenschutz**“ umfasst den Schutz der Person und des Eigentums des Auftraggebers, aber auch den Schutz seiner Organe (Organwalter), also seiner Mitarbeiter etc.
[26] Mit „**Verantwortungsschutz**“ werden jene Fälle bezeichnet, in welchen der Auftraggeber den Schutz von Personen aus dem Titel der Verkehrssicherungspflicht oder aus vorvertraglichen Verpflichtungen und dergleichen vorzusorgen hat.
[27] Unter „**Fremdschutz**“ wird der Schutz von Personen verstanden, zu welchen ein privater Auftraggeber einer Videoüberwachung in keiner Rechtsbeziehung steht. Der „Fremdschutz“ gegen sicherheitspolizeiliche Gefahren ist Monopol der Sicher-

schied[28], sind für den Gesetzgeber nur folgende Zwecke rechtmäßig für „Videoüberwachung“ im definierten Sinne:[29] Rechtmäßige Zwecke einer Videoüberwachung, insbesondere der Auswertung und Übermittlung der dabei ermittelten Daten, sind nur der Schutz des überwachten Objekts oder der überwachten Person (also: Eigenschutz), oder die Erfüllung rechtlicher Sorgfaltspflichten (also Verantwortungsschutz), jeweils einschließlich der Beweissicherung (im Hinblick auf Ereignisse nach Abs. 1).

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

- Werbung für einen Veranstaltungsort durch Veröffentlichung der Aufnahmen im Internet („WebCam“-Anwendungen; zB Wetter- oder Tourismuskameras)
- wissenschaftliche Untersuchungen (zB Wegeleitsysteme, Verhalten von Personengruppen)

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

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

Bilddaten sind dann personenbezogene Daten, wenn die Kameraeinstellung es grundsätzlich erlaubt, die aufgenommenen Personen (insbesondere: deren Gesichtszüge) zu erkennen. (vgl. hiezu auch Beispiel Nr. 3 im Arbeitspapier WP 136 der Art. 29 Gruppe[30] über den Begriff der „personenbezogenen Daten“).

Für das Vorliegen einer „Verarbeitung personenbezogener Daten“ kommt es nicht darauf an, ob die aufgenommen Personen tatsächlich identifiziert werden; es genügt vielmehr, dass diese grundsätzlich identifizierbar sind (vgl. hiezu § 4 Z 1 DSG 2000 bzw. Art. 2 (a) der Datenschutz-RL 95/46/EG). „Identifizierbar“ sind Daten auch dann, wenn nicht der Aufnehmende, sondern nur ein Dritter (zB eine Sicherheitsbehörde) voraussichtlich in der Lage sein wird, eine Identifikation erfolgreich vorzunehmen (so Erwägungsgrund 26 der RL 95/46/EG). Dafür reicht es aus, wenn die Identitätsfeststellung nachträglich durch Zuordnung der Bilddaten zu Namen durch die Zusatzinformationen Datum, Zeit und Ort der Aufnahme unter Zuhilfenahme weiterer Mittel (zB Personenbeschreibung, Fahndungsdaten, Namenslisten etc) erfolgt oder erfolgen kann.

Das Vorliegen personenbezogener Daten und damit die Anwendbarkeit des DSG 2000 kann nur dort ausgeschlossen werden, wo aufgrund des Standortes der Kamera im Zusammenspiel mit der Auflösung der Bilddaten die Identifizierung von Personen ausgeschlossen werden kann. Dies ist in der Regel der Fall, wenn Gesichter nicht erkennbar sind.

Ob Bilddaten aber, wie die Datenschutzkommission vertreten hat, generell nicht als sensible Daten iSd § 4 Z 2 DSG 2000 (obwohl Rückschlüsse auf Gesundheit oder ethnische Herkunft möglich sind) gelten (weshalb § 9 DSG 2000 zur Beurteilung der schutzwürdigen Geheimhaltungsinteressen nicht einschlägig wäre), kann nunmehr dahingestellt bleiben, weil der Gesetzgeber eben für Videoüberwachung eine Sonderregel getroffen hat. Die Durchsuchung von mit einer Videoüberwachung gewonnenen Daten nach sensiblen Daten

heitsbehörden und kann von Privaten nicht als Rechtsgrundlage für ihre Videoüberwachung in Anspruch genommen werden.

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

[29] § 50a Abs. 2 DSG 2000.

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

als Auswahlkriterium ist aber unzulässig (§ 50a Abs. 7 DSG 2000).

3. Zur Meldepflichtigkeit von Videoüberwachung

Nur „Datenanwendungen" müssen dem Datenverarbeitungsregister gemeldet werden (vgl. §§ 16 ff DSG 2000). Eine „Datenanwendung" liegt vor, wenn die zur Erreichung des Zwecks der Datenanwendung vorgenommenen Verarbeitungsschritte „zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen" (§ 4 Z 7 DSG 2000). Die Datenschutzkommission vertrat die Ansicht, dass nur die Videoüberwachung mit Datenaufzeichnung eine „Datenanwendung" ist.

