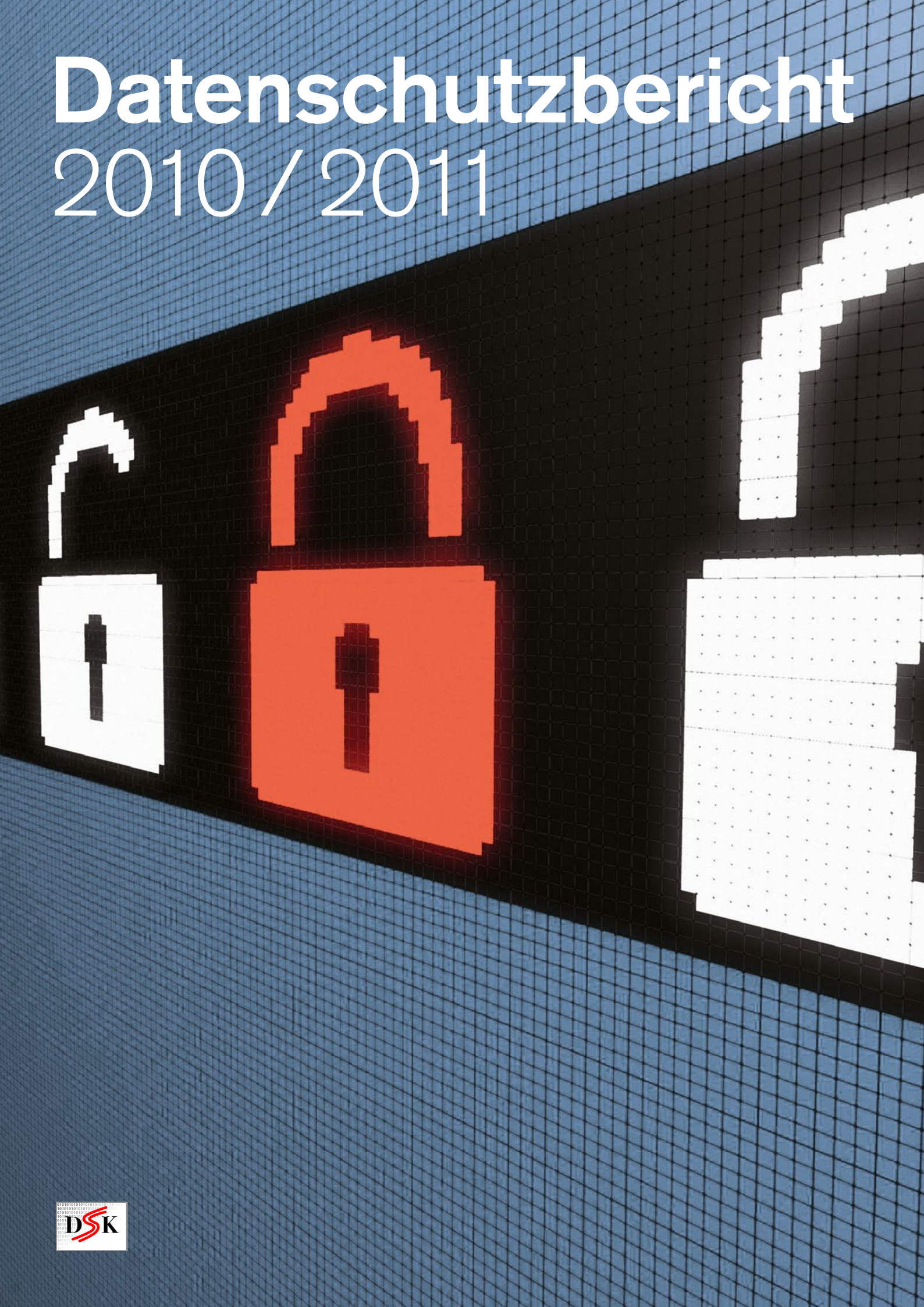
Datenschutzbericht
2010 / 2011



DSK

Datenschutzbericht 2010–2011

Wien, 2012

Impressum

Medieninhaber, Herausgeber und Redaktion:
Datenschutzkommission (DSK, Bundesbehörde
gemäß §§ 35ff DSG 2000), Hohenstaufengasse 3, 1010 Wien.
Kontakt: dsk@dsk.gv.at
Website: www.dsk.gv.at

Fotonachweis: BKA | ARGE Grafik
Gestaltung: BKA | ARGE Grafik
Druck: BM.I Digitalprintcenter
Wien, 2012

Inhalt

1 Einleitung

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

Ihr hiermit vorgelegter vierzehnter Datenschutzbericht umfasst den Zeitraum vom 1. Jänner 2010 bis 31. Dezember 2011. Es handelt sich hierbei um den ersten Datenschutzbericht der mit 1. Juli 2010 bestellten Datenschutzkommission.

Wie im letzten Datenschutzbericht müssen grundsätzliche Erwägungen zur Situation einer Datenschutz-Kontrollbehörde in Österreich, insbesondere auch im Zusammenhang mit der Regierungsvorlage zur Verwaltungsgerichtsbarkeits-Novelle 2012[1] (vgl. Pkt. 5.4. des 13. Datenschutzberichtes, der sich noch auf den Entwurf einer Verwaltungsgerichtsbarkeits-Novelle 2010[2] bezieht) und der beabsichtigten Einführung einer zweistufigen Verwaltungsgerichtsbarkeit 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 letzten Bericht auch auf vorhergehende Amtsperioden der Datenschutzkommission Bezug.

In den Berichtszeitraum fallen auch die ersten Erfahrungen mit der am 1. Jänner 2010 in Kraft getretenen DSG-Novelle 2010 – den dadurch bedingten Änderungen in der Behördenpraxis wird ebenfalls Raum gegeben.

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 Verwaltungsgerichtsbarkeits-Novelle 2012, RV 1618 BlgNR.

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 sechs 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 DSG 2000). 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 Datenschutzkommissionsmitglieder 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 ein Ersatzmitglied sind von der Bundesregierung aus dem Kreis der Bundesbediensteten[7] vorzuschlagen.

2.2 Die Mitglieder der Datenschutzkommission im Berichtszeitraum

Die Zusammensetzung der Datenschutzkommission von 1. Jänner 2010 bis 30. Juni 2010 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

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.

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

Mit 1. Juli 2010 wurden die Datenschutzkommissionsmitglieder neu bestellt. Die Zusammensetzung der Datenschutzkommission von 1. Juli 2010 bis 31. Dezember 2011 war wie folgt:

- Dr. Anton Spenling, Vorsitzender (richterliches Mitglied)
- Dr. Eva Souhrada-Kirchmayer, geschäftsführendes Mitglied
- Mag. Helmut Hutterer
- Dr. Claudia Rosenmayr-Klemenz
- Dr. Klaus Heissenberger
- Mag. Daniela Zimmer

Ersatzmitglieder
- Dr. Gerhard Kuras, stv. Vorsitzender (richterliches Ersatzmitglied)
- Dr. Gregor König, Llm, stv. geschäfts-führendes Mitglied
- Dr. Michaela Blaha
- Mag. Huberta Maitz-Strassnig
- Dr. Josef Gundacker
- 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.

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 richtungsweisender 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 z. B. die Erstattung von Empfehlungen) oder die Vornahme von Registrierungen im Datenverarbeitungsregister (nicht aber z. B. 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 § 7 des E-Government-Gesetzes 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 Die Geschäftsstelle der Datenschutzkommission

3.1 Aufgaben und Organisation der Geschäftsstelle

Die Geschäftsstelle unterstützt die Datenschutzkommission in allen Angelegenheiten der Datenschutzkommission, einschließlich ihrer Aufgaben als Stammzahlenregisterbehörde. In der Geschäftsstelle sind zwei Referate eingerichtet, 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 der Geschäftsstelle 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

Am Ende des Berichtszeitraumes verfügte die Geschäftsstelle über insgesamt 20,55 Planstellen auf Vollbeschäftigungsäquivalent-Basis mit folgender Wertigkeit;

- 11 A/a Planstellen (einschließlich einer Behinderten-Planstelle),
- 2,5 B/b Planstellen und
- 7,05 C/c Planstellen

Davon entfielen 12,05 Planstellen auf das Datenverarbeitungsregister und 8,5 Planstellen auf den restlichen Teil der Geschäftsstelle.

Nach wie vor nimmt das Datenverarbeitungsregister etwa 60 % der gesamten Personalressourcen der Geschäftsstelle in Anspruch, 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 im Rahmen der Kontrollverfahren nach § 30 DSG 2000 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. Eine weiter gehende Entlastung des DVR ist daher unabdingbar. In diesem Zusammenhang ist zu erwähnen, dass der am 25. Jänner 2012 von der Europäischen Kommission vorgestellte Entwurf einer Datenschutz-Grundsatz-Verordnung eine generelle Meldepflicht nicht mehr vorsieht, dass aber riskante Datenverwendungen auch weiterhin vorweg von der Datenschutzbehörde geprüft werden sollen. Es scheint daher erwägenswert, im Lichte dieser geplanten Entwicklungen auf EU-Ebene bereits gewisse Entlastungen im Meldewesen vorzusehen.

Im Berichtszeitraum wurde im Rahmen des Budgetbegleitgesetzes (BGBl. I Nr. 112/2011) eine DSG-Novelle beschlossen, mit der der Zeitpunkt, zu dem die neue DVR-Verordnung spätestens erlassen werden muss, vom 1. Jänner 2012 auf den 1. September 2012 verschoben wurde. Hintergrund für diese Novelle ist die Tatsache,

dass das Unternehmensserviceportal, über das auch ein Großteil der DVR-Meldungen laufen soll, erst später als geplant (nämlich erst etwa ab Mitte des Jahres 2012) zur Verfügung stehen soll. Damit blieb die Belastung des DVR in der derzeitigen Form auch nach dem 1. Jänner 2012 weiterhin aufrecht.

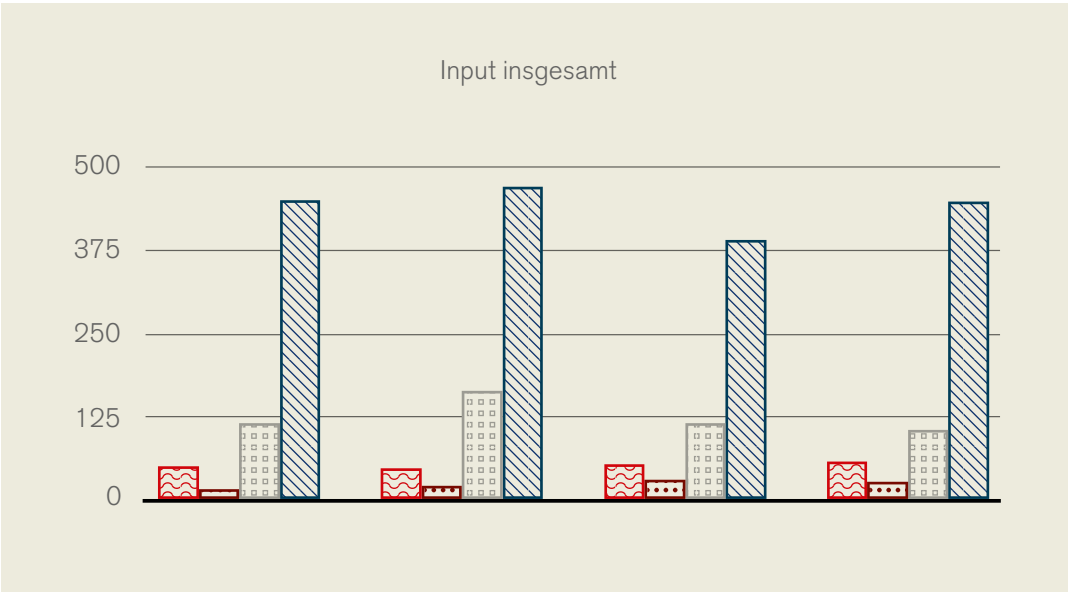
Im Bereich des Büros der Datenschutzkommission traten im Berichtszeitraum zusätzlich zu den »Normalbelastungen« auch noch weitere personelle Engpässe auf, die mit längeren urlaubsbedingten (im Nachhang und im Vorfeld von Karenzurlauben und Mutterschutz) und ausbildungsbedingten Abwesenheiten sowie Krankenständen im Zusammenhang standen.

Im Übrigen wird nochmals darauf hingewiesen, dass von dem 1999 im Vorblatt zur Regierungsvorlage zum DSG 2000 unter »Kosten« 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 wurde überhaupt kein zusätzliches Personal in Rechnung gestellt. An dem Umstand, dass die österreichische Datenschutzkommission im europäischen Vergleich hinsichtlich ihrer Personalausstattung extrem unterdotiert ist, hat sich im Berichtszeitraum somit nichts geändert.

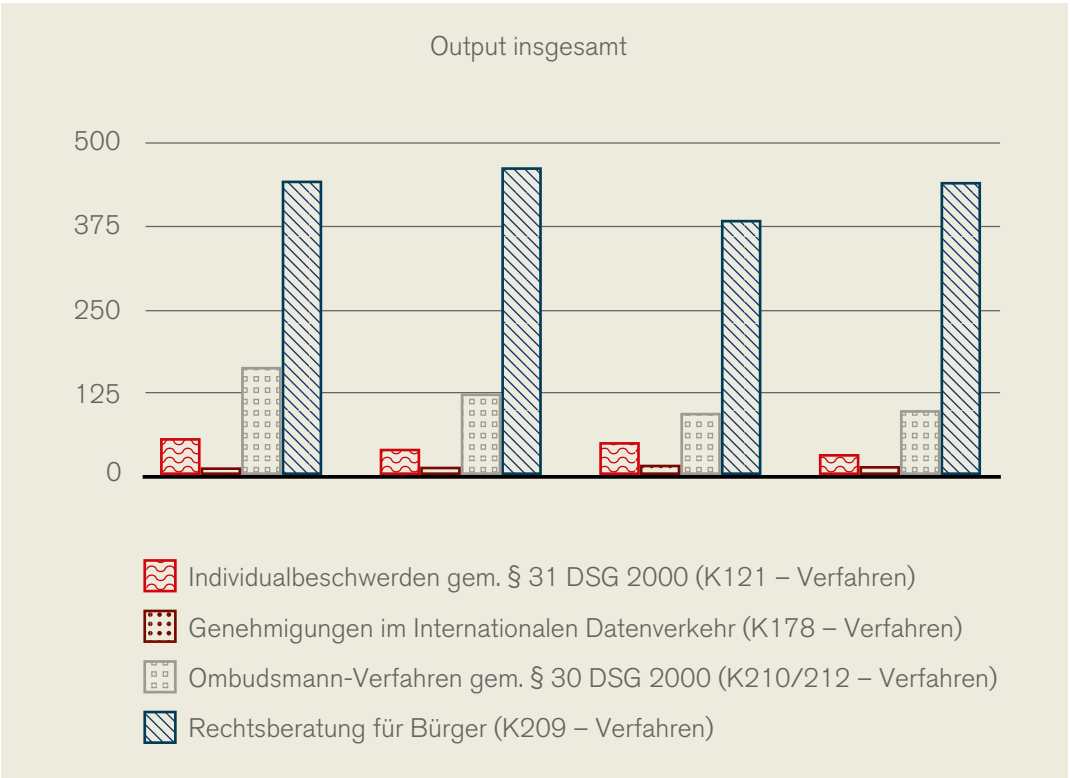
4 Geschäftsgang

4.1 Statistische Darstellung des Geschäftsganges (Gesamtübersicht)

Geschäftsfälle – Input



Geschäftsfälle – Output



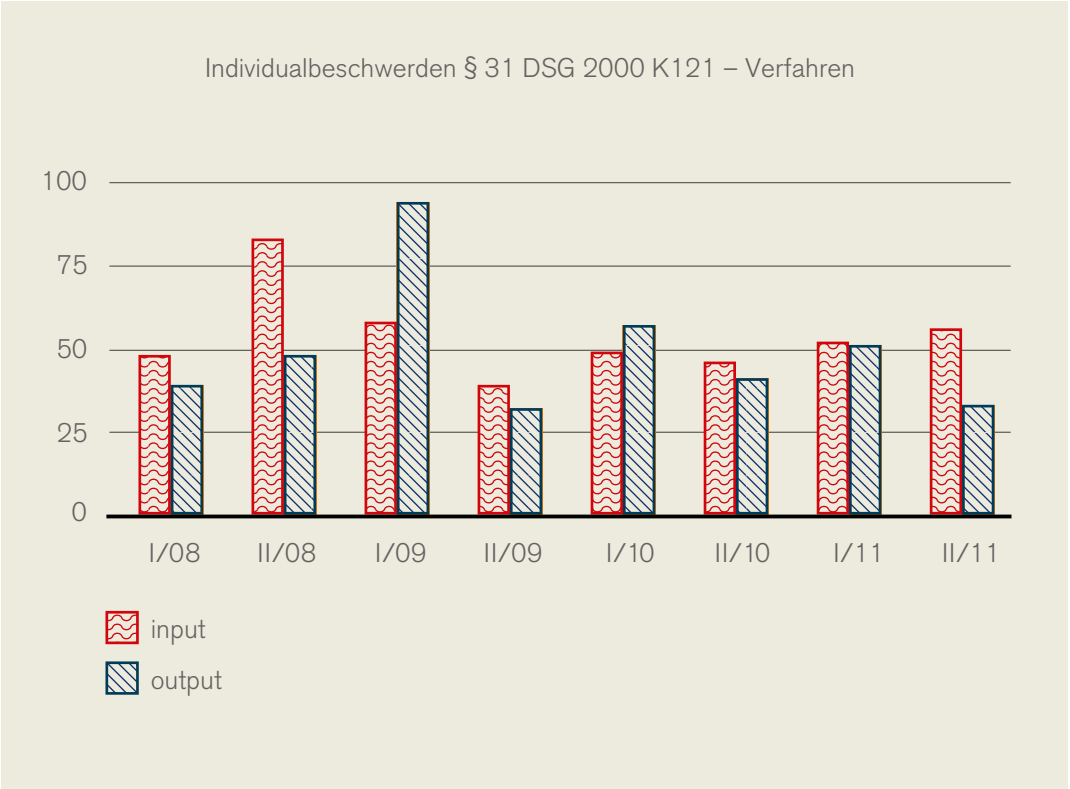
	Eingangsstücke				Erledigungen			
	1. Halb-jahr 2010	2. Halb-jahr 2010	1. Halb-jahr 2011	2. Halb-jahr 2011	1. Halb-jahr 2010	2. Halb-jahr 2010	1. Halb-jahr 2011	2. Halb-jahr 2011
Individualbeschwerden (K121-Verfahren)	49	46	52	56	57	41	51	33
Ombudsmannverfahren nach § 30 DSG 2000 (K210 + K212)	128	181	131	125	191	128	107	113
Rechtsauskünfte (K209)	444	464	385	442	444	464	385	442
Genehmigungen nach § 46 und 47 DSG 2000 (K202)	2	5	3	6	9	4	5	6
Genehmigungen im Internationalen Datenverkehr (K178)	15	20	29	26	13	14	17	15
Auskunft Schengen (K250)	7	17	9	16	7	17	9	16

Erledigungen	**1. Halbjahr 2010**	**2. Halbjahr 2010**	**1. Halbjahr 2011**	**2. Halbjahr 2011**
Entscheidungen der Kommission im Registrierungs-verfahren (K503 und K600)	7	75	115	40

4.2 Die Verfahren vor der DSK

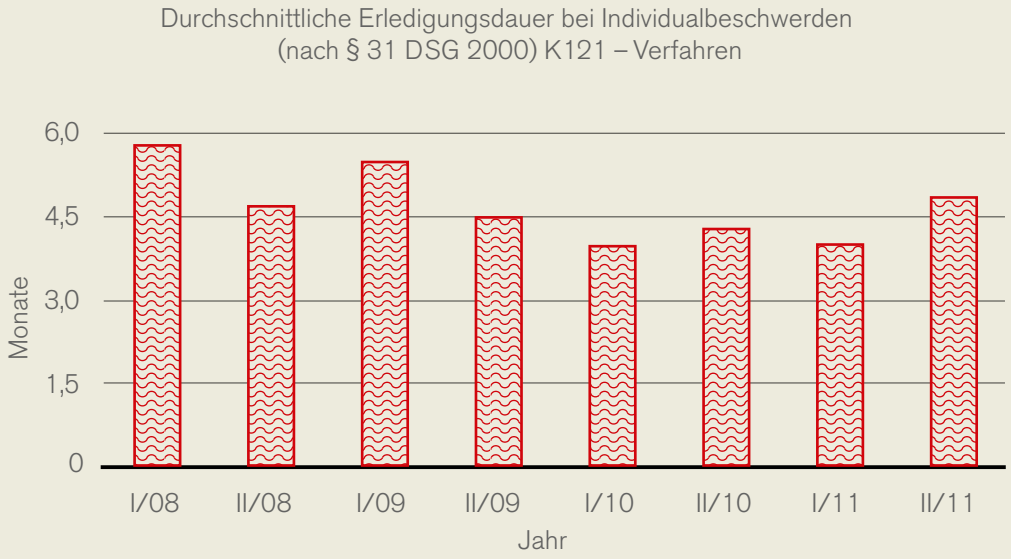
4.2.1 Individualbeschwerdeverfahren (§ 31 DSG 2000)

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

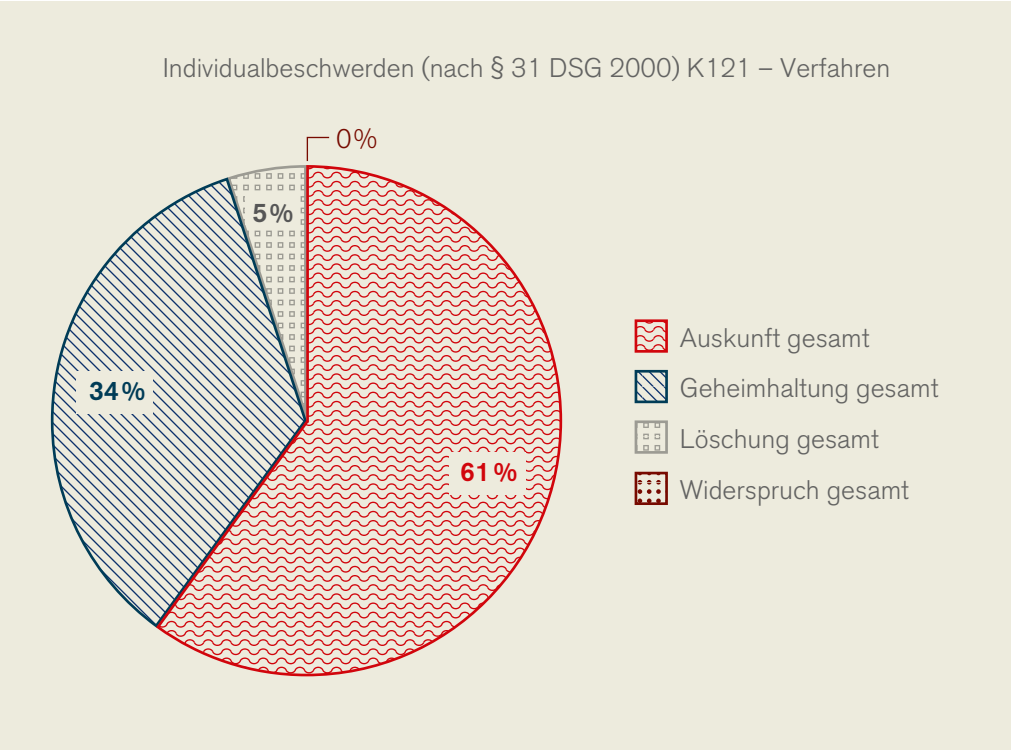


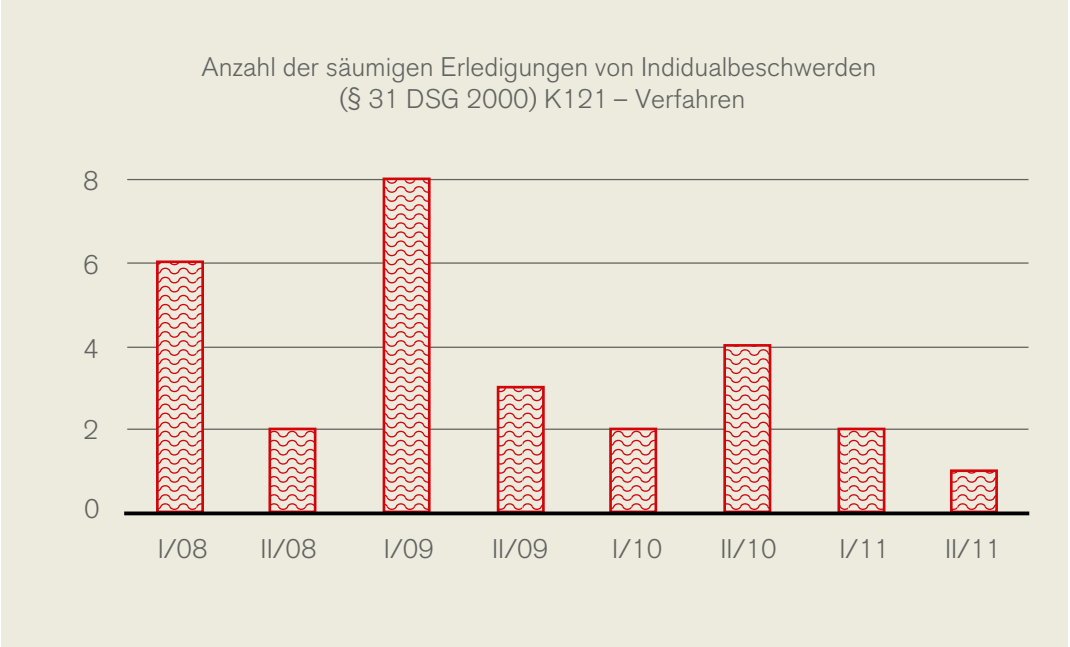
Graphische Übersicht des Arbeitsanfalls:

Graphische Übersicht der durchschnittlichen Erledigungsdauer:

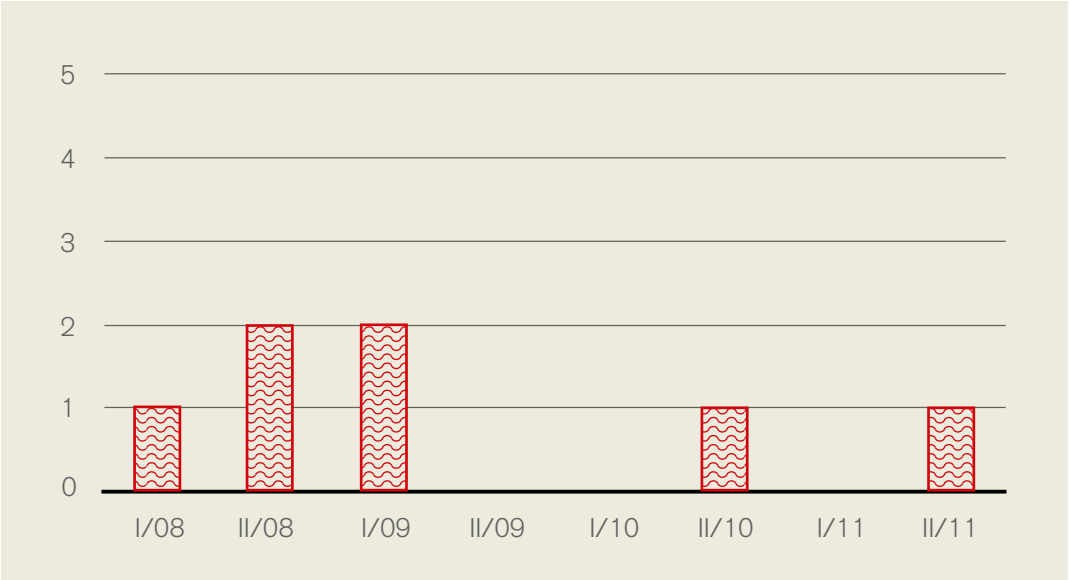


Individualbeschwerden (Berichtszeitraum):



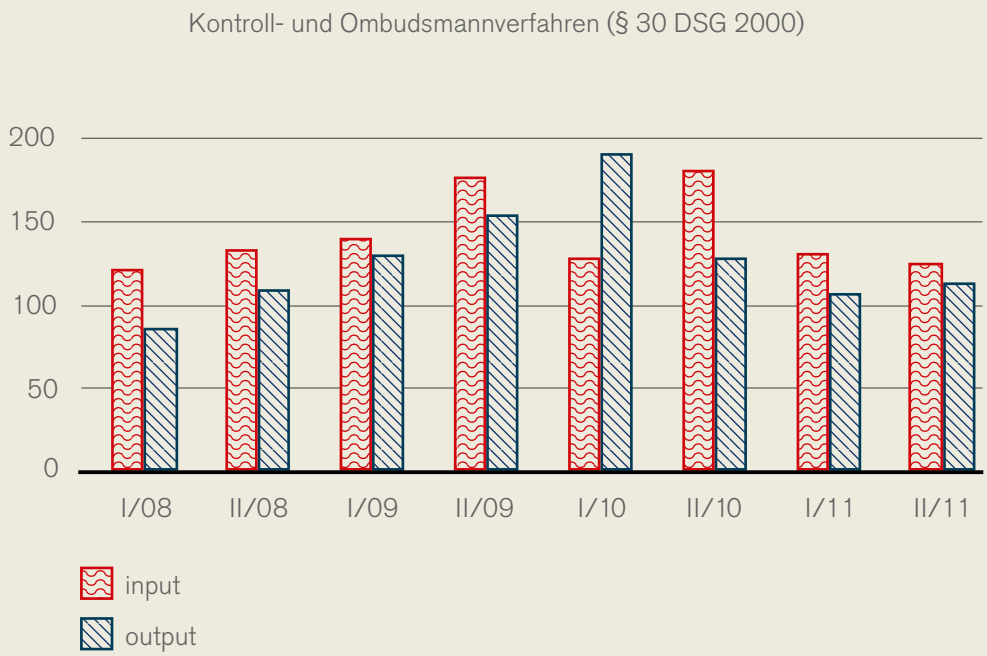


Erledigungen von Individualbeschwerden außerhalb der sechsmonatigen Frist des § 73 AVG:



Säumnisbeschwerden an den Verwaltungsgerichtshof:

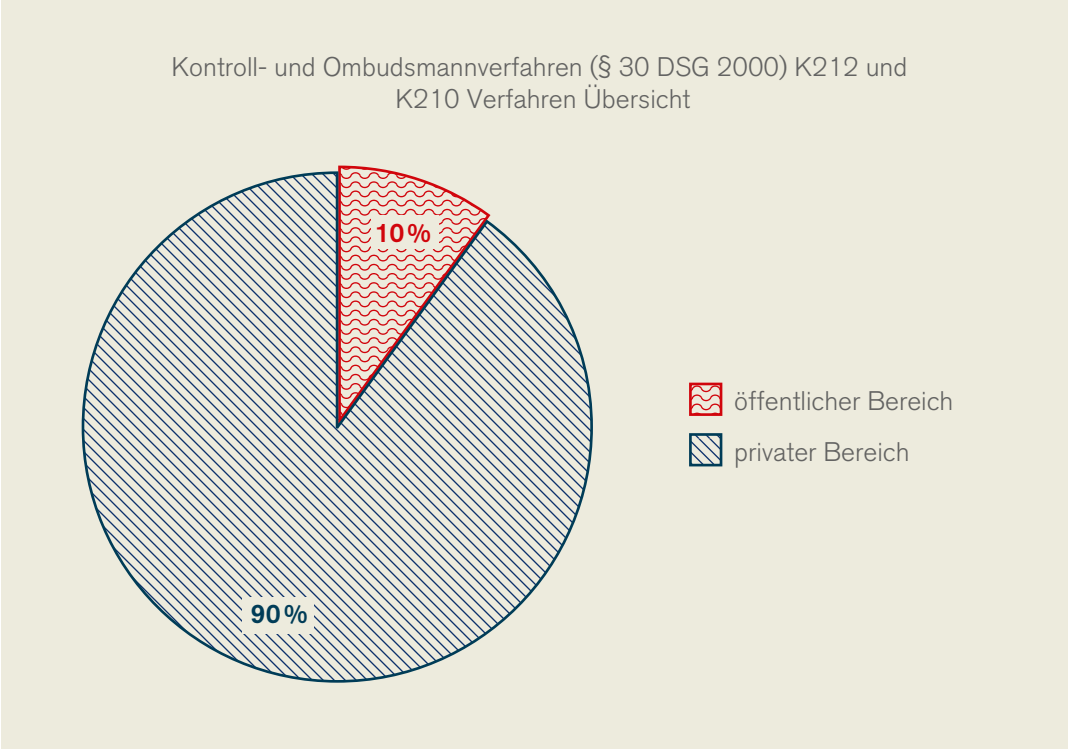
4.2.2 Ombudsmannverfahren (§ 30 DSG 2000)



Hier war der Arbeitsanfalls im Berichtszeitraum gegenüber den Vorjahren gleichbleibend hoch:

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

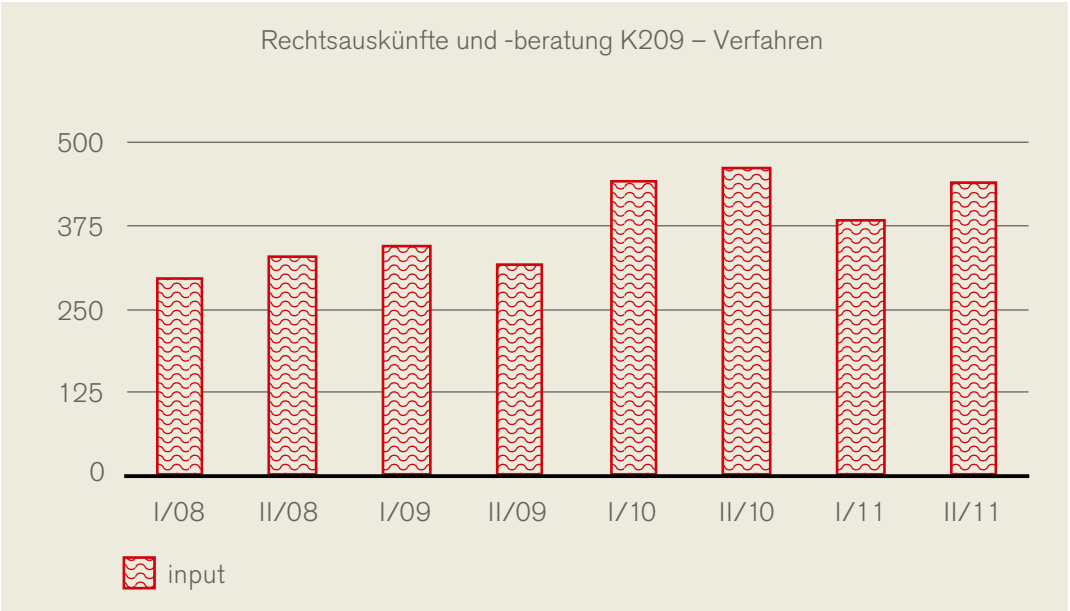
Etwa 90 % der Eingaben im Ombudsmannverfahren betreffen den privaten Bereich, etwa 15 % sind daneben amtswegig durchgeführte Verfahren (siehe auch 4.2.6.), entweder aufgrund einer Eingabe einer nicht betroffenen Person oder aufgrund eigener Wahrnehmung der DSK.



4.2.3 Rechtsauskünfte an Bürger (K209-Verfahren)

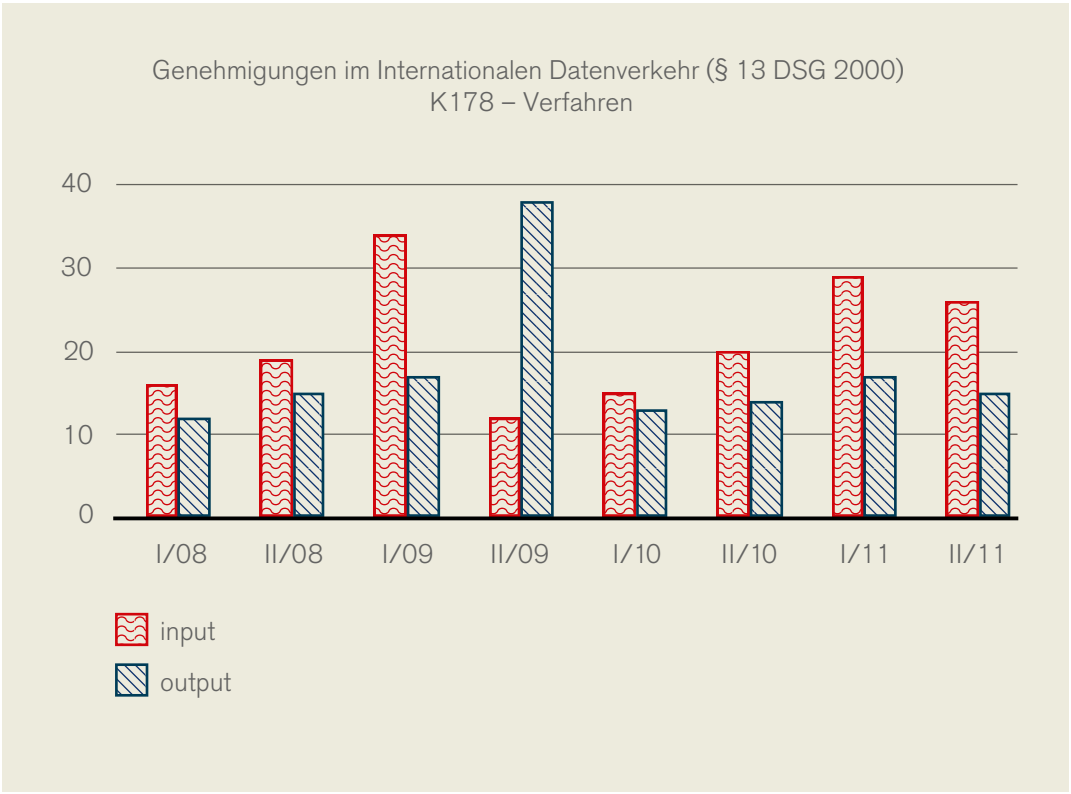
Wie wichtig diese vom Büro der DSK wahrgenommene Funktion geworden ist, ergibt sich anschaulich aus der untenstehenden Graphik. In dieser Statistik sind die zahlreichen telefonischen Auskünfte nicht enthalten, über deren Häufigkeit keine Aufzeichnungen geführt werden.