Dabei stellt digitale Bildaufzeichnung jedenfalls eine „Datenanwendung" dar, analoge Datenaufzeichnung nur dann, wenn sie als „Datei" iSd § 4 Z 6 DSG 2000 organisiert ist (vgl. hiezu § 58 DSG 2000). Auch dann aber, wenn ein konkreter Einsatz von Videokameras nicht als „Datenanwendung" zu werten ist, unterliegt dieser Sachverhalt zumindest den Regelungen des Grundrechts auf Datenschutz.

Videoüberwachung, die zum Zweck der Verhinderung und Verfolgung von strafbarem Verhalten durchgeführt wird, gilt nicht als Datenverwendung für „rein private oder familiäre Tätigkeiten", da hier die Verwendung der Bilddaten für einen nichtprivaten Zweck, nämlich den der Strafverfolgung, im Vordergrund der Datenermittlung steht. Videoüberwachung für diesen Zweck wird daher – sofern sie eine Datenanwendung darstellt – grundsätzlich als meldepflichtig angesehen.

Videoüberwachung, die hingegen für rein private oder familiäre Datenanwendung betrieben wird (wie zB ein Babyfon mit Aufzeichnung), ist nicht meldepflichtig. Die Datenschutzkommission sieht in ihrer Judikatur[31] unter dieser Ausnahme auch die reine Zugangsüberwachung von Einfamilienhäusern – auch bei Zweck der Verhinderung und Verfolgung von strafbarem Verhalten –, sofern weder öffentlicher Grund noch Grund von Dritten erfasst ist. Diese Aufnahmen können im Rahmen des § 45 Abs. 2 DSG 2000 als Beweismaterial vor Polizei und Gericht herangezogen werden (vgl nunmehr allerdings die Abgrenzungskriterien der Standard- und Muster-Verordnung weiter unten).

Die Meldepflicht trifft generell den Auftraggeber (§ 4 Z 4 DSG 2000), auch wenn er die Durchführung der Überwachung einem Anderen überlässt. Dieser Dritte, zB auch ein Privatdetektiv, ist bloßer datenschutzrechtlicher Dienstleister (§ 4 Z 5 DSG 2000), solange er seinen Auftrag nicht überschreitet.

Durch die Änderungen der DSG-Novelle 2010 ist klargestellt, dass Videoüberwachungen der Meldepflicht gemäß den §§ 17ff DSG 2000 unterliegen (§ 50c Abs. 1 DSG 2000), von der lediglich Fälle der Echtzeitüberwachung sowie Aufzeichnungen auf einem analogen Speichermedium (wegen mangelnder Strukturiertheit) ausgenommen sind.[32]

Überdies erging kürzlich (außerhalb des Berichtszeitraumes) eine Novelle zur Standard- und Muster-Verordnung[33], mit der ein Standard Videoüberwachung (SA032) geschaffen wurde, der Videoüberwachungsanlagen in Banken, Juweliergeschäften (inkl. Handel mit Antiquitäten und Kunstgegenständen, Gold- und Silberschmied), Trafiken und Tankstellen von der Meldepflicht ausnimmt, wenn sie sich innerhalb des Standards bewegen (insbesondere betreffend der überwachten Bereiche und der Aufzeichnungsdauer von 72 Stunden). Schließlich wird mit dieser Novelle zur StMV auch die Überwachung von „bebauten Privatgrundstücken (samt

[31] Datenschutzkommission 8.5.2009, K600.064-001/0002-DVR/2009.
[32] § 50c Abs. 2 DSG 2000; neben den Fällen des § 17 Abs. 2 und 3 DSG 2000.
[33] BGBl. II Nr. 152/2010.

Hauseingang und Garage)“ von der Meldepflicht ausgenommen, wenn der Standard nicht verlassen wird (insbesondere soweit die Aufzeichnungsdauer von 72 Stunden nicht überschritten wird).

Der Gesetzgeber stellt überdies – im Sinne der bisher im Datenverarbeitungsregister geübten Praxis – klar, dass mehrere überwachte Objekte oder überwachte Personen, für deren Videoüberwachung derselbe Auftraggeber eine gesetzliche Zuständigkeit oder rechtliche Befugnis (§ 7 Abs. 1) hat, auf Grund ihrer gleichartigen Beschaffenheit oder ihrer räumlichen Verbundenheit in einer Meldung zusammengefasst werden können, wenn sich diese auf die gleiche Rechtsgrundlage stützt. Insbesondere für den Filialbetrieb kommt dieser Regelung Bedeutung zu (§ 50c Abs. 3 DSG 2000).