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



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

Graphische Darstellung von Input und Output im Bereich »Internationaler Datenverkehr«:



Die bereits im vorigen Berichtszeitraum erreichte Beschleunigung der Verfahren durch Beseitigung von Unklarheiten in diesem Bereich zeigte sich teilweise auch in den Jahren 2010 und 2011. Dass Genehmigungsverfahren nach wie vor gelegentlich mehr als sechs Monate in Anspruch nehmen, ist darauf zurückzuführen, dass das Genehmigungsverfahren eine registrierungsfähige Meldung jener Datenanwendung voraussetzt, aus der die Daten übermittelt bzw. überlassen werden sollen.

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

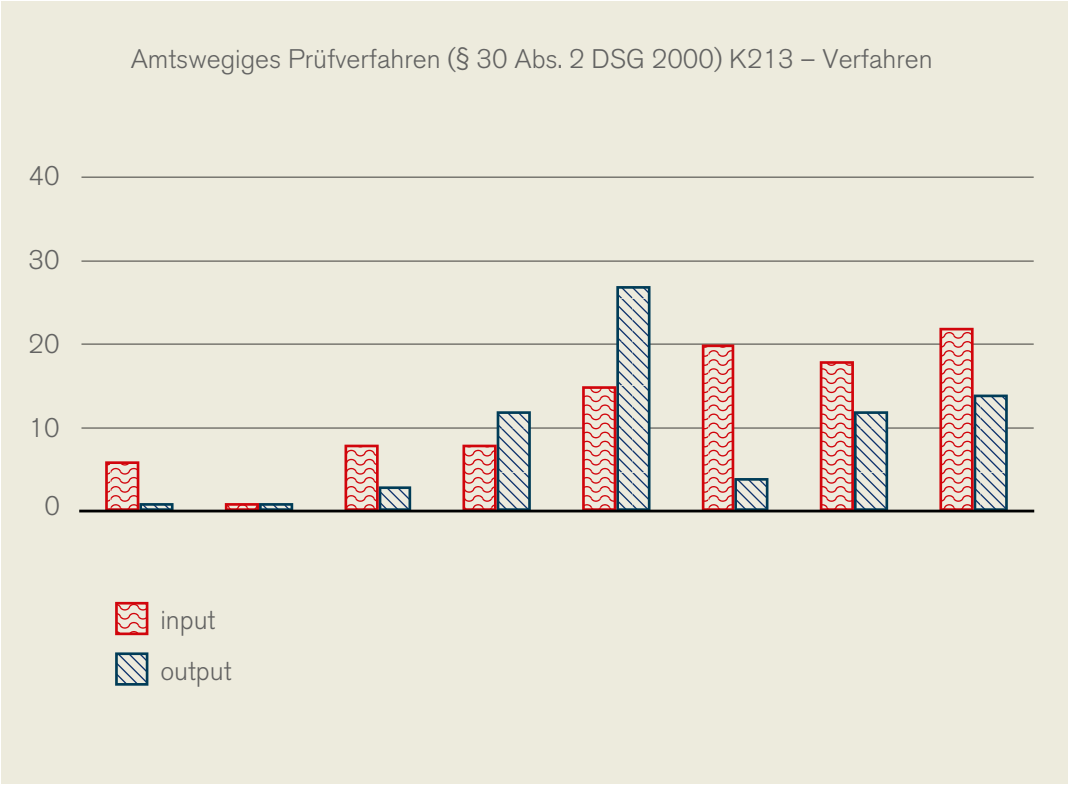
Die Registrierung der Meldung einer Datenanwendung erfolgt nicht mit Bescheid, sondern mit bloßer Mitteilung, die nicht der Rechtskraft fähig ist (der meldende Auftraggeber erwirbt durch die Registrierung keinen Rechtsanspruch darauf, die Datenanwendung in der gemeldeten Form durchführen zu dürfen).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

Im Berichtszeitraum hat sich die Notwendigkeit, Bescheide im Registrierungsverfahren zu erlassen, zum einen im Zusammenhang mit der Meldung von Videoüberwachungen ergeben, zum anderen bei der Einrichtung von Informationsverbundsystemen in einzelnen Branchen (vgl. hiezu auch die Ausführungen in Abschnitt 8).

4.2.6 Amtswegige Prüfverfahren

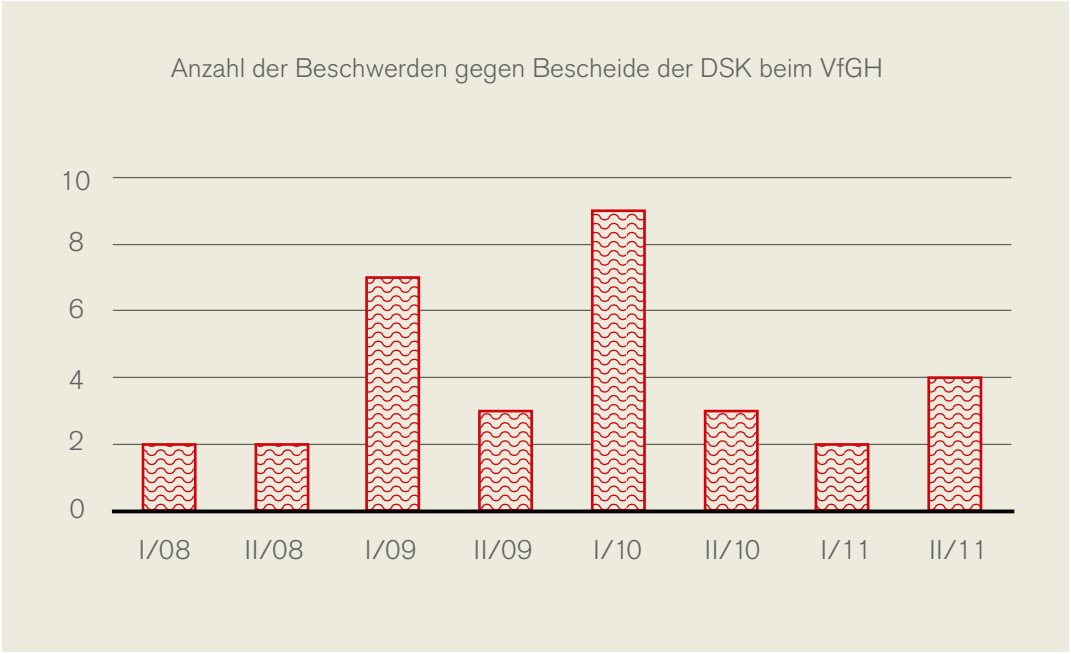
Diese haben sich im Berichtszeitraum hauptsächlich auf den Sektor Kreditinformation und Kreditauskunfteien konzentriert. Überdies wurden einige amtswegige Prüfverfahren im Zusammenhang mit den Hacking-Attacken von Anonymous Österreich eingeleitet, da in einigen Fällen der Verdacht der Verletzung von Datensicherheitsmaßnahmen gegeben war.

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

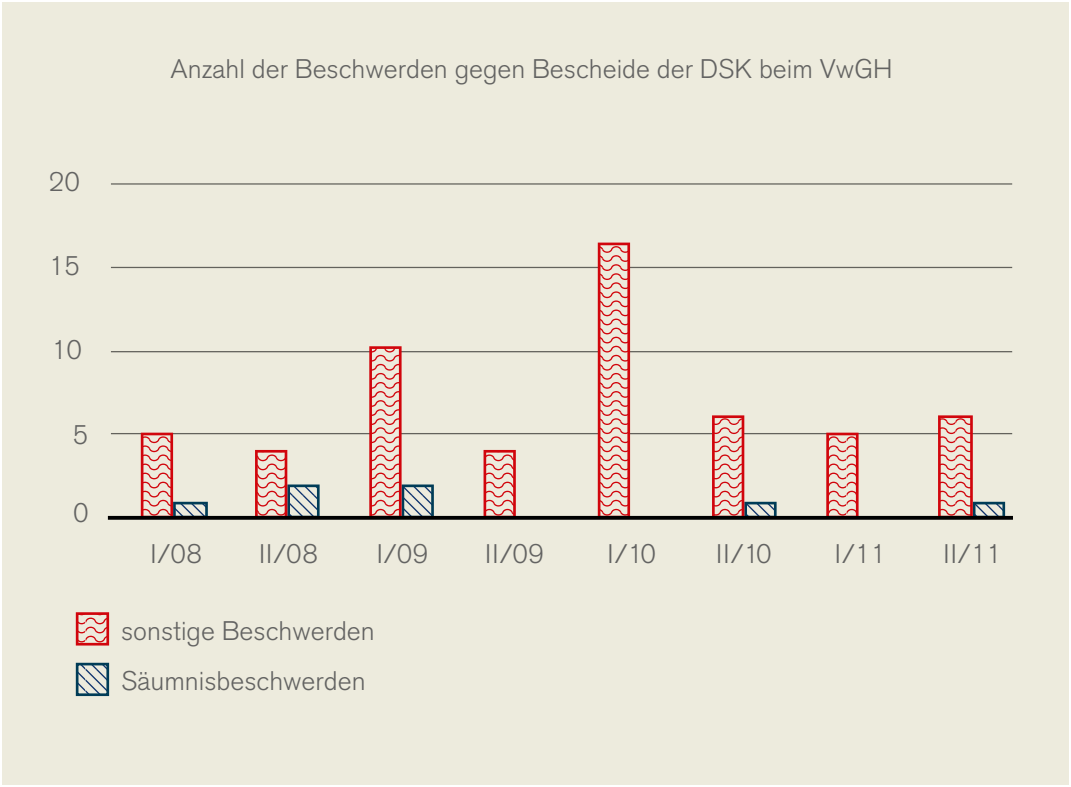


4.2.7 Äußerungen in Beschwerdeverfahren vor dem Verfassungs- und Verwaltungsgerichtshof

Graphische Darstellung der Verfahren vor dem VfGH:



Graphische Darstellung der Verfahren vor dem VwGH:



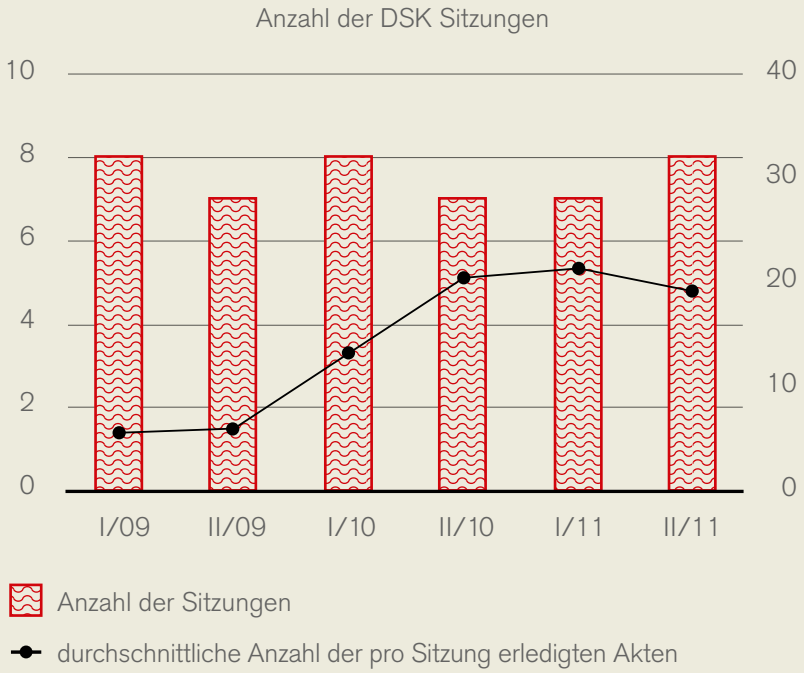
Von den 6 im Berichtszeitraum gegen Bescheide der DSK erhobenen VfGH-Beschwerden sind sämtliche noch nicht entschieden. Von den 8 früher gegen DSK-Bescheide erhobenen VfGH-Beschwerden wurden 7 abgelehnt und eine abgewiesen. Keiner Beschwerde wurde daher stattgegeben.

Im Berichtszeitraum wurde gegen 13 Bescheide der DSK Verwaltungsgerichtshofsbeschwerde erhoben, davon erfolgte in einem Fall eine Abweisung; in den restlichen 12 Fällen steht die Entscheidung noch aus. Im Berichtszeitraum wurden auch 18 Fälle entschieden, die bereits früher eingegangen waren: davon endeten 4 Fälle mit Zurückweisung, 6 Fälle mit Einstellung und 8 Fälle mit Abweisung. Auch hier wurde keiner Beschwerde daher stattgegeben.

Weiters wurde im Berichtszeitraum vor dem Verwaltungsgerichtshof in 2 Fällen Säumnisbeschwerde erhoben. In einem Fall davon wurde vom VwGH die Beschwerde zurückgewiesen.

4.3 Sitzungen der Datenschutzkommission

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



Graphische Darstellung der Sitzungshäufigkeit und Effizienz:

5 Kritische Anmerkungen zur Personal- und Organisationssituation der Datenschutzkommission

5.1 Zu den Aufgaben der Datenschutzkommission und ihrer Personalausstattung

5.1.1 Grundsätzliches zur Personalausstattung

An dem Umstand, dass die Datenschutzkommission – gemessen an der Einwohnerzahl – viel weniger Personal besitzt als die meisten anderen Datenschutz-Kontrollstellen der Mitgliedstaaten der Europäischen Union, hat sich nichts geändert. War im letzten Datenschutzbericht noch davon die Rede, dass die österreichische Behörde rund halb so viel Mitarbeiter hat als vergleichbare Behörden, sind einige dieser anderen Behörden inzwischen personalmäßig noch aufgestockt worden, so dass die österreichische Behörde im Vergleich dazu noch mehr abfällt.

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. Aus Sicht der Datenschutzkommission wäre es daher notwendig, eine Lösung für die erheblichen Altlasten des DVR vorzusehen und darüber hinaus die Vorabkontrollpflicht von Datenanwendungen zu reduzieren.

Wie bereits in Kapitel 3 angesprochen, wird sich die Umsetzung von DVR-Online noch verzögern, da die für die Anwendbarkeit der einschlägigen Bestimmungen in der DSG-Novelle 2010 die Erlassung einer neuen DVR-Verordnung Voraussetzung ist und diese nunmehr erst bis 1. September 2012 erlassen werden muss.

5.1.2 Kontinuierliche Aufgabenerweiterung

Die Datenschutzkommission weist weiters darauf hin, dass durch die Erlassung neuer Gesetze, die intensiv in das Grundrecht auf Datenschutz eingreifen, höhere Beschwerdezahlen zu erwarten sind. Dies gilt für jene Gesetze, die im Zusammenhang mit der Umsetzung der Vorratsdatenspeicherung beschlossen wurden (TKG-Novelle sowie die die Abfrage regelnde StPO- und SPG-Novelle), aber auch für das Transparenzdatenbankgesetz und die SPG-Novelle 2011, mit der unter anderem die erweiterte Gefahrenerforschung auf Einzelpersonen ausgedehnt wurde. Weiters wurden durch die Umsetzung des so genannten »EU-Telekom-Pakets« in Form der »TKG-Novelle 2011« der Datenschutzkommission neue Befugnisse und Verpflichtungen (Entgegennahme von »Data breach notifications« und Erteilung von Anordnungen in diesem Zusammenhang, Kooperation mit der Regulierungsbehörde) eingeräumt bzw auferlegt.

Sollte in absehbarer Zeit ein »ELGA«-Gesetz (betreffend die Einrichtung einer »Elektronischen Gesundheitsakte« beschlossen werden, wird mit weiteren Beschwerden an die Datenschutzkommission (zumindest im Rahmen von Kontroll- und Ombudsmannverfahren) zu rechnen sein.

Weiters sind in den von der EU-Kommission am 25. Jänner 2012 vorgelegten Vorschlägen zum neuen Rechtsrahmen im Datenschutz (Grundsatz-Verordnung und Richtlinie), die die Richtlinie 95/46/EG und den Rahmenbeschluss 2008/977/JI ablösen sollen, einheitliche Pflichten und Befugnisse der Datenschutzbehörden vorgesehen, die weit über die Aufgaben der Datenschutzkommission hinausgehen.

5.1.3 Beschwerden von Bürgern und Verfahren von Amts wegen

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, grundsätzlich innerhalb von 6 Monaten durchzuführen.

Bei den Ombudsmannverfahren ist es im Berichtszeitraum allerdings keineswegs immer gelungen, eine Erledigungsdauer von weniger als 6 Monaten zu erreichen. Die Zahl dieser Verfahren nimmt bei gleichbleibender Personalkapazität stetig zu und kann daher selbst durch Überstundenleistung nicht mehr ausgeglichen werden. Zwei zusätzliche Referenten/Referentinnen wären in diesem Bereich unbedingt erforderlich. Auch viele – von Amts wegen gebotene – Kontrollverfahren lassen sich wegen des Personalmangels nicht oder nicht in angemessener Zeit erledigen.

Ergänzend sei angemerkt, dass die (sich über das ganze Bundesgebiet erstreckenden) immer wieder notwendigen Einschauen – vor allem im Bereich der Videoüberwachung – mit dem vorhandenen Personal in keiner Weise bewerkstelligt werden können. Dafür müssten noch weitere Mitarbeiter und Mitarbeiterinnen aufgenommen werden, die entsprechende Dienstreisen zu absolvieren hätten.

Weiters hat sich im Berichtszeitraum das Problem der mangelnden Datensicherheitsmaßnahmen als besonderer Gegenstand von § 30-Verfahren herauskristallisiert. Dies betrifft vor allem jene Verfahren, die infolge von Aktionen der Gruppe »Anonymous Austria« eingeleitet wurden. In diesem Zusammenhang hat es sich als besonderes Problem herausgestellt, dass die Datenschutzkommission nicht einmal über einen Mitarbeiter mit technischer Ausbildung verfügt. Nachdem sich die Beschwerden in Kontrollverfahren zunehmend neben der Videoüberwachung auf das Internet (inklusive Suchmaschinenproblematik und Soziale Netzwerke) fokussieren, ist die Arbeit ohne technisches Know-how praktisch nicht mehr zu bewältigen.

5.1.4 Zusammenarbeit auf EU-Ebene

Diesbezüglich hat sich die Situation gegenüber dem letzten Datenschutzbericht in keiner Weise geändert.

Es ist nach wie vor nur durch besondere Anstrengungen möglich, (wenn auch oft nur sehr oberflächlich) an den wichtigsten Aktivitäten der Art. 29 Gruppe und mancher ihrer Unterarbeitsgruppen sowie an den Sitzungen der Gemeinsamen Kontrollinstanzen der Dritten Säule (vgl. dazu Abschnitt 7) teilzunehmen. Die Beschickung einiger Unterarbeitsgruppen ist jedoch mangels Ressourcen gar nicht möglich.

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«), aber auch grenzüberschreitende Datenschutzprobleme wie »Google Street View«. Überdies leistete die Datenschutzgruppe als Beratungsorgan der Europäischen Kommission kontinuierlich Beiträge im Zusammenhang mit der Erarbeitung der neuen Rechtsinstrumente im Datenschutz und wird auch in der weiteren Diskussion ihre Expertise zur Verfügung stellen. Daran zeigt sich, wie wichtig es auch für kleine Datenschutzbehörden wäre, sich entsprechend einbringen zu können.