4. Wann darf eine Videoüberwachungsanlage in Betrieb genommen werden?

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

Durch § 50c Abs. 1 DSG 2000 ist nunmehr klargestellt, dass Videoüberwachungen der Vorabkontrolle (§ 18 Abs. 2 DSG 2000) unterliegen, sofern der Auftraggeber nicht in der Meldung zusagt, die Videoüberwachungsdaten zu verschlüsseln und unter Hinterlegung des einzigen Schlüssels bei der Datenschutzkommission sicherzustellen, dass eine Auswertung der Videoaufzeichnungen nur im begründeten Anlassfall durch eine bestimmte Stelle stattfindet. Zu erinnern ist auch daran, dass die der Standard- und Muster-Verordnung entsprechenden Videoaufzeichnungen ja überhaupt von der Meldepflicht ausgenommen sind.

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

Jede Ermittlung personenbezogener Daten stellt einen Eingriff in das Grundrecht auf Datenschutz dar. Eingriffe sind nur unter den Voraussetzungen des § 1 Abs. 2 DSG 2000 erlaubt. Auch die Ermittlung von Bilddaten mit Videokameras ist daher nur unter den Voraussetzungen des § 1 Abs. 2 DSG 2000 zulässig, d.h. wenn entweder die Zustimmung aller Betroffenen vorliegt oder die Ermittlung im lebenswichtigen Interesse der Betroffenen notwendig ist oder ein überwiegendes berechtigtes Interesse eines anderen – insbesondere des Auftraggebers – gegeben ist. Überdies ist natürlich auch für private Auftraggeber eine spezielle gesetzliche Grundlage iSd § 1 Abs. 2 DSG 2000 für Videoüberwachung denkbar.

Während im Fall von Videoüberwachung regelmäßig die Zustimmung aller potentiell Betroffenen schwer einzuholen bzw. nachzuweisen sein und eine Überwachung im lebenswichtigen Interesse nur in den seltensten Fällen vorliegen wird, ist die Prüfung eines überwiegenden berechtigten Interesse des Auftraggebers der Regelfall.

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

Angesichts des Verhältnismäßigkeitsgebots (§ 1 Abs. 2 letzter Satz DSG 2000) für

jeden Grundrechtseingriff ist weiters der Nachweis erforderlich, dass ein festgestelltes berechtigtes Interesse an der Datenverwendung in einer bestimmten Konstellation das (ebenfalls berechtigte) Interesse des Betroffenen an der Geheimhaltung seiner Daten überwiegt. Nur bei Vorliegen eines „*überwiegenden berechtigten Interesses*" ist die Verwendung personenbezogener Daten tatsächlich zulässig.

An dieser grundsätzlichen Sichtweise ändern auch die in der DSG-Novelle 2010 zur Zulässigkeit von Videoüberwachung vorgesehenen Bestimmungen nichts (siehe dazu ausführlicher sogleich im nächsten Punkt).

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

Videoüberwachung für behördliche Zwecke bedarf jeweils einer besonderen gesetzlichen Grundlage (vgl. den Gesetzesvorbehalt in § 1 Abs. 2 DSG 2000 und Art. 18 B-VG). Die Zulässigkeit von Videoüberwachung für sicherheitsbehördliche Zwecke ist im Sicherheitspolizeigesetz abschließend geregelt (vgl. § 54 Abs. 6 und 7 SPG). Die Sicherheitsbehörden selbst dürfen Videoüberwachung nur an „öffentlichen Orten" betreiben, d.h. an Orten, die von einem nicht von vornherein bestimmten Personenkreis betreten werden können (§ 27 Abs. 2 SPG).

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

Private können ein „berechtigtes Interesse" an Videoüberwachung (im Sinne einer systematischen Kontrolle eines Raumes) allenfalls aus dem Bestehen eines „hausrechtsähnlichen Verfügungsrechts" ableiten, d.h. aus dem Recht, über das Betreten eines Ortes und Sich-Aufhalten an diesem Ort zu verfügen. Private können daher überhaupt nur dort Videoüberwachung betreiben, wo das Bestehen bzw. der Schutz dieses Verfügungsrechts denkbar ist, also nicht im „öffentlichen Raum".[34] Den „Privaten" gleichzuhalten sind Auftraggeber des öffentlichen Bereichs bei der Besorgung von Aufgaben der Privatwirtschaft.

Betreffend die Einteilung des Raumes aus dem Blickwinkel der Verfügungsberechtigung über den Zutritt kann folgendes gesagt werden:

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

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

- „Öffentlicher Raum" ist jener Bereich, in dem sich jedermann grundsätzlich unbeschränkt aufhalten darf und eine Zutrittkontrolle rechtlich nicht – oder nur aus besonderem Anlass – zulässig ist. Dies

[34] Dabei gibt es natürlich Grenzfälle wie die Grundstücksgrenze oder die Hausfassade.

betrifft etwa Straßen, Plätze, die freie Natur etc.

– „Beschränkt öffentlicher Raum“ ist jener Bereich, in dem zwar ein privatrechtliches Verfügungsrecht über die Örtlichkeit besteht, die Berechtigung des Zutritts jedoch nicht auf von vornherein bestimmte Personen (zB „Schüler der Schule“, „Patienten“ etc.) beschränkt ist. Demgegenüber stehen Räumlichkeiten, zu welchen der Zutritt nur bestimmten Personen gestattet ist, zB den Mitarbeitern eines Unternehmens. Dieser Bereich wird im Folgenden als „nichtöffentlicher Raum“ bezeichnet, wobei hier als besondere Kategorie noch der „private Raum“ unterschieden werden kann, der rein privaten, insbesondere Wohnzwecken vorbehalten ist. Diese Unterscheidung schien hinsichtlich des Ausmaßes der Verfügungsgewalt über den Zutritt sinnvoll.