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 strategisch ausgerichtete Einflussnahme auf die Arbeit auf europäischer Ebene ist unter diesen Voraussetzungen jedoch nicht zu denken.

5.1.5 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 in den letzen Berichten 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.

Es scheint daher dringend geboten, die Datenschutzkommission durch Zurverfügungstellung der nötigen Ressourcen in die Lage zu versetzen, ihre Prüfkompetenz in umfangreicherem Maße wahrzunehmen (siehe oben Kap. 5.1.3.).

5.1.6 Öffentlichkeitsarbeit

a) Information der Öffentlichkeit in Datenschutzfragen

Die Datenschutzkommission und ihre Geschäftsstelle sind trotz dauernden Zeitmangels 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, bei 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

Im Berichtszeitraum sind für den Datenschutz wesentliche Gesetzes- und Verordnungsentwürfe regelmäßig auch der Datenschutzkommission zur Stellungnahme im Begutachtungsverfahren zugeleitet worden.

Die Datenschutzkommission macht von der Möglichkeit zur Stellungnahme bei besonders wichtigen Entwürfen (ausnahmsweise auch im EU-Bereich im Hinblick auf öffentliche Konsultationen) regelmäßig Gebrauch, und zwar auch dann, wenn sie zur Teilnahme im Begutachtungsverfahren nicht ausdrücklich aufgefordert worden sein sollte. Besonders erwähnenswert sind die Stellungnahmen der Datenschutzkommission zum Gesamtkonzept der Europäischen Kommission im Datenschutz und die Stellungnahmen zum Transparenzdatenbankgesetz, zum Gesundheitstelematikgesetz (insbesondere punkto ELGA) und zur SPG-Novelle 2011 (Anti-Terrorismuspaket).

5.1.7 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 der Geschäftsstelle der DSK

Wie im letzten Datenschutzbericht erwähnt, ist die Geschäftsstelle der Datenschutzkommission seit 2009 zur Gänze am Standort Hohenstaufengasse untergebracht.

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

5.3 Zur organisatorischen Stellung der Datenschutzkommission und ihrer Geschäftsstelle

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. Formell ist bisher von dieser Bestimmung noch nicht Gebrauch gemacht worden. Es besteht aber eine informelle Zusammenarbeit mit dem Datenschutzrat., indem das geschäftsführende Mitglied an Sitzungen und Diskussionen des Datenschutzrates teilnimmt.

5.3.2 Die Geschäftsstelle

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 Bundeskanzleramt als Geschäftsstelle zur Verfügung gestellt hat. Der Bundeskanzler ist Dienstvorgesetzter der Bediensteten dieser Geschäftsstelle (vgl. § 37 Abs. 2 DSG 2000).

5.3.3 Ausblick

Das zwischenzeitig (im Jahre 2010) 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 z. B. 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.

Inzwischen hat die Europäische Kommission im Verfahren C-614/10 Klage beim EuGH gegen die Republik Österreich wegen mangelnder Unabhängigkeit der Datenschutzkommission eingebracht. Eine mündliche Verhandlung hat im April 2012 stattgefunden. Das Urteil ist allenfalls auch im Laufe des Jahres 2012 zu erwarten.

5.4 Zur Regierungsvorlage einer Verwaltungsgerichtsbarkeits-Novelle 2012

Im Berichtszeitraum wurde von der Bundesregierung die Regierungsvorlage einer Verwaltungsgerichtsbarkeits-Novelle 2012 beschlossen. Diese sieht nach wie vor die Auflösung zahlreicher Behörden, so auch der Datenschutzkommission, vor.

Zu dem unter Zl BKA-601.999/0001-V/1/2010 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 aufkommensneu-

trale – 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 Entscheidungen in erster Instanz und für die dafür notwendigen Sachverhaltsermittlungen gedacht, sodass übertragene Datenschutzkommissions-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.

Überdies 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.«

In diesem Zusammenhang ist darauf hinzuweisen, dass in dem von der EU-Kommission am 25. Jänner 2012 vorgelegten Vorschlag für eine Datenschutz-Grundsatz-Verordnung der Aufsichtsbehörde effektive Eingriffsbefugnisse wie die Anordnung der Löschung oder Berichtigung einer Datenanwendung eingeräumt werden, so dass es wohl kaum Sinn machen würde, derartige Befugnisse der Datenschutzkommission zu entziehen. Wenn die Kompetenzen der Kontrollstelle aber im Grunde nicht reduziert werden sollen und im Gegenteil in Zukunft eine Ausweitung der Befugnisse zu erwarten ist, stellt sich wiederum die Frage nach der Sinnhaftigkeit einer Auflösung der Datenschutzkommission. Ein Bundesverwaltungsgericht könnte sinnvoller Weise nur als zweite Instanz agieren (was im Übrigen mit zusätzlichen Kosten verbunden ist). Die geplante Auflösung der Datenschutzkommission sollte seitens der Gesetzgebung im Lichte der oben stehenden Ausführungen daher nochmals überdacht werden.

6 Zum Inhalt der im Berichtszeitraum durchgeführten Verfahren[9]

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

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

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

6.1.1 Recht auf Auskunft

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

Mit der DSG-Novelle 2010 wurde die DSK in die Lage versetzt, ein Verfahren wegen behaupteter Verletzung auf Auskunft formlos einzustellen, wenn die Rechtsverletzung beseitigt scheint und der Beschwerdeführer nicht binnen angemessener Frist begründet, warum die Rechtsverletzung zumindest teilweise als noch nicht beseitigt erachtet wird (§ 31 Abs. 8 DSG 2000). Wesensänderungen in der Sache durch die Äußerung bedeuten nun gesetzlich explizit eine konkludente Zurückziehung der ursprünglichen Beschwerde (die die formlose Einstellung des Beschwerdeverfahrens nach sich zieht) und gleichzeitiger Einbringung einer neuen Beschwerde (ebenda).

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

a. Schaffung von automationsunterstützter Durchsuchbarkeit für Auskunftserteilung (K121.220/0005-DSK/2010, 19. 2. 2010)

Sachverhalt

Die Beschwerdeführerin behauptete eine Verletzung im Recht auf Auskunft durch den Beschwerdegegner durch Ablehnung der Auskunft, zunächst begründet mit mangelnder Betroffenenstellung, schließlich mangels verarbeiteter Daten (Negativauskunft). Die Sache befindet sich nunmehr im zweiten Rechtsgang, nachdem die teilstattgebende Entscheidung der DSK vom 2. Februar 2007 vom VwGH aufgehoben wurde.

Auf das Auskunftsbegehren der Beschwerdeführerin im Februar 2006 reagierte der Beschwerdegegner, eine Kreditauskunftei, mit Schreiben im selben Monat, mit der Begründung ablehnend, die Beschwerdeführerin sei nicht Betroffene. Diese Ansicht ergänzte er im Schreiben aus März 2006 durch folgende Ausführungen: *»Da wir Ihre Daten nicht verwenden, kommt Ihnen keine Parteienstellung zu.«*

Im anschließenden Beschwerdeverfahren vor der DSK legte die Beschwerdeführerin dar, dass sie von dritter Seite erfahren habe, dass sie als »betreibender Gläubiger« in der Datenbank des Beschwerdegegners aufscheine. Der Beschwerdegegner änderte seine Verantwortung daraufhin dahin gehend, dass er keine Daten über die Beschwerdeführerin in jenen Datenfeldern seiner Datenbank finden könne, die direkt durchsuchbar seien. Das Datenfeld »betreibender Gläubiger«, das in den die Schuldner betreffenden Datensätzen zwar vorhanden, aber nur gelegentlich ausgefüllt sei, könne nicht direkt, sondern nur indirekt im Umweg über den Namen des Schuldners angesprochen werden. Es sei nicht ausgeschlossen, dass die Beschwerdeführerin im Feld »betreibender Gläubiger« bei einzelnen Schuldnern aufscheine, doch könne dies ohne Kenntnis des Namens der infrage kommenden Schuldner nicht festgestellt werden, ohne die gesamte Datenbank zu durchforsten, die einige Mio Datensätze enthalte. Die Beschwerdeführerin werde daher zur Mitwirkung in Form der Bekanntgabe der Namen der infrage kommenden Schuldner aufgefordert. Dieser Aufforderung ist die Beschwerdeführerin zu keinem Zeitpunkt des Verfahrens nachgekommen.

Eine Abfrage der Datenbank nach dem Namen der Beschwerdeführerin (in verschiedenen Schreibweisen) unter Zuhilfenahme

9 Sämtliche hier genannten Entscheidungen sind abrufbar im Rechtsinformationssystem des Bundes (RIS) unter www.ris.bka.gv.at/dsk

der für die Abfrage im Internet zur Verfügung stehenden automationsunterstützten Suchroutinen lieferte tatsächlich keinen Treffer.

Mit Schreiben aus Juli 2009 erteilte der Beschwerdegegner eine abschließend formulierte Antwort auf das Auskunftsbegehren der Beschwerdeführerin, in dem er die Erteilung einer inhaltlichen Auskunft mit der Begründung verweigert, dass ihr überwiegende berechtigte Interessen als Auftraggeber infolge unzumutbaren Aufwands entgegenstünden. Die Beschwerdeführerin hat sich zu den Ausführungen über den notwendigen händischen Durchsuchungsaufwand nicht geäußert, sondern nur festgehalten, dass eine Behauptung der überwiegenden berechtigten Interessen des Beschwerdegegners bzw die Unmöglichkeit der ‚seriellen' Durchsuchung der Datenbank nach ihr als Gläubiger aufgrund der Anzahl der Datensätze zum Ergebnis führen würde, dass ihr Auskunftsrecht gem § 26 DSG 2000 komplett ausgeschaltet wäre.

Rechtliche Würdigung

Im vorliegenden Beschwerdefall hat der Beschwerdegegner zuletzt im Juli 2009 eine Rechtshandlung gesetzt, die als Beantwortung eines Auskunftsbegehrens im Sinne des § 26 Abs. 4 DSG 2000 innerhalb eines laufenden Verfahrens vor der DSK zu deuten ist (§ 31 Abs. 8 DSG 2000).

Der VwGH hat in seinem aufhebenden Erkenntnis präzise ausgeführt, dass der Auftrag an den Beschwerdegegner zu lauten hat, »*Auskunft im Umfang des § 26 Abs. 1 DSG 2000 zu geben oder bekannt zu geben, dass keine der Auskunftspflicht unterliegenden Daten über die Beschwerdeführerin verarbeitet werden*«. Die DSK hatte daher zu prüfen, ob die vom Beschwerdegegner der Beschwerdeführerin im Juli 2009 erteilte Antwort auf ihr Auskunftsbegehren diesen Anforderungen entspricht. Diese Antwort verweigert die Auskunftserteilung mit der Begründung, dass überwiegende berechtigte Interessen des Auftraggebers einer Pflicht zur inhaltlichen Auskunftserteilung über die gesamte Datenbank – also auch über diejenigen Teile, die der Auftraggeber mit seinen Mitteln nicht automationsunterstützt direkt ansprechen kann – entgegenstünden. Der Beschwerdegegner bestreitet somit das Bestehen einer Auskunftspflicht bzw »*gibt bekannt, dass (im konkreten Fall) keine einer Auskunftspflicht (nach Abs. 1) unterliegenden Daten vorhanden sind*«. Die Begründung, dass eine »*händische*« Durchsuchung eines Datenbestandes von 2,2 Mio Datensätzen einen großen Zeitaufwand verursachen würde, erschien der DSK glaubwürdig.

Dem Argument der Beschwerdeführerin, die Relevanz der Aufwandsfrage würde zum Ergebnis führen, dass ihr Auskunftsrecht »*komplett ausgeschaltet würde*«, folgte die DSK mit folgender Begründung nicht: Es wurde festgestellt und der Beschwerdeführerin auch mehrfach mitgeteilt, dass mit den vorhandenen automationsunterstützten Suchmitteln in der Datenbank keine Daten über sie auffindbar sind. Offen ist, ob in jenen Teilen der Datenbank, die nicht direkt anhand des Namens der Beschwerdeführerin durchsuchbar sind, Daten über sie vorhanden sind. Zur Auffindung solcher Daten gäbe es folgende Möglichkeiten:

a. die Beschwerdeführerin gibt die Namen ihrer Schuldner bekannt,
b. die Datenbank wird händisch durchgesehen oder
c. es wird zusätzliche Software erzeugt oder beschafft, um den automationsunterstützten Zugriff auch auf die derzeit nicht im Direktzugriff stehenden Teile der Datenbank nach dem Namen der Beschwerdeführerin durchsuchbar zu machen.

Ad a) Der Aufforderung zur Mitwirkung gem § 26 Abs. 3 DSG 2000 in Form der Bekanntgabe von Schuldnernamen kam die Beschwerdeführerin – offenbar aus nicht näher substantiierten Datenschutzbedenken – nicht nach.

Ad b) Was die händische Durchsuchung betrifft, teilte die DSK die Auffassung, dass der hiefür notwendige Aufwand unverhältnismäßig wäre.

Ad c) Was die Verwendung zusätzlicher Durchsuchungssoftware betrifft, wäre der hiefür notwendige Aufwand vermutlich nicht übermäßig groß, doch stellte sich die ganz grundsätzliche Frage, ob ein Auftraggeber rechtlich verhalten ist, über die bei ihm zur Abfrage in einer Datenanwendung verwendete Software hinaus für Zwecke einer Auskunftserteilung zusätzliche Software zum Einsatz zu bringen: Dagegen sprechen erhebliche Bedenken, da damit das zunächst nicht vorhandene besondere datenschutzrechtliche Missbrauchsrisiko einer (direkten) Auffindbarkeit erst erzeugt wird und damit die Erfüllung der Auskunftsverpflichtung letztlich zum datenschutzrechtlichen Nachteil des Auskunftswerbers mutiert. Diese Fragestellung gewinnt noch dadurch an datenschutzrechtlicher Brisanz, dass infolge der Beschaffung besonderer Software zur Auffindung bisher nicht auffindbarer Daten auch die datenschutzrechtliche Stellung vieler anderer Betroffener negativ beeinflusst wird, da die eigens beschaffte Software nunmehr in der Datenbank generell eingesetzt werden kann.

In diesem Zusammenhang wurde auch bedacht, dass »Datenschutz« grundsätzlich zur Abwehr jener besonderen Gefahren entwickelt wurde, die sich aus der automationsunterstützten Verarbeitung von personenbezogenen Daten ergeben. Zu diesem Gefahrenpotential gehört auch die Direktsuche. Diese besonderen Gefahren bestehen nicht, wenn gespeicherte Datenmengen »händisch« (sequentiell) durchsucht werden müssen, um Daten über eine bestimmte Person zu finden. Das Recht auf Auskunft dient dem Schutz des Betroffenen gegen die besonderen Gefahren des Einsatzes von automationsunterstützter Datenverarbeitung. Die DSK ist der Auffassung, dass die Verpflichtung zur Auskunftserteilung nicht so ausgelegt werden darf, dass sie Anlass für die Herbeiführung einer datenschutzrechtlichen Gefährdung wird, die sonst nicht gegeben wäre. Daten eigens automationsunterstützt auffindbar zu machen, die sonst ohne diese, eine Suche erleichternde Methode nicht auffindbar wären, widerspricht dem Sinn von Datenschutz. Dies gilt insbesondere auch hinsichtlich jener Betroffenen, deren Daten durch allfällige für die Auskunftserteilung eigens erzeugter neuer Suchmöglichkeiten nunmehr ebenfalls erleichtert auffindbar werden, obwohl sie dies ihrerseits nie angestrebt haben. Der Auftraggeber einer Datenanwendung ist daher nach Ansicht der DSK nicht verhalten, zur Beantwortung eines Auskunftsbegehrens Suchsoftware einzusetzen, die ihm bei der von ihm sonst vorgenommenen Verwendung der Datenbank nicht zur Verfügung steht.

Die vom Beschwerdegegner erstattete Beantwortung des Auskunftsbegehrens war somit vollständig, da er dargelegt hat, warum nach seiner Auffassung eine Pflicht zur Auskunftserteilung im vorliegenden Fall nicht besteht und dies nachvollziehbar damit begründet hat, dass eine vollständige automationsunterstützte Durchsuchung in seiner Datenbank technisch nicht möglich sei und eine händische Durchsuchung des Datenbestandes angesichts des hiefür notwendigen Aufwands nicht zumutbar sei. Die Beschwerde wurde daher abgewiesen.

Dieser Bescheid wurde beim Verwaltungsgerichtshof angefochten. Das Verfahren ist anhängig.

b. Auskunft aus Akten eines parlamentarischen Untersuchungsausschusses (K121.615/0006-DSK/2010, 12. 5. 2010)

Sachverhalt

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Auskunft dadurch, dass seinem Auskunftsbegehren, gerichtet an eine Person in ihrer Funktion als Abgeordnete zum österreichischen Nationalrat und Mitglied eines Untersuchungsausschusses im Parlament, das zahlreiche Fragen zu diesem Ausschuss enthielt, bisher nicht nachgekommen worden sei. Die DSK möge daher prüfen, ob das im DSG 2000 verankerte Auskunftsrecht vom Datenverarbeiter erfüllt wird.

Rechtliche Würdigung

Der Beschwerdeführer sieht sich in seinem Recht auf Auskunft gem § 1 Abs. 3 Z 1 DSG 2000 iVm § 26 DSG 2000 durch das »Parlament Republik Österreich« dadurch

verletzt, dass auf sein Auskunftsbegehren nicht reagiert wurde. § 1 Abs. 5 DSG 2000 bestimmt, dass gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechts auf Auskunft auf dem Zivilrechtsweg geltend zu machen ist. In allen übrigen Fällen ist die DSK zur Entscheidung zuständig, es sei denn, dass Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind. Gemäß § 31 Abs. 1 DSG 2000 erkennt die DSK (u. a.) über Beschwerden von Personen, die behaupten, in ihrem Recht auf Auskunft nach § 26 DSG 2000 verletzt zu sein, soweit sich das Auskunftsverlangen nicht auf die Verwendung von Daten für Akte im Dienste der Gesetzgebung oder der Gerichtsbarkeit bezieht.

Sollten daher von einem Auskunftsbegehren Akte der Gesetzgebung betroffen sein, ist die Überprüfung einer Auskunft der Zuständigkeit der DSK entzogen. Im Konkreten hat der Beschwerdeführer ein Auskunftsbegehren an einen Abgeordneten des Nationalrates gerichtet, das inhaltlich zahlreiche Fragen zu einem Untersuchungsausschuss bzw zur Datenverwendung im Nationalrat selbst enthielt. Bevor zu beurteilen wäre, ob sämtliche dieser Fragen überhaupt vom Recht auf Auskunft gem. § 26 DSG 2000 gedeckt sind, stellt sich für die Zuständigkeit die Frage, ob die Tätigkeit des Nationalrates bzw. die Tätigkeit eines Untersuchungsausschusses Akte der Gesetzgebung sind.

Zur Staatsfunktion »Gesetzgebung« sind alle Verhaltensweisen von gesetzgebenden Organen zu zählen (Adamovich/Funk/Holzinger, Österreichisches Staatsrecht, Band 2: Staatliche Organisation; Rz 26014). Dazu gehören Akte der parlamentarischen Versammlung (z. B. Gesetzesbeschlüsse) und von Ausschüssen, aber auch von Organen (z. B. dem Präsidenten des Nationalrates und der Parlamentsdirektion) oder von Abgeordneten bei Ausübung ihres Berufes. Zur Gesetzgebung gehören auch jene Tätigkeiten gesetzgebender Organe, die das B-VG unter dem Titel »Mitwirkung an der Vollziehung« behandelt (Art. 50 bis 55 B-VG). Dem Bereich der Staatsfunktion Gesetzgebung sind sogar die parlamentarischen Hilfsdienste zuzuordnen (Adamovich/Funk/Holzinger, aaO, Rz 26015).

Gemäß Art. 53 B-VG kann der Nationalrat durch Beschluss Untersuchungsausschüsse einsetzen. Der Untersuchungsausschuss ist ein Organ der Gesetzgebung, das weder als Gericht noch als Verwaltungsbehörde iSd B-VG qualifiziert werden kann. Die von einem solchen Ausschuss gesetzten Akte sind weder als gerichtliche noch als verwaltungsbehördliche Akte deutbar; es handelt sich bei diesen vielmehr um unmittelbaren Vollzug der Bundesverfassung und des GOG-NR. Dies folgt auch aus dem Fehlen einer entsprechenden Zurechnungsregel im B-VG. Akte eines Gesetzgebungsorgans oder eines Teilorgans des Gesetzgebungsorgans können nur dann als »Verwaltungsakte« qualifiziert werden, wenn dies eine verfassungsrechtliche Zurechnungsregel – wie etwa Art. 30 Abs. 6 B-VG – normiert (Mayer, in: Mayer/Platzgummer/Brandstetter, Untersuchungsausschüsse und Rechtsstaat, S 1 ff).

Dieser Rechtsansicht schloss sich die DSK an, womit das verfahrensgegenständliche Auskunftsbegehren auf Akte der Gesetzgebung im Sinn des § 1 Abs. 5 DSG 2000 bzw § 31 Abs. 1 DSG 2000 gerichtet ist, sodass eine Verletzung im Recht auf Auskunft ihrer Zuständigkeit entzogen und die Beschwerde somit zurückzuweisen war.

c. Auskunftsrecht bei Videoüberwachung (Rechtslage nach DSG-Novelle 2010) (K121.605/0014-DSK/2010, 30. 7. 2010)

Sachverhalt

Der Beschwerdeführer stellte am 18. Jänner 2010 mit der Behauptung, er sei am 17. Jänner 2010 von der registrierten Videoüberwachungsanlage der Beschwerdegegnerin (Personenbeförderungsunternehmen) erfasst worden, ein Auskunftsbegehren an die Beschwerdegegnerin und ersuchte insbesondere um die Bekanntgabe der Daten selbst. Seiner Mitwirkungspflicht kam er durch genaue Angaben zur Situation (Linie, Zeit,

Ort) und zu seiner Person (Kleidung, Größe, Haarfarbe etc.) nach. Zum Identitätsnachweis legte er dem Auskunftsbegehren auch eine Ausweiskopie bei. Das Begehren wurde per E-Mail an vier E-Mail-Adressen der Beschwerdegegnerin, die auf deren Website als Kontaktadressen angegeben waren, übermittelt.

Die Beschwerdegegnerin teilte dem Beschwerdeführer Allgemeines zur registrierten Videoüberwachungsanlage (Zweck, Aufbewahrungsdauer, Auswertungsfälle) mit, verweigerte aber mit Verweis auf die Rechtsprechung der DSK zur alten Rechtslage (Bescheid vom 5. Dezember 2008, GZ K121.401/0009-DSK/2008) eine Auskunft über die Daten selbst, da keine Auswertungen erfolgt seien. Überdies sei das Auskunftsbegehren erst nach Ablauf der Aufzeichnungsdauer bei der zuständigen Abteilung eingelangt.

Rechtliche Würdigung

Die noch nach der Rechtslage vor Inkrafttreten der DSG-Novelle 2010 (BGBl I Nr 133/2009) mit Bescheid der DSK für die Beschwerdegegnerin registrierte Videoüberwachung erfüllt für die DSK unzweifelhaft den Videoüberwachungsbegriff des § 50a Abs. 1 DSG 2000, sodass – neben den allgemeinen Bestimmungen des DSG 2000 – auch die Bestimmungen des Abschnittes 9a. des DSG 2000 (idF der DSG-Novelle 2010) zur Anwendung gelangen. § 50e Abs. 1 DSG 2000 bezieht sich zum Recht auf Auskunft ausdrücklich auf § 26 DSG 2000 in der Weise, dass die Form der Auskunftserteilung »abweichend von § 26 Abs. 1« geregelt wird: Auskunft ist dabei – in erster Linie – durch Zurverfügungstellung einer Kopie der Videobildaufzeichnungen über den Auskunftswerber zu erteilen. Aus dem Umstand, dass § 50e aber nur Abweichungen von § 26 DSG 2000 regelt, schließt die DSK, dass er keine völlig neue und eigenständige Art der Auskunft regeln will, sondern das bereits gemäß § 26 DSG 2000 bestehende Auskunftsrecht für aufgezeichnete Bilddaten ergänzen und anpassen will. Hieraus folgt, dass dann, wenn ein Auskunftsanspruch schon gemäß § 26 DSG 2000 bzw den sonstigen Regelungen des DSG 2000 ausgeschlossen wäre, auch kein Auskunftsrecht aus aufgezeichneten Bilddaten nach § 50e bestünde.

Die DSK hat auf Basis der Rechtslage vor Inkrafttreten der DSG-Novelle 2010 zum Auskunftsanspruch aus aufgezeichneten Bilddaten für den Fall, dass keine Auswertung aus diesen Bilddaten stattgefunden hat, wiederholt ausgeführt, dass ein Auskunftsanspruch nicht besteht, indem sie eine Analogie zur Ausnahme vom Auskunftsanspruch bei Vorliegen indirekt personenbezogener Daten (§ 29 DSG 2000) gezogen hat (vgl. für viele den Bescheid vom 5. Dezember 2008, GZ K121.385/0007-DSK/2008, siehe eine ausführliche Zusammenfassung dieser Entscheidung im Heft 01/2009).

Da nun § 50e DSG 2000 keinen weitergehenden Auskunftsanspruch als § 26 DSG 2000 normiert, sondern lediglich die Modalitäten bei der Ausübung des Auskunftsrechts aus Videoüberwachungen näher regelt, nämlich wie die Bilddaten selbst bekannt zu geben sind, sah die DSK keinen Anlass, von ihrer bisherigen Rechtsprechung abzuweichen, zumal die dort angeführten Argumente für die Ausnahme vom Auskunftsrecht durch die Änderung der Rechtslage mit der DSG-Novelle 2010 nicht entkräftet werden. Auch in den EB zur RV (472 d.B., XXIV. GP) wird – wohl in Kenntnis der zitierten Judikatur der DSK – ausgeführt, dass § 50e das Auskunftsrecht für Videoüberwachung lediglich »modifiziert«, also keinen neuen Auskunftsanspruch schaffen soll. Eine andere Auslegung kann dem Gesetzgeber gerade in Kenntnis der Rechtsprechung der DSK nicht unterstellt werden. Die Anwendbarkeit von § 50e DSG 2000 setzt also voraus, dass überhaupt ein Auskunftsanspruch besteht, was iSd genannten Rechtsprechung nur hinsichtlich ausgewerteter Videoaufzeichnungen der Fall wäre.

Wenn dagegen allenfalls ins Treffen geführt wird, dass diese Rechtsprechung der DSK mit der dem DSG 2000 zugrunde liegenden Richtlinie 95/46/EG (RL) nicht vereinbar sei, so wird auf deren Art. 13 verwiesen, wonach die Mitgliedstaaten u. a.

vom Auskunftsrecht iSd Art. 12 RL Ausnahmen vorsehen können, die notwendig sind, um die Rechte und Freiheiten anderer Personen zu wahren (lit. g). Nichts anderes soll die Rechtsprechung der DSK bewirken: Es soll dem Auftraggeber nicht allein aufgrund eines Auskunftsbegehrens die Kenntnis über die erfassten – vom Betroffenen unterschiedenen – Personen gegeben werden. Da im konkreten Fall eine Auswertung nicht vorgenommen wurde, war die Beschwerde mangels Bestehen eines Auskunftsanspruchs in Bezug auf die Bilddaten selbst gemäß § 26 DSG 2000 (iVm § 50e DSG 2000) abzuweisen.

Dieser Bescheid wurde beim Verwaltungsgerichtshof angefochten. Das Verfahren ist anhängig.

d. Auskunft aus dem PAD (K121.632/0008-DSK/2010, 24. 11. 2010)

Sachverhalt

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Auskunft dadurch, dass die Beschwerdegegnerin (eine Sicherheitsdirektion) sein ausdrücklich auch auf automations- wie nicht-automationsunterstützt geführte Aktenprotokollierungs- und Aktendokumentationssysteme (wie Protokollbücher, Steckzettelindices, AMKO, AVNT und PAD sowie kriminalpolizeiliche Erhebungs- bzw Kopienakten) bezogenes Auskunftsbegehren hinsichtlich der Akten ohne Begründung nicht beantwortet habe.

Tatsächlich wurde gegen den Beschwerdeführer in den Jahren 2008 und 2009 vom Landeskriminalamt ein kriminalpolizeiliches Ermittlungsverfahren wegen Verdachts von Straftaten nach §§ 144, 146 ff, 201 und 207a StGB geführt. Das entsprechende Verfahren wurde in einem zumindest teilweise automationsunterstützt geführten und dokumentierten Akt im polizeilichen Aktenverwaltungssystem PAD gespeichert.

Die Beschwerdegegnerin erteilte dem Beschwerdeführer betreffend die Datenanwendungen Personenfahndung, Personeninformation, kriminalpolizeilicher Aktenindex, Sachenfahndung und erkennungsdienstliche Evidenz eine inhaltlich negative Auskunft (Formulierung entsprechend den Bestimmungen des SPG). Sie ergänzte diese Auskunft im laufenden Verfahren dahin gehend, dass zu den oben angeführten Ermittlungen »ein unter der Aktenzahl … elektronisch angelegter Akt im polizeilichen Aktenverwaltungssystem (PAD)« besteht. Dieser sei jedoch nicht Teil eines Informationsverbundsystems und für andere Dienststellen nicht einsehbar. Da der Beschwerdeführer aufgrund der erfolgten gerichtlichen Einstellung des Strafverfahrens »polizeilich ein unbeschriebenes Blatt« sei, »wurden diese Daten den bisherigen Gepflogenheiten entsprechend nicht beauskunftet.«

Rechtliche Würdigung

Bei der Datenanwendung PAD handelt es sich um ein System, das der Aktenverwaltung und automationsunterstützten Dokumentation von Aktenstücken dient (Rechtsgrundlage § 13 Abs. 2 SPG). Hinsichtlich des Auskunftsrechts ist zwischen den im Aktenverwaltungssystem erfassten Daten zur Verwaltung des Aktes und dem Inhalt des Aktes zu unterscheiden. Auf letztere bezieht sich das Akteneinsichtsrecht nach dem in § 53 StPO geregelten Verfahren.

Jedenfalls beim mithilfe von PAD geführten Aktenregister betreffend kriminalpolizeiliche Ermittlungsverfahren handelt es sich um automationsunterstützt verarbeitete personenbezogene Daten, die »nach Maßgabe gesetzlicher Bestimmungen« dem verfassungsmäßigen Auskunftsrecht gemäß §§ 1 Abs. 3 Z 1 und 26 Abs. 1 DSG 2000 unterliegen. Die Auskunftspflicht besteht insoweit auch hinsichtlich der Daten, die nur mehr für Dokumentationszwecke gespeichert (»abgelegt«) sind und insbesondere Dritten wie anderen Behörden und Dienststellen nicht mehr zugänglich gemacht werden (eigentliche Protokolldaten, »äußere Verfahrensdaten«). Die »bisherigen Gepflogenheiten« der Beschwerdegegnerin stellen dabei keinen Grund für die Nichtgewährung der Auskunft dar.

Hinsichtlich der im PAD auch erfassten Inhaltsdaten ist betreffend die Ausnahmen vom Auskunftsrecht neben § 26 Abs. 2 DSG 2000 (etwa die Z 5 leg. cit.) oder den

Rechten insbesondere anderer Verfahrensbeteiligter auch auf § 26 Abs. 8 DSG 2000 zu verweisen. Diese Bestimmung sieht vor, dass in dem Umfang, in dem eine Datenanwendung hinsichtlich der verarbeiteten Daten von Gesetzes wegen für den Betroffenen einsehbar ist, das Recht auf Auskunft nach Maßgabe der das Einsichtsrecht vorsehenden Bestimmungen zu gewähren ist und für das Verfahren der Einsichtnahme die das Einsichtsrecht regelnden Gesetzesbestimmungen maßgeblich sind. Nur soweit ein Einsichtsrecht überhaupt nicht geregelt ist, kann der Auskunftsanspruch nach § 26 DSG 2000 geltend gemacht werden. Der von den Regelungen über die Akteneinsicht erfasste Bereich fällt daher als Spezialfall der direkten Kenntnisnahme des authentischen Inhalts (auch) elektronisch dokumentierter Aktenstücke unter die Ausnahmebestimmung des § 26 Abs. 8 DSG 2000. Das bedeutet, dass das Auskunftsrecht nach § 26 DSG 2000 den Betroffenen ermöglicht, von den sie betreffenden Akten Kenntnis zu erlangen, dass aber die Frage, ob sie Anspruch auf den Inhalt des Aktes haben, durch die jeweiligen Bestimmungen über die Akteneinsicht geregelt wird.

Im Anlassfall war die Einsicht in den elektronischen Akt eines kriminalpolizeilichen Ermittlungsverfahrens nach den dafür vorgesehenen Regeln (§§ 51 ff StPO) zulässig, insbesondere sieht § 53 Abs. 2 StPO ausdrücklich die Möglichkeit einer »elektronischen Akteneinsicht« vor. Daraus folgt, dass die Beschwerdegegnerin den Beschwerdeführer durch die Ablehnung einer inhaltlichen Auskunft über die im PAD verarbeiteten, ihn betreffenden äußeren Verfahrensdaten des gegenständlichen Ermittlungsverfahrens in seinem Recht auf Auskunft verletzt hat. Soweit damit die Einsicht in den – in Papierform oder elektronisch – dokumentierten Akteninhalt (»innere« Verfahrensdaten wie Textdokumente, Scans fremder Urkunden etc) verwehrt worden ist, wurde jedoch kein subjektives Recht des Beschwerdeführers verletzt.

e. Interne Zugriffe auf Daten sind keine Übermittlungen (K121.643/0002-DSK/2011, 21. 1. 2011)

Sachverhalt

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Auskunft dadurch, dass ihm der Beschwerdegegner in der grundsätzlich erteilten Auskunft vom Juli 2010 im Speziellen Auskunft darüber verweigert habe, wer Zugriff auf bestimmte ihn betreffende Daten (eine bestimmte E-Mail an den Beschwerdeführer) gehabt habe und an wen diese weitergeleitet worden seien. Er benötige die Auskunft, um den unrichtigen Inhalt der E-Mail gegenüber den Empfängern richtigstellen zu können.

Dieses spezielle Auskunftsbegehren wurde vom Beschwerdegegner abgelehnt; die Daten seien nicht übermittelt worden, sondern nur den zuständigen Betreuern zugänglich gewesen.

Rechtliche Würdigung

Der für Zwecke eines Verwaltungsverfahrens, dessen Partei der Beschwerdeführer war und ist, dokumentierte E-Mail-Schriftverkehr stellt zwar einen auf die Partei Bezug nehmenden Datenbestand dar. Solange diese Daten allerdings beim Auftraggeber nur gespeichert werden und Personen zugänglich waren, die mit dem Verfahren befasst wurden, liegt kein Akt der Datenübermittlung vor, der der Auskunftspflicht unterliegt. Dafür, dass die Daten an weitere Auftraggeber oder durch Zweckänderung gemäß § 4 Z 12 DSG 2000 übermittelt worden sind, liegt weder eine ausdrückliche Behauptung vor, noch sind dafür im Verfahren Anhaltspunkte hervorgekommen. Es liegt auch (entgegen der im Verfahren geäußerten Meinung des Beschwerdeführers) keine Dienstleistung iSd § 4 Z 5 DSG 2000 vor.

f. Ist die Abfrage von EKIS-Daten auskunftspflichtig? (K121.649/0003-DSK/2011, 18. 2. 2011)

Sachverhalt

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Auskunft dadurch, dass der Beschwerdegegner (Bundesministerium für Inneres) im Auskunftsschreiben bzw dessen Ergänzung keine Auskunft darüber erteilt habe, von wem und zu welchem Zeitpunkt etwaige EKIS-Abfragen durchgeführt wurden.

Die Auskunft des Beschwerdegegners ergab, dass in den EKIS-Datenanwendungen Personenfahndung, Personeninformation, KPA, Sachenfahndung, erkennungsdienstliche Evidenz, automationsunterstütztes Fingerabdrucksystem und DNA-Datenbank im Auftrag des Beschwerdegegners keine der Auskunftspflicht unterliegenden Daten verarbeitet würden. Es wurde darauf hingewiesen, dass in der Datenanwendung Sachfahndung durch eine Bezirkshauptmannschaft (verlorener Führerschein) und in der Datenanwendung KPA durch eine weitere Bezirkshauptmannschaft Daten zur Person des Beschwerdeführers verarbeitet würden. Weitere Auskunfts- oder Löschungsbegehren wären an diese Sicherheitsbehörden zu richten. In der Datenanwendung »Evidenthaltung von Aufnahmewerbern für den Exekutivdienst« würden keine den Beschwerdeführer betreffenden Daten verarbeitet. Eine Auskunft aus dem Strafregister sei gemäß Strafregistergesetz (Ausstellung einer Strafregisterbescheinigung) einzuholen. Nach Rüge durch den Beschwerdeführer in Bezug auf die EKIS-Abfragen ergänzte der Beschwerdegegner die Auskunft dadurch, indem er mitteilte, dass Übermittlungen gemäß § 4 Z 12 DSG 2000 nur die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister (sowie die Datenverwendung für ein anderes Aufgabengebiet) sei. Für die Datenanwendungen, in denen der Beschwerdegegner Daten verarbeite, sei diese Auskunft auch korrekt erfolgt. Auf die Daten, die im Auftrag weiterer Sicherheitsbehörden verarbeitet würden, ist nochmals verwiesen worden.

Rechtliche Würdigung

Im Fall der Datenanwendung EKIS handelt es sich um ein Informationsverbundsystem (§ 4 Z 13 DSG 2000), für das der Beschwerdegegner nur insoweit Auftraggeber ist, als er selbst die Entscheidung trifft, Daten in den systemzugehörigen Datenanwendungen (wie dem KPA) zu verarbeiten. Für Daten, die andere Sicherheitsbehörden verarbeiten, konnte sich der Beschwerdegegner als Betreiber mit Recht darauf beschränken, gemäß § 50 Abs. 1 DSG 2000 »den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber« bekanntzugeben. Dies ist auch geschehen.