Das Vorliegen eines „berechtigten Interesses“ Privater an einer Videoüberwachung ergibt sich aus dem Zweck, zu dem die Videoüberwachung betrieben werden soll, und dem Ausmaß der Verfügungsberechtigung über den Ort, der überwacht werden soll. Die Datenschutzkommission zog dabei für ihre Beurteilung die Matrix auf dieser Seite heran, die verdeutlicht, in welchen Konstellationen ein berechtigtes Interesse eines Privaten an einer Videoüberwachung denkmöglicherweise bestehen kann (ob die Videoüberwachung im Einzelfall tatsächlich zulässig ist, hängt davon ab, ob das berechtigte Interesse im konkreten Fall als „überwiegend“ zu werten ist, siehe dazu den nächsten Punkt).

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

Auch dort, wo grundsätzlich nur Behörden aufgrund besonderer gesetzlicher Ermächtigung Videoüberwachung betreiben dürfen, also im „öffentlichen Raum“, können Private als Dienstleister solcher Auftraggeber an der Videoüberwachung mitwirken – sie leiten ihre Berechtigung diesfalls aus den gesetzlichen Zuständigkeiten der Auftraggeber ab.[35]

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

Bei der Vornahme von Videoüberwachung für Zwecke der Wahrnehmung behördlicher Aufgaben wird diese Frage durch jene gesetzlichen Bestimmungen beantwortet, die angesichts des Gesetzesvorbehalts des § 1 Abs. 2 DSG 2000 als Grundlage eines solchen Grundrechtseingriffs vorhanden sein müssen. Nunmehr legt auch die DSG-Novelle 2010 für private Auftraggeber fest, wann diese überwiegenden berechtigten Interessen zur Videoüberwachung vorliegen (siehe dazu sogleich unten).

Für die Rechtslage 2009 galt nun:

spw. Datenschutzkommission 11. 7. 59/0016-DSK/2008. Gegen diesen lie Erstbeschwerdegegnerin gemäß B-VG Beschwerde an den Verwalf (VwGH) erhoben. Mit Erkenntnis ıber 2009, Zl. 2008/17/0152-8, hat Beschwerde stattgegeben und den attgebenden) Spruchpunkt 1. aufge- ıuszug aus den Entscheidungsgrün-

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

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

Schwieriger ist die Beurteilung, ob ein überwiegendes berechtigtes Interesse vorliegt, in Fällen der Videoüberwachung von Verkaufsräumen allgemein, des Eingangsbereich zu Wohnhäusern oder Wohnungen, von Gebäudefassaden etc. Die Frage etwa, ob grundsätzlich von einer besonderen Gefährdung durch Wohnungseinbrüche oder Fassadenbeschädigung durch Grafitti auszugehen ist und daher die Videoüberwachung des Eingangs- oder Fassadenbereichs von Häusern immer ein „überwiegendes berechtigtes Interesse“ darstellt, muss differenziert beantwortet werden: Wesentlich ist zunächst, ob und wieweit durch die Überwachung auch öffentlicher Raum (zB der Gehsteig vor dem Haustor) betroffen ist; dies ist entsprechend der obigen Matrix nur im Ausnahmefall zulässig, d. h. nur im absolut unvermeidlichen sachlichen und räumlichen Ausmaß. Es wird daher zB einer den Eingang vom Hausinnern her überwachenden Anlage der Vorzug zu geben sein vor einer auch den Gehsteig erfassenden Vorrichtung. Die Datenschutzkommission hat in diesen Fällen bisher eine allgemein erhöhte Gefahrenlage verneint, sodass der Nachweis einer konkreten Gefährdung, etwa durch Nachweis von Vorfällen, die mit dem zweckgebundenen Einsatz der Anlage vermieden werden sollen, im überwachten Raum selbst oder in der unmittelbaren Nachbarschaft dieses überwachten Raumes, erforderlich ist.