Der jeweilige Auftraggeber (BH 1 für EKIS-Sachenfahndung bzw BH 2 für EKIS-KPA) kann hinsichtlich des Auskunftsrechts zu Empfängern oder Empfängerkreisen von Datenübermittlungen in Anspruch genommen werden. Auch die DSK wies darauf hin, dass nicht jede Abfrage eine Datenübermittlung ist. So unterscheiden die datenschutzrechtlichen Definitionen des § 4 Z 9 und Z 12 DSG 2000 ausdrücklich zwischen dem Übermitteln von Daten und bspw. dem Abfragen oder Benutzen. Da gemäß § 26 Abs. 1 DSG 2000 aber nur »allfällige Empfänger und Empfängerkreise von Übermittlungen« zu beauskunften sind, sind einzelne Vorgänge der Datenverarbeitung gemäß § 4 Z 9 DSG 2000, die durch Organwalter oder Bedienstete des Auftraggebers ausgeführt werden, wie das Abfragen, Benützen oder Ausgeben (inkl Ausdrucken) von Daten, nicht Gegenstand der Pflicht zur Auskunftserteilung an den Betroffenen.

g. Identitätsnachweis bei Auskunft war überspannt (K121.715/0010-DSK/2011, 2. 9. 2011)

Sachverhalt

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Auskunft dadurch, dass die Beschwerdegegnerin (eine Bundespolizeidirektion) auf sein Auskunftsbegehren betreffend seine für Zwecke anhängiger und abgeschlossener Verwaltungsstrafverfahren gespeicherten Daten mit der Aufforderung reagiert habe, sein Geburtsdatum,

seinen Geburtsort sowie die Vornamen seiner Eltern anzugeben. Er sei dem nicht gefolgt, da er seiner Mitwirkungspflicht bereits durch die Übermittlung eines Identitätsnachweises (Kopie seines Führerscheins als Beilage zum Auskunftsbegehren) nachgekommen sei. Die Auskunftserteilung unterblieb.

Der übermittelte Führerschein enthielt Vor- und Familien-/Nachnamen des Beschwerdeführers, Geburtsdatum und Geburtsort, Ausstellungsdatum des Führerscheins sowie ein Lichtbild und eine Faksimile-Wiedergabe der Unterschrift des Beschwerdeführers.

Rechtliche Würdigung

Die Beschwerde war berechtigt. Das Gesetz fordert vom Betroffenen und Auskunftswerber in § 26 Abs. 1 DSG 2000 die Erbringung eines Identitätsnachweises als Voraussetzung für die Erteilung einer Auskunft über seine Daten durch den angesprochenen Auftraggeber. Der Identitätsnachweis ist conditio sine qua non für das Entstehen eines Anspruchs auf inhaltliche Auskunft. Diese Bestimmung hat den erkennbaren Zweck, jedem möglichen Missbrauch des Auskunftsrechts zur Informationsbeschaffung durch Dritte einen Riegel vorzuschieben. Ein Auftraggeber darf ohne Vorliegen eines Identitätsnachweises keine Daten an den Auskunftswerber – von dem er in diesem Moment nur annehmen kann, dass er tatsächlich der Betroffene ist – übermitteln, da er sonst das Datengeheimnis gem § 15 Abs. 1 DSG 2000 verletzen könnte. Bloßes Vertrauen auf die Identität des Auskunftswerbers kann den Identitätsnachweis nicht ersetzen, da mit einer derart großzügigen Auslegung der Wortfolge »in geeigneter Form nachweist« dem Schutzzweck der Norm die Grundlage entzogen wäre.

Sorgfaltspflichten (§§ 6, 14 DSG 2000) verpflichten die Beschwerdegegnerin auch dazu, vor Auskunftserteilung einen Identitätsnachweis zu verlangen. Dieser Obliegenheit ist der Beschwerdeführer allerdings bereits durch Übermittlung einer Ausweiskopie samt Faksimile-Wiedergabe seiner eigenhändigen Unterschrift (zusätzlich zum eigenhändig unterschriebenen Auskunftsbegehren) nachgekommen: Für die Frage, wie ein »Identitätsnachweis iSd § 26 Abs. 1 DSG 2000« zu erbringen ist, ist darauf abzustellen, was darzutun geeignet ist, dass das Auskunftsbegehren von der als Auskunftswerber bezeichneten und in ihrer Identität amtlich bestätigten Person herstammt. In der Rechtsprechung der DSK wurde mehrfach die Kopie eines amtlichen Lichtbildausweises als ausreichender Nachweis angesehen, um durch Vergleich der Unterschriften im Ausweis und auf dem Auskunftsbegehren mit hinreichender Sicherheit die Feststellung der Identität des Auskunftswerbers zu ermöglichen und die Echtheit des Auskunftsbegehrens zu erkennen.

Hier hat der Beschwerdeführer einen gültigen Identitätsnachweis erbracht. Die ins Treffen geführte Mitwirkungsobliegenheit gem § 26 Abs. 3 DSG 2000 dient dem Zweck, dem Auftraggeber ein Mittel in die Hand zu geben, um ausufernde und ihn unbillig belastende Auskunftsbegehren einzugrenzen (arg: »um ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden«), nicht aber, einen Identitätsnachweis verlangen zu können. Auf § 26 Abs. 3 DSG 2000 konnte daher die Aufforderung, weitere Daten zwecks Identitätsprüfung bekannt zu geben, nicht wirksam gestützt werden.

Anhaltspunkte dafür, dass ausgehend vom vollständigen Namen, Geburtsdatum und Geburtsort die konkrete Gefahr bestanden hätte, Auskunft über nicht den Beschwerdeführer betreffende Daten zu erteilen, was die Beschwerdegegnerin zu weiteren Rückfragen berechtigen könnte, bestanden im gegenständlichen Fall nicht. Die Beschwerdegegnerin hat durch Bestehen auf Übermittlung der Vornamen der Eltern des Beschwerdeführers und Unterbleiben der Auskunft den Beschwerdeführer in diesem Recht verletzt.

6.1.2 Recht auf Geheimhaltung

a. Datenermittlungen durch KIAB (K121.560/0003-DSK/2010, 24. 2. 2010)

Sachverhalt

Die Beschwerdeführer (ein Unternehmen, dessen Geschäftsführer sowie ein Projektleiter) behaupten eine Verletzung im Recht auf Geheimhaltung durch verschiedene Datenverwendungsschritte, die die Sondereinheit KIAB des Beschwerdegegners (eines Finanzamtes) bzw. für diese handelnde Beamte im Rahmen von Kontrollen auf einer Baustelle in Kärnten im Frühjahr 2009 durchgeführt hätten.

Bedienstete der Sondereinheit KIAB führten dabei Kontrollen der Einhaltung ausländerbeschäftigungs- und sozialversicherungsrechtlicher Vorschriften durch. Die Erstbeschwerdeführerin wurde auf dieser Baustelle an diesem Tag als Subunternehmerin der X tätig und beschäftigte dort polnische Arbeitnehmer, die wiederum von einer portugiesischen Firma, einer weiteren Subunternehmerin, diesmal der Erstbeschwerdeführerin, auf die Baustelle entsendet worden waren. An einem bestimmten Tag forderte ein KIAB-Mitarbeiter telefonisch Unterlagen beim Zweitbeschwerdeführer, dem Geschäftsführer der Erstbeschwerdeführerin, an, wobei er dessen Mobiltelefonnummer (Firmenhandy mit Geheimnummer) verwendete. Diese Nummer war von einem Mitarbeiter der Erstbeschwerdeführerin vor Ort bekannt gegeben worden. Später gab die Erstbeschwerdeführerin diese Nummer weiters im Zuge einer Meldung bei der ZKO als Kontaktnummer bekannt. Im Zuge der Kontrollen nahmen Mitarbeiter der KIAB weiters Kopien der Stundenaufzeichnungen der Baustelle (Angaben der von den einzelnen Beschäftigten je Werktag geleisteten Arbeitsstunden) entgegen, die später gescannt und in einer verfahrensbezogenen Datenanwendung (»KIAB online«) verwendet wurden. An einem anderen Tag wurde den KIAB-Mitarbeitern anlässlich einer weiteren Kontrolle ausdrücklich von anwesenden Vertretern der Beschwerdeführer untersagt, die Mobilfunknummern des Zweit- und des Drittbeschwerdeführers (Projektleiter) zu benützen, trotzdem wurden beide in der Folge telefonisch kontaktiert, wobei der Drittbeschwerdeführer zur Bekanntgabe der geheimen Mobilfunknummer des Zweitbeschwerdeführers an einen weiteren KIAB-Mitarbeiter aufgefordert wurde.

Rechtliche Würdigung

Die DSK führte zunächst aus, dass sie gesetzmäßig nicht dazu berufen ist, eine allgemeine Rechtskontrolle über die Verfahrensführung anderer Behörden auszuüben. So weit die Beschwerdeführer solche allgemeinen Mängel rügen, wurden sie auf die entsprechenden Rechtsschutzmöglichkeiten (insbesondere die Rüge relevanter Verfahrensmängel im Zuge jedes denkbaren Berufungsverfahrens, gleich ob nach BAO, AVG oder VStG) verwiesen.

In der Sache selbst besteht grundsätzlich ein – im Fall von Verwaltungsübertretungen insbesondere durch § 25 Abs. 1 iVm § 26 Abs. 1 VStG, im allgemeinen Verwaltungsverfahren durch die §§ 37 und 39 Abs. 2 AVG sowie besondere Zuständigkeitsbestimmungen zum Ausdruck kommendes – berechtigtes Interesse der zuständigen Behörde an der Verwendung personenbezogener Daten, insbesondere deren Ermittlung für Zwecke eines Verwaltungs(straf)verfahrens, welches das Interesse der Betroffenen an der Geheimhaltung ihrer personenbezogenen Daten überwiegt, sodass gem § 8 Abs. 1 Z 4 bzw § 8 Abs. 4 Z 3 DSG 2000 eine Verletzung von nach § 1 Abs. 1 leg cit. bestehenden schutzwürdigen Geheimhaltungsinteressen nicht vorliegt. Als Maßstab für eine Beurteilung der Zulässigkeit der Datenermittlung in solchen Verfahren verbleibt für die DSK das Übermaßverbot als Ausdruck des in § 1 Abs. 2 und § 7 Abs. 3 DSG 2000 normierten Verhältnismäßigkeitsgrundsatzes: Wenn es denkmöglich ist, dass die von einer in der Sache zuständigen Behörde ermittelten Daten nach Art und Inhalt für die Feststellung des relevanten Sachverhalts geeignet sind, ist die Zulässigkeit der Ermittlung aus datenschutzrechtlicher Sicht gegeben (siehe den Bescheid vom 29. November 2005, K121.046/0016-DSK/2005).

Die Verwendung der Mobilfunknummern ist in diesem Sinne eindeutig für den Verfahrenszweck als relevant und nicht überschießend zu werten, womit die Frage dahingestellt bleiben kann, ob tatsächlich ein auf § 8 Abs. 1 Z 2 DSG 2000 gestütztes sinngemäßes Verbot des Wählens einer Mobilfunknummer ausgesprochen werden kann, wie die Beschwerdeführer behaupten. Gleiches gilt für die Frage, ob der Beschwerdegegner berechtigt war, die Daten der Stundenaufzeichnungen zu verarbeiten und zu verwenden. Unabhängig von der Frage, ob es sich dabei um ein Geschäftsgeheimnis der Erstbeschwerdeführerin (Kalkulationsgrundlage) handelt, so erscheint es doch eindeutig denkmöglich, dass diese Aufzeichnungen für den Zweck des vom Beschwerdegegner geführten Ermittlungsverfahrens, nämlich zur Feststellung des relevanten Sachverhalts (etwa in der Frage, ob ein ausländischer Arbeitnehmer tatsächlich auf der fraglichen Baustelle beschäftigt worden ist), geeignet sind. Es kann dabei im Gegensatz zu den Ausführungen der Beschwerdeführer nicht entscheidend darauf ankommen, ob der Beschwerdegegner bei der Datenermittlung für Zwecke eines konkreten Ermittlungsschritts das AVG oder die BAO anzuwenden hatte, da jedenfalls § 8 Abs. 1 Z 4 und Abs. 3 Z 1 DSG 2000 als eine Art »allgemeiner Rückfallsebene« in Verbindung mit den Bestimmungen des § 26 Abs. 1 AuslBG und des § 7b Abs. 5 AVRAG (Einsichtsrechte) eine ausreichend konkrete Grundlage für entsprechende Datenermittlungen bilden. Die Beschwerde wurde daher zur Gänze abgewiesen.

b. Übermittlung von Meldedaten an eine politische Partei (K121.564/0006-DSK/2010, 14. 4. 2010)

Sachverhalt

Der Beschwerdeführer behauptete eine Verletzung im Recht auf Geheimhaltung dadurch, dass die Beschwerdegegnerin, eine Marktgemeinde, seine Meldedaten (Namen, akademischen Grad, Adresse, Meldung als Hauptwohnsitz am [Datum]) an die Ortsgruppe einer bestimmten politischen Partei übermittelt habe, die diese in ihrem lokalen Informationsblatt in der Rubrik »Zuzüge« zusammen mit den Daten anderer Personen veröffentlicht habe.

Tatsächlich übermittelte das Marktgemeindeamt diese Daten, zusammen mit den Daten anderer Zuzüge eines bestimmten Zeitraums, auf Weisung des Bürgermeisters an die Ortsgruppe der politischen Partei, die diese in ihrem Mitteilungsblatt veröffentlichte.

Rechtliche Würdigung

Die DSK sah die Beschwerde aus folgenden Gründen als berechtigt an:

Die Melderegister sind gem. § 16 Abs. 1 MeldeG nur insoweit öffentlich, als nach nicht einer Auskunftssperre unterliegenden Personen gesucht werden darf, die der Anfragende durch Angabe des Namens und eines weiteren Merkmals nach § 16 Abs. 1 MeldeG eindeutig bestimmen kann, um deren nähere Adressdaten zu erfahren. Die Auswahl und Übermittlung von Meldedaten nach dem Kriterium »aktuelle Zuzüge« ohne Erfüllung der Voraussetzungen des § 16 Abs. 1 MeldeG durch den Anfrager ist rechtlich nicht gedeckt. Meldedaten dürfen also nicht pauschal und für ganze Kategorien von Betroffenen an Dritte übermittelt werden. Auch die Berufung der Beschwerdegegnerin auf »Gewohnheitsrecht« (»lang und weit geübten Praxis«) rechtfertigt die Vorgangsweise nicht, da der österreichischen Rechtsordnung im Bereich des öffentlichen Rechts jedes Gewohnheitsrecht fremd ist.

Schließlich war der Hinweis der Beschwerdegegnerin auf ein »öffentliches Interesse« an der in Beschwerde gezogenen Datenverwendung verfehlt. Einerseits kann für einen gesetzlich klar geregelten Zweck wie den der Verwendung von Meldedaten eine über den gesetzlich geregelten Umfang hinausgehende Datenverwendung nicht auf den Rechtfertigungstatbestand nach § 8 Abs. 1 Z 4 DSG 2000 gestützt werden, da in solchen Fällen die gesetzlich geregelte Datenverwendung als taxativ anzusehen ist. Andererseits begründet das »Interesse« einer größeren Zahl von Menschen kein überwiegendes und berechtigtes Interesse, auf das

die Beschwerdegegnerin ihr Handeln contra legem auch nur abstrakt stützen könnte. Die in Beschwerde gezogene Datenübermittlung stellte somit einen nicht gerechtfertigten Eingriff in das Grundrecht des Beschwerdeführers auf Geheimhaltung personenbezogener Daten dar.

c. Elektronische Hochschülerschaftswahl 2009 (K121.580/0007-DSK/2010, 12. 5. 2010)

Sachverhalt

Die Beschwerdeführerin behauptete, dadurch im Recht auf Geheimhaltung verletzt worden zu sein, dass bei ihrer Teilnahme an der ÖH Wahl 2009 mittels elektronischer Stimmabgabe (E-voting) ihr elektronischer Stimmzettel in einer Weise verarbeitet wurde, dass ihre Stimme auf sie persönlich rückführbar war, bzw. dass die eingesetzten technischen und organisatorischen Vorkehrungen davor nicht ausreichend geschützt hätten und die Datenanwendung daher in das Grundrecht weiter eingriff, als dies für die Durchführung der Wahl erforderlich sei. Weiters brachte die Beschwerdeführerin vor, dass die von der Wahlkommission zur Verfügung gestellte Software auf ihrem Computer einen Systemabsturz verursacht habe. Die Beschwerdeführerin macht geltend,

a. dass § 34 Abs. 4 des HSG 1998 nicht jenen Anforderungen entspreche, wie sie § 1 Abs. 2 DSG 2000 für Eingriffsermächtigungen in das Grundrecht auf Datenschutz fordere. Die Normierung der allgemeinen Zulässigkeit des E-Votings mit pauschalem Verweis auf die HochschülerInnenschaftswahlordnung 2005 sei keine ausreichende gesetzliche Grundlage.
b. dass im HSG 1998 keine angemessenen Schutzgarantien zugunsten der verwendeten sensiblen Daten zu finden seien, wie dies § 1 Abs. 2 2. Satz DSG 2000 vom Materiengesetzgeber verlange.
c. dass das Gebot des gelindesten Mittels verletzt worden sei, indem nach dem Ende des E-Votings die Stimmen in einer Form, die die Herstellung des Personenbezugs ermöglicht und somit die Feststellung, welche Person wie gewählt habe, zugelassen habe, auf eine CD-ROM gebrannt worden seien.

Die DSK möge daher feststellen, dass die Beschwerdeführerin durch das E-Voting im Rahmen der ÖH-Wahl 2009 in ihrem Recht auf Datenschutz verletzt worden sei.

Die Beschwerdeführerin nahm am 18. Mai 2009 an der elektronischen Hochschülerinnen- und Hochschülerschaftswahl 2009 (im Folgenden kurz: Wahl) teil. Dabei verursachte der von der Wahlkommission zur Verfügung gestellte Wahlclient auf ihrem Computer einen Systemabsturz. Erst nach einem Neustart des Computers konnte die Beschwerdeführerin ihre Stimme abgeben. Dabei wurde die Stimme in verschlüsselter Form und ohne Zwischenspeicherung direkt an das Wahlsystem übermittelt. Nach Ende der letzten Wahlhandlung wurde knapp nach 17:00 Uhr mit der Auszählung der Papierstimmzettel begonnen. Ungefähr 1,5 Stunden später wurden die verschlüsselten Stimmen aus dem Wahlsystem in das Wahladministrationssystem zur Auszählung der elektronisch abgegebenen Stimmen auf einer CD übermittelt. Die Auszählung erfolgte in Anwesenheit der Wahlkommissionsmitglieder auf einem mobilen Computer durch einen Mitarbeiter der BRZ-GmbH mit deren geheimen Schlüssel. Der Vorgang wurde durch einen gerichtlich beeideten IT-Ziviltechniker überwacht.

Im Wahlsystem waren die Identitätsdaten und die Wahlstimme getrennt voneinander verschlüsselt. Bei der Stimmauszählung wurden zuerst alle Identitätsdaten (keine Namen, sondern ausschließlich bereichsspezifische Personenkennzeichen [bPK]) mit dem geheimen Schlüssel der BRZ-GmbH entschlüsselt. Dabei wurden jene Stimmen aus der elektronischen Urne entfernt, die von nicht stimmberechtigten Personen abgegeben wurden. Zugleich wurden alle Identitätsdaten vom Datensatz entfernt und gelöscht. Die noch mit dem Schlüssel der Wahlkommission verschlüsselten Wahlstimmen wurden dann gemischt und in das Wahladministrationssystem übermittelt.

Dort wurden sie mithilfe der geheimen privaten Schlüssel von zwei Mitgliedern der Wahlkommission entschlüsselt und gezählt.