Es muss in jedem Fall der Verhältnismäßigkeitsgrundsatz und das „Prinzip des gelindesten (Eingriffs-)Mittels“ zur Anwendung gebracht werden. Im nichtöffentlichen Raum sind es nicht die Datenschutzinteressen der Allgemeinheit, die durch Videoüberwachung betroffen werden, sondern die der speziell zutrittsberechtigten Personen. Wo hier das überwiegende berechtigte Interesse jeweils liegt (bei der Datenermittlung durch Videoüberwachung oder beim Recht auf Datenschutz) hängt vom Zweck der Videoüberwachung, von der Natur der Rechtsbeziehung zwischen Auftraggeber und Überwachten etc. ab. Die Videoüberwachung eines solchen Raumes zu Zeiten, in welchen sich dort niemand zulässigerweise aufhält (etwa während der Nachtstunden), wird regelmäßig als zulässig anzusehen sein, da hier niemand vorrangige Datenschutzinteressen geltend machen kann, wenn er unberechtigterweise solchen Raum betreten hat und dabei gefilmt wird. (Festzuhalten ist, dass ein- und derselbe Raum seinen Charakter je nach Widmung durch den Verfügungsberechtigten ändern

kann – etwa von „beschränkt öffentlich“ während der Tageszeit auf „nichtöffentlich“ während der Nachtstunden). Konflikte hinsichtlich gegenläufiger berechtigter Interessen können sich jeweils nur gegenüber solchen Personen ergeben, die berechtigt sind, sich im überwachten Bereich aufzuhalten.

Mit der DSG-Novelle 2010 drückt der Gesetzgeber nun selbst aus, wann er ein überwiegendes berechtigtes Interesse zur Videoüberwachung iSd oben genannten Definition verwirklicht sieht:

Jedenfalls zulässig, also ohne Verletzung schutzwürdiger Geheimhaltungsinteressen des Betroffenen, ist Videoüberwachung demnach, wenn entweder die Videoüberwachung im lebenswichtigen Interesse einer Person erfolgt, oder Daten über ein Verhalten verarbeitet werden, das ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden, oder der Betroffene der Verwendung seiner Daten im Rahmen der Überwachung ausdrücklich zugestimmt hat.[36] Jeder dieser Fälle hat einen engen Anwendungsbereich: die Schwierigkeiten mit der datenschutzrechtlichen Zustimmung bei Videoüberwachung wurden schon oben geschildert. Videoüberwachung im lebenswichtigen Interesse des Betroffenen wäre etwa dort denkbar, wo diese unmittelbares Handeln ermöglicht, also nur bei Echtzeitüberwachung, etwa bei Übertragung aus dem Krankenzimmer einer Intensivstation zur Stationswarte. Die Ausnahme betreffend Daten eines Betroffenen über sein öffentlich wahrnehmbares Verhalten können eine Videoüberwachung dem Grunde nach überhaupt nicht rechtfertigen, sondern jeweils nur die konkrete Verwendung dieser Bilddaten des konkreten Betroffenen.

Jedenfalls unzulässig ist Videoüberwachung betreffend Ereignisse an Orten, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen[37] sowie die Videoüberwachung zum Zweck der Mitarbeiterkontrolle an Arbeitsstätten, wobei dieser Fall die Leistungskontrolle der Mitarbeiter verbietet, die Videoüberwachung an Arbeitsstätten zu anderen Zwecken aber nicht ausschließt.[38] Überdies erklärt der Gesetzgeber den automationsunterstützten Bildabgleich sowie die Durchsuchung der gewonnenen Videodaten nach sensiblen Daten (§ 4 Z 2 DSG 2000) als Auswahlkriterium als unzulässig.[39]

Im Großteil der Fälle wird für die Frage der Zulässigkeit von Videoüberwachung im Rahmen der Verhältnismäßigkeitsprüfung wiederum auf eine Interessensabwägung abgestellt, wobei allerdings der Gesetzgeber vorgibt, unter welchen Voraussetzungen schutzwürdige Geheimhaltungsinteressen der Betroffenen nicht verletzt werden.[40] Dies ist der Fall, wenn

− bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt oder die überwachte Person könnte das Ziel oder der Ort eines gefährlichen Angriffs werden, oder

− unmittelbar anwendbare Rechtsvorschriften des Völker- oder des Gemeinschaftsrechts, Gesetze, Verordnungen, Bescheide oder gerichtliche Entscheidungen dem Auftraggeber spezielle Sorgfaltspflichten zum Schutz des überwachten Objekts oder der überwachten Person auferlegen, oder

− sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte Objekt/die überwachte Person betreffenden Ereignisse erschöpft, diese also weder gespeichert (aufgezeichnet) noch in sonst einer anderen Form weiterverarbeitet werden (Echtzeitüberwachung), und sie zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt.

[36] § 50a Abs. 3 DSG 2000.

[37] Etwa Umkleidekabinen, Toiletten oder fremde Privatwohnungen.

[38] § 50a Abs. 5 DSG 2000.

[39] § 50a Abs. 7 DSG 2000.

[40] § 50a Abs. 4 DSG 2000. Man beachte, dass diese Vorgaben nur gelten, wenn Videoüberwachung nicht im Rahmen der Vollziehung hoheitlicher Aufgaben erfolgt.

Mit dem ersten Fall beschreibt der Gesetzgeber den Fall, der bis dato in der Judikatur der Datenschutzkommission als Eigenschutz bezeichnet wurde, mit dem zweiten Fall den Verantwortungsschutz (der allerdings nach dem Gesetzeswortlaut nicht aus vertraglichen Vereinbarungen resultieren darf). Schließlich ist auch die Echtzeitüberwachung zum Eigenschutz zulässig.

8. Auskunftsrecht bei Videoüberwachung

Mit der Auftraggeberschaft einer Datenanwendung verbunden stellt sich auch die Frage nach der Geltendmachung des Auskunftsrechts gemäß § 26 DSG 2000. Im Zusammenhang mit Videoüberwachungsanlagen stellen sich dabei mehrere Probleme. Da Grundvoraussetzung einer erfolgreichen Auskunft das Vorhandensein der Daten ist, wird der Rechtzeitigkeit des Auskunftsbegehrens besonderes Augenmerk zu schenken sein. Ein Auskunftsbegehren muss daher innerhalb der registrierten Aufzeichnungsdauer beim Auftraggeber einlangen – nur dann wirkt die Löschungssperre des § 26 Abs. 7 DSG 2000.

Der Auskunftswerber hat sich auch gegenüber dem Auftraggeber „in geeigneter Form" zu identifizieren. Damit ist die Zuordnung eines Auskunftsbegehrens zu einem bestimmten Betroffenen möglich. Bei Auskünften aus Bildaufzeichnungen besteht allerdings das Problem der Zuordnung eines Abgebildeten zu einem die Auskunft begehrenden Betroffenen (Frage der Authentifikation). Dazu wird es zumindest erforderlich sein, dass der Auskunftswerber im Rahmen seiner Mitwirkungsobliegenheit des § 26 Abs. 3 DSG 2000 die Örtlichkeit und den Zeitraum seines Aufenthalts im überwachten Bereich sowie seine Person (körperliche Merkmale, Kleidung zum gegenständlichen Zeitpunkt) genau umschreibt. Inwieweit darüber hinaus Anforderungen an die Authentifikation gestellt werden müssen, ist durch Rechtsprechung (noch) nicht geklärt.

Schließlich stellt sich bei Videoüberwachung auch die Frage der Form der Auskunftserteilung der Bilddaten selbst. Das Gesetz verlangt Schriftlichkeit, die Auskunft kann daher in der Übergabe der Bilddaten selbst oder in der Beschreibung des Verhaltens des Betroffenen in den Aufnahmen bestehen. Auch hier herrscht in der Judikatur noch keine Klarheit.

Die Datenschutzkommission hat in ihrer Rechtsprechung einen Auskunftsanspruch aus nicht-ausgewerteten Videoaufzeichnung verneint[41], indem sie eine Parallele zu indirekt personenbezogenen Daten zog. Solange der Auftraggeber die Videoaufzeichnungen nicht ausgewertet hat, kennt er die Daten nicht und darf auch regelmäßig von ihnen keine Kenntnis nehmen, es sei denn, dass ein Auswertungsanlass tatsächlich eingetreten ist, der im Registrierungsverfahren als Fall des Vorliegens eines überwiegenden berechtigten Auswertungsinteresses anerkannt wurde. Der Auftraggeber weiß also nicht, „zu wessen Person" Daten gespeichert sind, und darf es auch – außer im Auswertungsanlassfall – nicht in Erfahrung bringen. Auch im Fall der indirekt personenbezogenen Daten ist die Identität der Betroffenen dem Auftraggeber unbekannt und darf auch nicht in Erfahrung gebracht werden. Hier hat der Gesetzgeber selbst das Bestehen eines Auskunftsrechts überhaupt verneint. Überdies kommen die Bilder von unbeteiligten Dritten damit nicht einmal dem Auftraggeber selbst zur Kenntnis, geschweige denn dem Auskunftswerber.

Kommt es hingegen zu Auswertungen aus den aufgezeichneten Daten, besteht ein Auskunftsanspruch dem Grunde wohl schon, da keine vergleichbare, einen Auskunftsanspruch ausschließende Wertung des Gesetzgebers gegeben ist bzw zur Auslegung seines Willens herangezogen werden kann. Inwieweit und in welcher Form dann tatsächlich Auskunft gegeben werden muss, hängt wohl von einer Interessenabwägung ab, die der Gesetzgeber mit § 26 Abs. 2 DSG 2000 prinzipiell anerkennt. Auswertungsfälle, die länger beim Auftraggeber gespeichert werden, werden

[41] Datenschutzkommission, 5.12.2008, K121.385/0007-DSK/2008 et al.

nämlich meist (zumindest bestimmbare) Daten von Personen enthalten, die einen Anlassfall (zB Einbruch, Vandalismus) verwirklicht haben. Eine Auskunft (vielleicht sogar gegenüber dem Täter) könnte dann den Interessen des Auftraggebers so zuwiderlaufen, dass diese als überwiegend iSd zitierten Bestimmung angesehen werden müssen.