Der in zwei Teile aufgeteilte geheime Schlüssel für die Entschlüsselung der Wahlstimmen wird ausschließlich von vier Mitgliedern der Wahlkommission sicher verwahrt. Die CD wird gem § 69 HSWO 2005 vom Vorsitzenden der Wahlkommission mindestens 5 Jahre lang sicher verwahrt. Die bei der Auszählung verwendete Hardware wurde nach Abschluss der Auszählung mechanisch zerstört.

Das Wahlsystem wurde unter der DVR Nr 4000407/001 und das Wahladministrationssystem wurde unter der DVR Nr 4000407/002 am 2. April 2009 im DVR registriert.

Rechtliche Würdigung

Gemäß § 39 HSG 1998 ist die Wahlkommission für die Durchführung der Wahlen zuständig und somit sowohl Auftraggeber iSd § 4 Z 4 DSG 2000 als auch Beschwerdegegner im gegenständlichen Verfahren. Die Aufnahme der Datenverarbeitung durch die Durchführung der elektronischen Wahl war nach Melde- und Vorabkontrollverfahren im DVR grundsätzlich zulässig.

Soweit die Beschwerdegegnerin nun vorbrachte, für den Einsatz von E-Voting bei der Wahl bestehe keine ausreichende gesetzliche Grundlage, da die im HSG 1998 enthaltenen Bestimmungen nicht ausreichend determiniert seien (ohne zu bestreiten, dass eine Rechtsgrundlage dem Grunde nach vorhanden ist – § 34 Abs. 4 HSG 1998 iVm der HSWO 2005), hielt ihr die DSK entgegen, dass die im Ergebnis behauptete Verfassungswidrigkeit des HSG 1998 bzw der HSWO 2005 nur vor dem VfGH geltend gemacht werden kann (Art. 140 Abs. 1 B-VG bzw. Art. 139 Abs. 1 B-VG). Die DSK hat überdies kein Recht zur Anfechtung von Verordnungen oder Gesetzen vor dem VfGH. § 34 Abs. 4 bis 6 HSG 1998 ordnen zweifelsfrei die Möglichkeit der elektronischen Stimmabgabe bei Hochschülerschaftswahlen gesetzlich an. Die §§ 61 ff HSWO 2005 spezifizieren auf Grundlage der Verordnungsermächtigung in § 34 Abs. 7 HSG 1998 nur die im Gesetz vorgesehenen technischen Funktionen und organisatorischen Pflichten im Detail, insbesondere welche Art von Software zu verwenden ist, welche Schlüssel einzusetzen sind und welche Anforderungen die BRZ GmbH zu erfüllen hat, in der die Applikation betrieben wird.

Der Behauptung, dass im HSG 1998 keine angemessenen Garantien für die Geheimhaltung der beim E-Voting verarbeiteten sensiblen Daten über die politische Meinung vorgesehen sind, war insbesondere § 34 Abs. 5 HSG 1998 entgegenzuhalten, der eingehende Vorgaben für angemessene Garantien macht. Ob diese Vorgaben im Lichte der Verfassungsbestimmung des § 1 Abs. 2 2. Satz DSG 2000 ausreichend sind, entscheidet wiederum nur der VfGH.

Die Behauptung der Verletzung des Gebots des gelindesten Mittels dadurch, dass nach dem Ende des E-Votings die Stimmen in einer Form, die die Herstellung des Personenbezugs ermöglicht und somit die Feststellung, welche Person wie gewählt habe, zugelassen habe, auf eine CD gebrannt worden seien, sah die DSK bei der Verwendung der für die Wahl eingesetzten Datenanwendungen nicht verwirklicht. Die Identitätsdaten dienten nur der Überprüfung der Wahlberechtigung vor der Auszählung der Stimmen. Bevor die Stimmen zwecks Zählung entschlüsselt werden, wird der Personenbezug der Stimme (ausschließlich das bPK des Wählers) gelöscht. Erst nach nochmaliger »Mischung« der Stimmen, um jede Erkennbarkeit nach der Reihenfolge unmöglich zu machen, werden die Stimmen entschlüsselt und gezählt. Diese Trennung der Verknüpfung zwischen den Identitätsdaten und dem »Stimmzettel« durch Löschung der Identitätsdaten vor »Öffnen« des Stimmzettels in Anwesenheit der Wahlkommissionsmitglieder erfolgt durch einen Mitarbeiter der BRZ-GmbH mit deren geheimen Schlüssel. Der Vorgang wird auch durch einen gerichtlich beeideten IT-Ziviltechniker überwacht. Die Mitglieder der Wahlkommission stellen Ihren Schlüssel zum »Öffnen« erst dann zur Verfügung, wenn die Identitätsdaten gelöscht wurden. Bei der elektronischen Wahl müssten daher sowohl

die Mitglieder der Wahlkommission als auch die BRZ-GmbH, der IT-Ziviltechniker und die DSK als Stammzahlenregisterbehörde oder eine andere Behörde aus demselben Bereich iSd § 9 Abs. 2 E-Governmentgesetz wie die Wahlkommission rechtswidrig zusammenwirken, um das Stimmverhalten einer bestimmten Person sichtbar zu machen.

Dem Gebot des Einsatzes des gelindesten Mittels wird durch diese mehrfach verschlüsselten Wahldaten auf einer CD, die zum Zwecke der Behandlung eines Einspruchs gegen die Wahl gem § 69 HSWO 2005 mindestens 5 Jahre lang aufzubewahren ist, gem § 14 DSG 2000 nachgekommen. Die Einhaltung und tatsächliche Umsetzung dieser Maßnahmen wurde sowohl durch die im § 34 Abs. 6 HSG 1998 vorgesehene Überprüfung durch eine Bestätigungsstelle gem § 19 Signaturgesetz, als auch im Vorabkontrollverfahren durch das DVR überprüft.

Die Beschwerde war somit insgesamt spruchgemäß abzuweisen.

Gegen diesen Bescheid hat die Beschwerdeführerin Beschwerde an den Verfassungsgerichtshof erhoben, über die dieser mit Erkenntnis vom 14. Dezember 2011, B 898/10-9, entschieden und den Bescheid der DSK aufgehoben hat. Dabei ist der Verfassungsgerichtshof unter Hinweis darauf, dass mit Erkenntnis vom 13. Dezember 2011, V 85-96/11, der 8. Abschnitt (§§ 61 bis 69) der Hochschülerinnen- und Hochschülerschaftswahlordnung 2005 (HSWO) als gesetzwidrig aufgehoben wurde und die Datenschutzkommission bei Erlassung des angefochtenen Bescheides die als gesetzwidrig aufgehobenen Bestimmungen angewendet hat, davon ausgegangen, dass es nach Lage des Falles nicht ausgeschlossen sei, dass dadurch die Rechtssphäre der Beschwerdeführerin nachteilig beeinflusst worden sei. Der Verfassungsgerichtshof hat allerdings in seinem Erkenntnis, mit dem er Teile der HSWO aufhob, ausdrücklich festgehalten, dass sich aus einer Zusammenschau der Bestimmungen des HSG 1998 mit den allgemeinen Grundsätzen des DSG 2000 eine verfassungsrechtlich hinlänglich präzise Regelung in Bezug auf Umfang und Grenzen der datenschutzrechtlichen Befugnisse der Wahlkommission entnehmen lässt. Der Beschwerdevorwurf, es fehle für die Durchführung des E-Voting im Rahmen der ÖH Wahl an einer ausreichenden gesetzlichen Grundlage iSd §1 Abs. 2 DSG 2000, erweise sich daher als nicht begründet. Es wurde daher von der DSK ein Ersatzbescheid erlassen, mit dem abermals die Beschwerde abgewiesen wurde.

d. Übermittlung von KFZ-Zulassungsdaten an italienische Polizeibehörde (K121.590/0006-DSK/2010, 30. 6. 2010)

Sachverhalt

Die Beschwerdeführerin behauptete eine Verletzung im Recht auf Geheimhaltung dadurch, dass die Beschwerdegegnerin, eine Bundespolizeidirektion, im April 2009 auf Amtshilfeersuchen der Gemeindepolizei eines bestimmten italienischen Urlaubsortes ihre Daten Name, Vorname und Wohnadresse aus der Datenanwendung »Evidenz von Zulassungsdaten und Antragstellern auf Wunschkennzeichen« (Informationsverbundsystem »Zulassungsevidenz« gemäß den §§ 40b und 47 KFG 1967) postalisch an die italienische Polizeibehörde übermittelt hat. Diese verwendete die Daten zur Ergänzung des Ermittlungsverfahrens bzw zur Adressierung einer wegen einer Straßenverkehrsübertretung im Juli 2008 gegen die Beschwerdeführerin erlassenen Strafverfügung.

Rechtliche Würdigung

Die DSK sah die Beschwerde als nicht berechtigt an, weil sich die Beschwerdegegnerin bei der gegenständlichen Datenübermittlung zu Recht auf die §§ 7 Abs. 2, 8 Abs. 3 Z 2 DSG 2000 und Art. 8 des Amtshilfevertrags Österreich-Italien (Vertrag über die wechselseitige Amtshilfe in Kraftfahrangelegenheiten, BGBl Nr 406/1990) stützen konnte. Nach dem klaren Wortlaut des Art. 8 des Vertrags »(erteilen) die Behörden der Vertragsstaaten … einander auf Ersuchen Auskunft über zugelassene Fahrzeuge«. Diese rechtliche Verpflichtung ist in keiner Weise eingeschränkt.

Der Einwand der Beschwerdeführerin, Art. 1 des Vertrags schließe »Strafsachen«

von seinem Anwendungsbereich aus, war hier nicht relevant, da eine Auskunft über die Identität des Zulassungsbesitzers – als eine Art der Information über zugelassene Fahrzeuge – noch keine automatische Verfangenheit des Zulassungsbesitzers als Beschuldigter in einem Strafverfahren bedeutet. Der Zulassungsbesitzer ist zunächst nur Auskunftsperson hinsichtlich der Identität des Lenkers.

Schon aus § 86 Abs. 3 KFG 1967 ergibt sich, dass die italienischen Behörden auch ohne den speziellen Amtshilfevertrag Auskünfte aus der Zulassungsevidenz für Zwecke der Verfolgung von »Übertretungen von Verkehrsvorschriften« einholen dürfen (vgl. Bescheid der DSK vom 9. Juni 2006, K121.124/0011-DSK/2006, und das dazu ergangene Erkenntnis des VwGH vom 27. September 2007, 2006/06/0322). Auch das Bestehen dieser Rechtsvorschrift verbietet es, Art. 1 des Amtshilfevertrags Österreich-Italien so eng auszulegen, dass jede Datenübermittlung aus der Zulassungsevidenz, die ein Strafverfahren gegen den Betroffenen zur Folge haben könnte, nicht gestattet wäre.

e. Radarmessung durch Gemeinde (K121.359/0009-DSK/2010, 30. 6. 2010)

Sachverhalt

Der Beschwerdeführer wurde am 15. November 2007 mit seinem Pkw in einer Ortschaft der Beschwerdegegnerin (Gemeinde X) von einer in der dort aufgestellten stationären Radarkabine (»Radarbox«) installierten Geschwindigkeitsüberwachungsanlage mit 56 km/h (zulässige Geschwindigkeit: 30 km/h) gemessen und automatisch fotografiert. Das Messgerät, das im Auftrag der Gemeinde (Auftraggeberin iSd § 4 Z 4 DSG 2000) für Zwecke der Verkehrsüberwachung im Gemeindegebiet (durch einen privaten Dienstleister) betrieben wird, ermittelt in Form eines Nachschusses (Heckansicht des Fahrzeugs) als grafische Datei eine Aufnahme des Fahrzeugs, die gespeichert und an die örtlich zuständige Bezirkshauptmannschaft zur Einleitung eines Verwaltungsstrafverfahrens weitergeleitet wird. Der Beschwerdeführer fühlte sich durch diese Datenermittlung in seinem Recht auf Geheimhaltung verletzt.

Mit Bescheid der DSK vom 11. Juli 2008, GZ: K121.359/0016-DSK/2008, wurde der Beschwerde in diesem Punkt stattgegeben und eine Verletzung des Beschwerdeführers im Recht auf Geheimhaltung festgestellt. Dagegen hat die Gemeinde Beschwerde an den VwGH erhoben, der besagten Bescheid mit Erkenntnis vom 8. September 2009, 2008/17/0152 wegen Rechtswidrigkeit des Inhalts aufgehoben hat. Die DSK habe sich bei ihrer Entscheidung ausschließlich auf die gesetzlichen Zuständigkeiten der Beschwerdegegnerin als Behörde gestützt, und sei weder auf die Frage eingegangen, ob die Gemeinde auch als Trägerin von Privatrechten eine sonstige »Befugnis« gemäß § 7 Abs. 1 DSG 2000 ausgeübt haben könnte, noch habe sie eine Abwägung der schutzwürdigen Interessen der Parteien vorgenommen. Damit sei der Bescheid jedoch mit inhaltlicher Rechtswidrigkeit belastet worden.

Rechtliche Würdigung

Die DSK stellte zunächst wie schon im ersten Rechtsgang klar, dass die Aufzeichnung der Bilddaten von KFZ-Kennzeichen die Verarbeitung personenbezogener Daten darstellt und verwies dazu auf das Erkenntnis des VfGH zur »Section Control« (vom 15. Juli 2007, G 147/06). Daten über bestimmbare Personen iSd § 4 Z 1 DSG 2000 liegen schon dann vor, wenn der einzige Sinn der Datenermittlung darin liegt, die hinter den Kennzeichen stehenden Personen (Kraftfahrzeughalter) zu identifizieren, sei es auch erst durch einen »Dritten«, nämlich die Strafverfolgungsbehörde. Es handelt sich also um die Ermittlung von Daten über »bestimmbare Personen« durch die Beschwerdegegnerin und bei der Bezirkshauptmannschaft um die Verarbeitung von Daten über »bestimmte Personen«.

Zur Auftraggebereigenschaft meinte die DSK, dass die Beschwerdegegnerin die Entscheidung getroffen hat, in ihrem Gemeindegebiet am festgestellten Ort die dargestellte automatische Geschwindigkeits-

überwachung durchführen zu lassen, und damit als Auftraggeberin iSd § 4 Z 4 DSG 2000 anzusehen ist. Mit der technischen Durchführung hat sie ein privates Unternehmen beauftragt und damit als Dienstleister gemäß § 4 Z 5 DSG 2000 herangezogen.

Die Beschwerdegegnerin gehört als Gebietskörperschaft mit dem Recht auf Selbstverwaltung (vgl. Art. 116 Abs. 1 B-VG) gemäß § 5 Abs. 2 Z 1 DSG 2000 zu den Auftraggebern des öffentlichen Bereichs. Der VwGH führt in seinem Erkenntnis dazu aus, dass daraus noch nicht zwingend gefolgert werden könne, dass die Beschwerdegegnerin in Vollziehung der Gesetze gehandelt habe. Dazu führte die DSK Folgendes aus:

In seinen Erkenntnissen vom 15. Juni 2007, VfSlg 18.146/2007 (»Section Control«), und 9. Dezember 2008, B 1944/07 (»Video-Geschwindigkeits- und Abstandsmessung«) hat der VfGH klar erkennen lassen, dass er verkehrspolizeiliche Überwachungsmaßnahmen zum hoheitlichen Handeln des Staates, nämlich zur Straßenpolizei, zählt, das einer strengen rechtlichen Determinierung bedarf. Diese Sichtweise wird in der seit der 22. StVO-Novelle, BGBl I 16/2009, geltenden Rechtslage insofern noch deutlicher, als im neuen XIII. Abschnitt der StVO 1960 unter der Überschrift »Besondere Vorschriften für die Verkehrsüberwachung mittels bildverarbeitender technischer Einrichtungen« in § 98b ausdrücklich (und nur) die (Bezirksverwaltungs-)Behörden zur punktuellen Radar-Geschwindigkeitsüberwachung ermächtigt werden. Die beschwerdegegenständliche Tätigkeit wird somit vom Gesetz eindeutig als behördliche Tätigkeit qualifiziert.

Würde der Beschwerdegegnerin als Selbstverwaltungskörper und Hoheitsträger zugebilligt werden, dieselben Aufgaben, die nach der Auslegung des VfGH und des Gesetzgebers hoheitlicher Natur sind, auch im Rahmen der Privatwirtschaftsverwaltung ausüben zu können – und damit an andere, weniger strenge, Grundrechtskautelen gebunden zu sein –, würde sie den entsprechenden Bestimmungen der StVO einen im Hinblick auf Art. 18 B-VG verfassungswidrigen Inhalt zumessen. Der Gesetzgeber selbst hat bereits in der im Eingriffszeitpunkt geltenden, hier anzuwendenden Fassung der StVO in § 94c auf diese Frage Bezug genommen, indem er eine durch Hoheitsakt (Verordnung der Landesregierung) vorzunehmende Übertragung behördlicher Befugnisse auf dem Gebiet der Straßenpolizei an Ortsgemeinden vorsieht. Die Bestimmung des § 94c StVO ginge ins Leere, wenn Gemeinden Tätigkeiten der Verkehrsüberwachung bereits aufgrund ihrer Befugnisse als Privatwirtschaftssubjekte entfalten könnten. Dass der Gesetzgeber inhaltsleere Bestimmungen erlassen hätte, kann ihm nicht unterstellt werden.

Eine Ermächtigung zur Vornahme von Verkehrsüberwachung im Rahmen der Privatwirtschaftsverwaltung kann auch nicht aus dem jedermann zustehenden Recht auf Anzeige an die zuständige Behörde abgeleitet werden. Dieses Anzeigerecht (als Zeuge) muss ganz grundsätzlich unterschieden werden von einer Berechtigung zur systematischen und dauernden Überwachung von Menschen mit dem Zweck der Feststellung, ob sie strafrechtswidriges Verhalten setzen werden. Letztere stellt einen tiefgreifenden Eingriff in das Grundrecht auf Datenschutz dar und kann daher, soweit sie zur Verfolgung öffentlicher Interessen erfolgt, in einer demokratischen Gesellschaft schon aus Gründen des Verhältnismäßigkeitsgebots für Grundrechtseingriffe keinesfalls als »Jedermannsrecht« angesehen werden, das ohne weiteres auch von Privaten vorgenommen werden könnte. Das Determinierungsgebot für Grundrechtseingriffe verlangt vielmehr, dass eine solche »Überwachung« mit dem Ziel der Feststellung und Bestrafung von strafrechtswidrigem Verhalten nur unter gesetzlich festgelegten Bedingungen stattfinden darf, die auch jene »angemessene Garantien« vorzusehen haben, die den Grundrechtseingriff verhältnismäßig und erträglich machen. Deshalb ist davon auszugehen, dass die ausdrückliche Regelung des § 98b in der 22. StVO-Novelle als abschließend zu betrachten ist.