Der Gesetzgeber bestimmt nun in § 50e DSG 2000, dass abweichend von § 26 Abs. 1 DSG 2000 dem Auskunftswerber, nachdem dieser den Zeitraum, in dem er möglicherweise von der Überwachung betroffen war, und den Ort möglichst genau benannt und seine Identität in geeigneter Form nachgewiesen hat, Auskunft über die zu seiner Person verarbeiteten Daten durch Übersendung einer Kopie der zu seiner Person verarbeiteten Daten in einem üblichen technischen Format zu gewähren ist. Alternativ kann der Auskunftswerber eine Einsichtnahme auf Lesegeräten des Auftraggebers verlangen, wobei ihm auch in diesem Fall die Ausfolgung einer Kopie zusteht. Die übrigen Bestandteile der Auskunft (verfügbare Informationen über die Herkunft, Empfänger oder Empfängerkreise von Übermittlungen, Zweck, Rechtsgrundlagen sowie allenfalls Dienstleister) sind auch im Fall der Überwachung schriftlich zu erteilen, wenn nicht der Auskunftswerber einer mündlichen Auskunftserteilung zustimmt.

	Auftraggeber, welche eine oder mehrere Videoüberwachung(en) gemeldet haben	Auftraggeber, bei welchen eine oder mehrere Videoüberwachung(en) registriert wurde(n)
2005	25	18
2006	76	12
2007	377	60
2008	1416 (darunter ca. 750 Banken)	279
2009	732	803
gesamt	2626	1172
	Geschätzte Datenanwendungen (Videoüberwachungen) gemeldet	Geschätzte Datenanwendungen (Videoüberwachungen) registriert
gesamt	2660	1200

§ 26 Abs. 2 ist mit der Maßgabe anzuwenden, dass in dem Fall, dass eine Auskunft wegen überwiegender berechtigter Interessen Dritter oder des Auftraggebers nicht in der in Abs. 1 geregelten Form erteilt werden kann, der Auskunftswerber Anspruch auf eine schriftliche Beschreibung seines von der Überwachung verarbeiteten Verhaltens oder auf eine Auskunft unter Unkenntlichmachung der anderen Personen hat.

Das Auskunftsrecht soll nur in Fällen der Echtzeitüberwachung ausgeschlossen sein.

9. Beispiele von Registrierungen

Im DVR sind ca. 2600 Videoüberwachungsanlagen (die von einer bis zu mehrere hundert Kameras umfassen können) gemeldet.

Beispiele von Registrierungen im Berichtszeitraum, bei denen das Vorliegen eines überwiegenden berechtigten Interesses an der Videoüberwachung angenommen wurde:

- Kassensaal einer Bank (Zweck: Eigenschutz und Verantwortlichkeitsschutz)
- Öffentlich zugänglicher Teil eines Museums (Zweck Eigenschutz)

− Eingang und Verkaufsraum eines Juweliergeschäftes (Zweck Eigenschutz)

− Waffen- und Munitionshersteller (Zweck: Eigenschutz, besondere Sicherheitsanforderungen auch aufgrund entsprechender behördlicher Auflagen)

− Fahrzeuge von Unternehmen des öffentlichen Verkehrs (Zweck Eigenschutz [einschl. Schutz der Mitarbeiter] und Verantwortungsschutz [Fahrgäste])

− Bahnhöfe bzw. Stationsgebäude/anlagen an öffentlichen Verkehrslinien (Zweck Eigenschutz [einschl. Schutz der Mitarbeiter] und Verantwortungsschutz [Fahrgäste])

− Fassade von denkmalgeschützten Gebäuden, die an öffentlichen Platz angrenzt (Zweck: Eigenschutz: Schutz vor Vandalismus)

− Geschäftsbereich einer Trafik, einschließlich der Auslage und Zigarettenautomaten (Zweck: Eigenschutz: Schutz vor Überfällen)

− Anlagenbereich einer Tankstellen (Zweck: Eigenschutz: Schutz vor Überfällen, Tankbetrug)

− Geschäftsbereich eines Juweliergeschäftes, einschließlich der Auslage (Zweck: Eigenschutz: Schutz vor Überfällen)

− Abgegrenzter Bereich einer Altstoffsammelinsel („Müllinsel“) (Zweck: Eigenschutz: Schutz vor Fehlablagerungen)

− Ein- und Ausfahrten eines nichteingezäunten Industriegebiets (Zweck: Eigenschutz: Schutz vor Einbruchsdiebstählen; Überwachung nur außerhalb der Geschäftszeiten)

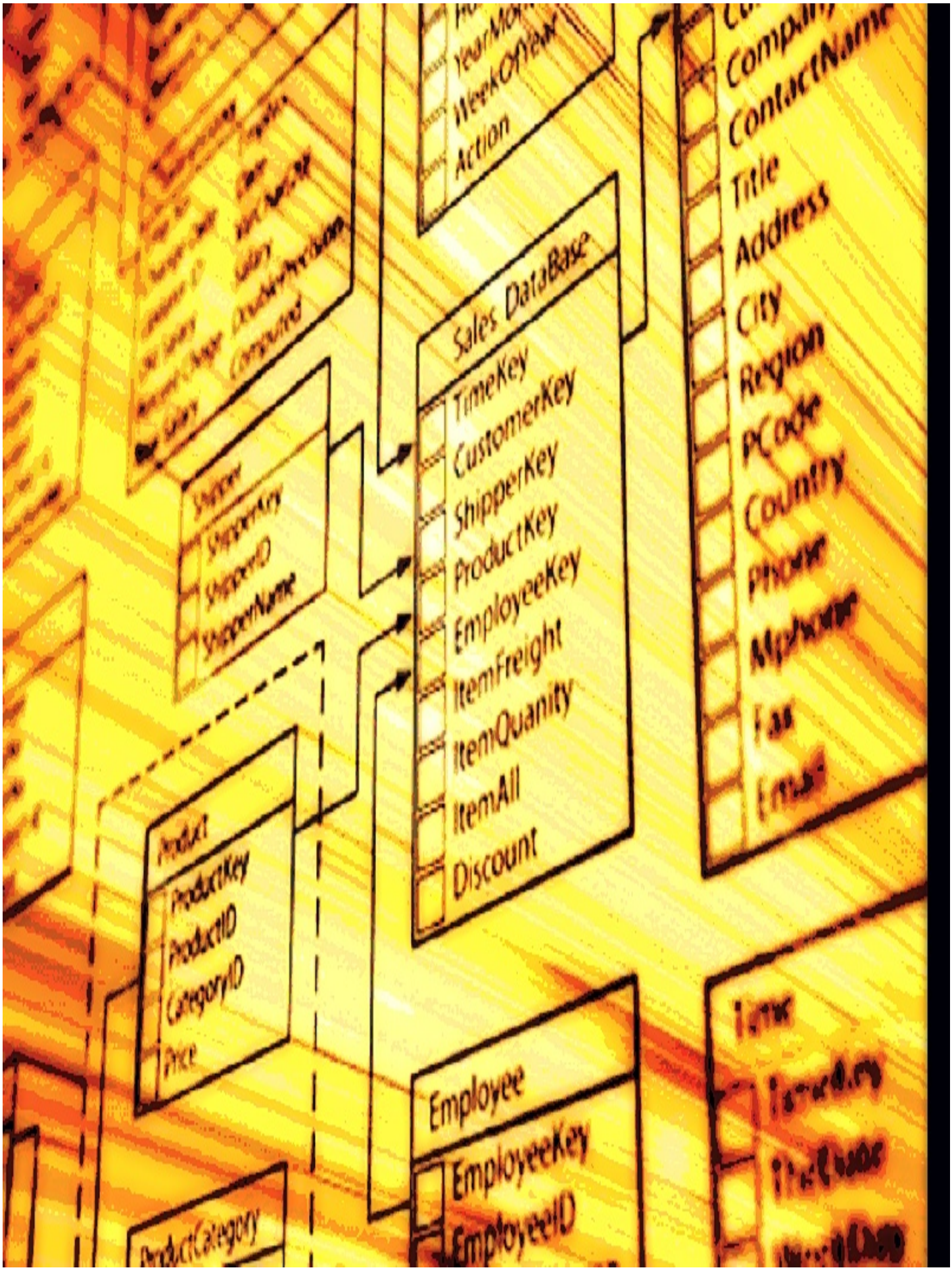
− Zugangsbereich eines Amtsgebäudes (Zweck: Eigenschutz; Privatwirtschaftsverwaltung

− Garage und Müllräume in Mehrparteienwohnhäusern (Zweck: Eigenschutz, Verantwortungsschutz; allerdings Ablehnung der Überwachung der Stiegenhäuser sowie der Zugangsbereiche zu einzelnen Wohnungen)

Videoüberwachungs-Statistiken (zum Stichtag 31.12.2009)

Typen von Videoüberwachungen in Österreich:

- Firmensitze/Betriebsgelände
- Kaufhäuser/Geschäfte
- Trafiken
- Juweliergeschäfte
- Banken
- Geldausgabeautomaten
- Lokale
- Schnellimbiss-Restaurants
- Konferenz-/Messezentren
- Hotels
- Munitionsfabrik
- Energieversorgungseinrichtungen
- Casinos
- Wettcafés
- Mehrparteienhäuser
- Einfamilienhäuser
- Öffentliche Verkehrmittel - Fahrzeuge
- Öffentliche Verkehrmittel - Stationen
- Fahrgastbereich in Taxis
- Parkgaragen/Parkplätze
- Autobahnrastplätze
- Tankstellen
- Spitäler
- Museen
- Theater
- Fußballstadien/Sportplätze
- Abfallsammelstellen
- Schulgelände (Außenbereiche)
- Öffentliche Gebäude (Ministerien, Parlament, Amtsgebäude)
- Öffentliche Plätze (durch die Sicherheitsbehörden aufgrund des SPG)


Sales DataBase
TimeKey
CustomerKey
ShipperKey
ProductKey
EmployeeKey
ItemFreight
ItemQuanity
ItemAll
Discount
Shipper
ShipperKey
ShipperID
ShipperName
Product
ProductKey
ProductID
CategoryID
Price
Employee
EmployeeKey
EmployeeID
ProductCategory
Action
Title
Address
City
Region
Country
Phone
Fax