Auch wenn man das Vorliegen von Privatwirtschaftsverwaltung bejahen würde, so würde die Interessenabwägung zu keinem

für die Beschwerdegegnerin positiven Ergebnis führen. Dabei müsste § 8 Abs. 4 DSG 2000 als Maßstab dienen (»Daten über verwaltungsbehördlich strafbare Handlungen«), wobei sich die Beschwerdegegnerin mangels einer gesetzlichen Zuständigkeit oder einer besonderen Ermächtigung oder Verpflichtung bei der Datenermittlung nur auf die Z 3 stützen könnte. Die Beschwerdegegnerin zählt nämlich nur als ein Rechtssubjekt, das – ähnlich einem Nachbarn und Straßenanrainer – seine Interessen verfolgt, ohne ein subjektives Recht auf Durchführung einer solchen Überwachung und auf Verfolgung von Verwaltungsübertretungen behaupten zu können. Dem gegenüber steht das subjektiv-öffentliche Recht des Beschwerdeführers, ohne überwiegende berechtigte, dh rechtlich positivierte und geschützte Interessen des Auftraggebers, nicht in seinem Grundrecht auf Geheimhaltung personenbezogener Daten verletzt zu werden. Der Gesetzgeber hat jedoch, nicht zuletzt um unerwünschten Versuchen der Selbsthilfe oder gar der Anmaßung behördlicher Befugnisse hintanzuhalten, dem Einzelnen und damit auch der Ortsgemeinde als Privatrechtssubjekt kein besonders geschütztes Recht verliehen, die Einhaltung straßenpolizeilicher Vorschriften zu kontrollieren. Insbesondere bestehen auch keine »gesetzlichen Sorgfaltspflichten« im Sinne von § 8 Abs. 4 Z 3 DSG 2000, die die Gemeinde zu solchem Vorgehen anleiten oder verpflichten würden, da die StVO die entsprechenden Pflichten eben der allgemeinen Straßenpolizeibehörde – hier der Bezirksverwaltungsbehörde – überträgt.

Das Argument, dass der Grundrechtseingriff ja im öffentlichen Interesse erfolge und schon deshalb ein »überwiegendes berechtigtes Interesse« im Sinne des § 8 Abs. 3 DSG 2000 gegeben sei, das die Vornahme der Datenermittlung rechtfertige, konnte aus folgendem Grund nicht überzeugen: Das Vorliegen eines »überwiegenden berechtigten Interesses« als Rechtsgrundlage einer Datenanwendung setzt voraus, dass der Auftraggeber der Datenanwendung zunächst ein »berechtigtes Interesse« nachweisen kann. Dass ein Privater ein berechtigtes, d. h. von der Rechtsordnung anerkanntes Interesse an der Verfolgung öffentlicher Interessen hätte, kann aber nicht als selbstverständlich angenommen werden. Grundsätzlich ist es die Aufgabe des Staates und seiner Organe, die öffentlichen Interessen mit dem vom Gesetz näher umschriebenen Inhalt und in der vom Gesetz näher determinierten Weise wahrzunehmen – ein Privater müsste eigens nachweisen, dass ihm die Verfolgung öffentlicher Interessen übertragen worden wäre. Eine Übertragung wäre im vorliegenden Zusammenhang nach § 94c StVO durch Hoheitsakt (Verordnung) auch möglich, doch ist sie tatsächlich nicht geschehen, sodass kein »berechtigtes Interesse« an der Vornahme von Handlungen der Verkehrsüberwachung durch die Gemeinde erkannt werden kann, wodurch auch das Vorliegen eines »überwiegenden berechtigten Interesses« an der Vornahme solcher Handlungen ausgeschlossen ist.

Aus § 7 Abs. 2 Z 1 DSG 2000 folgt in einem zweiten Schritt der zwingende Schluss, dass auch die Übermittlung der Daten an die Bezirksverwaltungsbehörde unrechtmäßig erfolgt ist, da diese schon nicht rechtmäßig verarbeitet worden sind. Durch die solcherart unrechtmäßige Datenverwendung hat die Beschwerdegegnerin den Beschwerdeführer in seinem Recht auf Geheimhaltung personenbezogener Daten verletzt. Der Beschwerde war daher im verbleibenden Umfang neuerlich stattzugeben.

Dieser Bescheid wurde beim Verwaltungsgerichtshof angefochten, die Beschwerde aber abgewiesen.

f. Kontodaten im Verfahren vor dem UFS (K121.585/0012-DSK/2010, 30. 7. 2010)

Sachverhalt

Die Beschwerdeführerin behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass sie der Unabhängige Finanzsenat (Beschwerdegegner) (UFS) aufgefordert habe, in einem Verfahren betreffend Anspruch auf Familienbeihilfe (involviert: ihre Mutter und ihr Vater) ihre Bankkonto-Auszüge der letzten drei Jahre (ohne Schwärzungen) als Beweismittel vorzulegen.

Gegenstand des Berufungsverfahrens vor dem UFS sei die auch der Beschwerdeführerin bekannt gegebene Frage, welcher der beiden Elternteile der Beschwerdeführerin zu Unrecht für sie Familienbeihilfe bezogen bzw. wer im betreffenden Zeitraum den überwiegenden Teil der Lebenshaltungskosten der Beschwerdeführerin getragen hatte. Die Beschwerdeführerin wurde dreimal als Zeugin geladen und mit Schreiben des Beschwerdegegners vom Oktober 2009 unter Angaben zum Verfahrensgegenstand (Berufung gegen Abweisung der Anträge auf Familienbeilhilfe und Rückforderung ausgezahlter Beträge, Verwendung von erhaltenen Unterhaltszahlungen des Vaters) aufgefordert, Bankunterlagen eines bestimmten Zeitraums als Beweismittel vorzulegen. Sie ist dieser Aufforderung sowie den Zeugenladungen jedoch nicht nachgekommen.

Rechtliche Würdigung

Die DSK hielt zunächst fest, dass der Beschwerdegegner in Familienbeihilfeangelegenheiten zur amtswegigen Feststellung des für die Zuerkennung eines Anspruches auf Familienbeihilfe maßgebenden Sachverhaltes verpflichtet ist (§ 2 lit a Z 1, § 25 Abs. 1 Z 2, § 91 Abs. 1 bis 3, § 114 Abs. 1, § 143 Abs. 1, § 169, § 171 und § 172 Abs. 1 BAO; § 2, § 2a Familienlastenausgleichsgesetz 1967). Zu diesem Zwecke kann der Beschwerdegegner auch die Beschwerdeführerin als offensichtlichen Anknüpfungspunkt für den Anspruch auf Familienbeihilfe ihres Vaters oder ihrer Mutter als Zeugin laden und von ihr alle Unterlagen verlangen, die erforderlich sind, um feststellen zu können, ob die Voraussetzungen für die Gewährung von Familienbeihilfe gegeben sind. Der Beschwerdegegner als zuständige Behörde konnte sich daher bei dem Versuch, die verfahrensrelevanten Daten (Kontoumsätze der Beschwerdeführerin) für die im Sachverhalt genannte strittige Frage des Verfahrens zu ermitteln, zu Recht auf die genannten Vorschriften berufen. Das Schreiben des Beschwerdegegners vom Oktober 2009 enthielt auch die notwendigen Angaben, die eine Zeugin bzw Besitzerin von verfahrensrelevanten Unterlagen in die Lage versetzen, den Zweck und Gegenstand der mit ihrer Unterstützung vorzunehmenden Beweisaufnahme zu erfassen. Eine »explizite« oder ausführliche Begründung für die Notwendigkeit dieser Beweisaufnahme muss entgegen der Ansicht der Beschwerdeführerin von der amtswegig vorgehenden Behörde hingegen nicht gegeben werden, nicht zuletzt, weil dies auf eine antizipative Würdigung des noch ausstehenden Beweises hinauslaufen könnte.

Darüber hinaus steht fest, dass es tatsächlich noch zu keiner Datenweitergabe gekommen war, da die Beschwerdeführerin die von ihr gewünschten Unterlagen nicht übermittelt hat und ihr gegenüber auch keine Zwangsmaßnahmen ergriffen worden sind. Die Nichtübermittlung soll vielmehr im Rahmen der Beweiswürdigung berücksichtigt werden. Bei dieser Sachlage handelt es sich also bloß um den Versuch einer Datenermittlung durch den Beschwerdegegner. Ob dies schon eine Datenschutzverletzung war, konnte angesichts obiger Ausführungen aber dahingestellt bleiben.

g. Daten in der sicherheitsbehördlichen Aktenverwaltung: Herkunft unbekannt (K121.626/0016-DSK/2010, 24. 9. 2010)

Sachverhalt

Der Beschwerdeführer behauptet in seiner Beschwerde eine Verletzung im Recht auf Auskunft, Löschung und Richtigstellung durch die Bundespolizeidirektion Wien. Betreffend den Beschwerdeführer ist verfahrensgegenständlich ein kriminalpolizeiliches Ermittlungsverfahren aktenkundig. Dieses Verfahren wegen Verdachts des Diebstahls (§ 127 StGB; Tatzeitpunkt August 2009) wurde gemäß § 190 Z 2 StPO mit Einstellung durch die Staatsanwaltschaft Wien im Oktober 2009 beendet. Es hat sich herausgestellt, dass der Anzeiger nicht den Beschwerdeführer (Vorname: »H***«) beschuldigt hat, sondern einen »T***« desselben Nachnamens wie der Beschwerdeführer.

Dementsprechend findet sich zur erwähnten GZ eine Eintragung in der Datenanwendung »Allgemeine Protokolle der Bundespolizeidirektion Wien« (im

Folgenden nach der technischen Systembezeichnung kurz: »PAD«). Das elektronische System »PAD« ist ein Aktenprotokollierungssystem (Aktenindex), das in der neueren Version »PAD 2.0« zusätzlich mit einem elektronischen Aktenbearbeitungs- und Aktenaufbewahrungssystem verbunden ist. Der nunmehr bei der Beschwerdegegnerin zum Einsatz kommende »PAD 2.0« besteht somit aus einem »formalen« Teil, der die »äußeren« Verfahrensdaten der Geschäftsfallbehandlung (Identitäts-, Adress- und Kontaktdaten von Betroffenen sowie Daten zum Verfahrensgegenstand, wie Sachverhalt [»Kurzsachverhalt«], Rolle der Betroffenen, Tatverdacht, befasste Behörden und allenfalls Verfahrensausgang) enthält und einem »inhaltlichen« Teil in Form von Aktentextdokumenten. Dieser inhaltliche Teil hat im konkreten Fall einige Dokumente wie Amtsvermerke, Personalblatt, Ladungen, EKIS-Webanfrage und Strafregisterauskunft enthalten.

Neben der PAD-Dokumentation besteht auch ein behördenüblicher Kopienakt (Papierakt) zur Dokumentation des Ermittlungsverfahrens.

Der PAD war zum Tatzeitpunkt überdies mit folgender Funktion ausgestattet: Beim erstmaligen Anlegen eines Aktes sind auch die Stammdaten der Personen, auf welche sich sein Aktenvorgang beziehen wird, einzugeben. Über Eingabe allein des Familiennamens im entsprechenden Feld wurden alle Personen dieses Familiennamens, die bereits zu einem früheren Zeitpunkt im PAD gespeichert wurden, in einer Liste dargestellt, worauf die gemeinte Person anhand des Vornamens ausgewählt werden kann. Daraufhin werden die Stammdaten der Person angezeigt. In der nunmehr aktuellen Version des PAD, die seit 1. Dezember 2009 im Einsatz ist, werden allenfalls passende bereits vorhandene Personendaten zur Auswahl angeboten, wenn die Pflichtfelder Familienname und Vorname sowie entweder Geschlecht oder genaues Geburtsdatum befüllt werden. Auch in der aktuellen Version werden lediglich die Stammdaten, nicht aber allfällige frühere Verfahrensdaten und Akteninhalte angezeigt.

Die Stammdaten des Beschwerdeführers müssen auch schon vor August 2009 (Zeitpunkt der Erstellung des oben genannten Aktes) im PAD vorhanden gewesen sein.

Dem Auskunfts- und Löschungsbegehren des Beschwerdeführers vom September 2009, dem zum Identitätsnachweis die Kopie seines Reisepasses angeschlossen war, kam die Beschwerdegegnerin im Hinblick auf die Auskunft insofern nach, als sie ihm aus dem Kriminalpolizeilichen Aktenindex (KPA) eine Negativauskunft erteilte, hinsichtlich des PAD die Vormerkung betreffend des Vorfalls aus August 2009 bekanntgab. Im Hinblick auf die Löschung wurde dem Begehren des Beschwerdeführers nicht Rechnung getragen, weil zunächst die Löschungssperre (§ 26 Abs. 7 DSG 2000) und nach Ablauf dieser Sperrfrist die Verarbeitung der Daten im PAD auf Grundlage des § 13 SPG für den Verarbeitungszweck der Aktenverwaltung zur Wiederauffindung der Aktenkopie und der Dokumentation behördlichen Handelns der Löschung entgegen stünde.

Mit Schreiben aus Mai 2010 ergänzte die Beschwerdegegnerin ihre Auskunft im Zuge des Verfahrens vor der DSK wie folgt: »Bedauerlicherweise wurden dem Antwortschreiben der Bundespolizeidirektion Wien vom *** offensichtlich auf Grund eines Kanzleigebrechens, die in den allgemeinen Protokollen der Bundespolizeidirektion Wien (automationsunterstützt) »PAD« elektronisch archivierten Dokumente nicht beigeschlossen. Die zum Zeitpunkt der Auskunftserteilung im PAD verfügbaren Dokumente werden nunmehr zur Komplettierung der Auskunft nachträglich zur Kenntnis gebracht.« Diesem Schreiben waren mehrere Dokumente aus dem »inhaltlichen« Teil des PAD angeschlossen.

Mit Schreiben aus Juni 2010 teilte die Beschwerdegegnerin dem Beschwerdeführer im Hinblick auf sein Löschungsbegehren mit: »Bezugnehmend auf Ihren Antrag, in dem Sie unter anderem ausdrücklich die Löschung Ihrer personenbezogenen Daten aus dem PAD-Akt *** begehren, teilt die Bundespolizeidirektion Wien mit, dass Ihrem Antrag auf Grundlage der § 26 Abs.

7 i.V.m. § 27 Abs. 1 Z 2 DSG 2000 insoweit entsprochen wurde, als die Löschung der Daten im Protokollteil des PAD (Personendaten und Rolle als Beschuldigter) am **.2010 durchgeführt und gleichzeitig beim entsprechenden Protokolleintrag nachstehender Hinweis angebracht wurde: »Irrtümlich als Beschuldigtendaten erfasste personenbezogenen Daten eines Unbeteiligten aus datenschutzrechtlichen Gründen am **.2010 gelöscht.« Durch das durch Löschung Ihrer Daten im Protokollteil des PAD erfolgte Lösen des Personenbezuges zu Ihrer Person sind die im Aktenverwaltungsteil unstrukturiert enthaltenen Ihre Person betreffenden Daten im Wege einer personenbezogenen Anfrage nicht mehr auffindbar. Eine Veränderung der im Aktenverwaltungsteil des PAD vorhandenen Dokumente durch Löschen der Ihre Person betreffenden Daten ist aus Sicht der BPD Wien wegen des Dokumentationszweckes nicht zulässig, da die Dokumente in der vorliegenden Form der Justiz vorgelegt wurden.

Rechtliche Würdigung

Zur behaupteten Verletzung im Recht auf Auskunft:

Die Beschwerdegegnerin hat auf das entsprechende Begehren des Beschwerdeführers vom September 2009 im September 2009 und im Mai 2010 Auskunft erteilt. Soweit das zweite Auskunftsschreiben nach Ablauf der achtwöchigen Frist des § 26 Abs. 4 DSG 2000 ergangen ist, führte die DSK aus, dass eine »Sanierung« einer ursprünglich nicht (bzw. nicht vollständig) erbrachten, zwar nach Beschwerdeerhebung, aber noch vor Bescheiderlassung erteilten Auskunft sowohl von ihr in ständiger Spruchpraxis anerkannt (z. B. Bescheid vom 18. September 2009, GZ K121.537/0013-DSK/2009, mwH) als auch nunmehr vom Gesetzgeber so vorgesehen ist (vgl. § 31 Abs. 8 erster Satz DSG 2000 idF der DSG-Novelle 2010). Des weiteren ist zu beachten, dass sowohl die DSK in ständiger Rechtssprechung (vgl. für viele den Bescheid vom 14. Februar 2007, GZ K121.240/0002-DSK/2007) wie auch die Gerichtshöfe des öffentlichen Rechts vertreten, dass sich das Auskunftsrecht nach dem DSG 2000 nicht auf Papierakten erstreckt (§ 1 Abs. 3 Z 1 iVm § 26 DSG 2000). Soweit also die Beschwerdegegnerin personenbezogene Daten des Beschwerdeführers in Papierakten verarbeitet, ist ein Auskunftsanspruch zu verneinen.

Die DSK erachtete die Auskunft auch soweit als vollständig, als dem Beschwerdeführer seine Daten sowohl aus dem Protokollteil als auch dem Aktenverwaltungsteil des PAD zum Akt GZ *** bekannt gegeben wurden. Die Daten zu jenem Vorfall allerdings, demzufolge die Stammdaten des Beschwerdeführers – wie festgestellt – im PAD bereits vor Anlegen des genannten Aktes vorhanden waren bzw die Herkunft dieser Daten hat die Beschwerdegegnerin nicht beauskunftet und den Beschwerdeführer daher insoweit in seinem Recht auf Auskunft verletzt.

Zur behaupteten Verletzung im Recht auf Löschung:

Im Schreiben vom September 2009 beantragte der Beschwerdeführer auch, gestützt auf § 27 DSG 2000, sämtliche personenbezogenen Daten zu seiner Person »im Zusammenhang mit dem Verfahren *** unverzüglich zu löschen«. Zwar nach Ablauf der achtwöchigen Frist des § 27 Abs. 4 DSG 2000, jedoch noch im laufenden Verfahren vor der DSK löschte die Beschwerdegegnerin sämtliche Daten des Beschwerdeführers im Protokollteil des PAD (Hinweis beim Protokolleintrag: »SVM; Irrtümlich als Beschuldigtendaten erfasste personenbezogene Daten eines Unbeteiligten aus datenschutzrechtlichen Gründen am **.2010 gelöscht.«), verweigerte jedoch weiterhin die Löschung »unstrukturiert enthaltenen« Daten des Beschwerdeführers im Aktenverwaltungsteil des PAD mit Hinweis auf den Dokumentationszweck.

Soweit die Daten des Beschwerdeführers aus dem Protokollteil des PAD (mit Anmerkung) gelöscht wurden, war seine Beschwerde nunmehr mangels Beschwer nicht mehr gerechtfertigt. Hinsichtlich der im Aktenverwaltungsteil nach wie vor (in unstrukturierten Dokumenten) enthaltenen Daten des Beschwerdeführers gilt Folgen-

des: In ihrem Bescheid vom 20. März 2009, GZ K121.453/0003-DSK/2009, hat die DSK bereits ausführlich dargelegt, warum sie eine Aufbewahrung von (elektronisch gespeicherten) Akten auch nach Verfahrensbeendigung für gerechtfertigt hielt. Diese Erwägungen waren sowohl betreffend die »äußeren« Verfahrensdaten (Protokollteil) als auch für die im PAD enthaltenen elektronischen Textdokumente (Aktenverwaltungsteil) anzuwenden.

Im gegenständlichen Fall stellt sich die Situation aber anders dar: Der PAD ist als internes Aktenverwaltungssystem auf Basis der Rechtsgrundlage des § 13 SPG grundsätzlich zulässig, wobei aber gemäß § 13 Abs. 2 SPG (u. a.) die Auswählbarkeit von Daten aus der Gesamtmenge der gespeicherten Daten nur nach dem Namen nicht vorgesehen sein darf, vielmehr ist ein auf den protokollierten Sachverhalt bezogenes weiteres Datum anzugeben. Eine Funktion des PAD, die allein aufgrund der Eingabe des Familiennamens oder auch nur der Eingabe des Vor- und Familiennamens zzgl. des Geschlechts oder des Geburtsdatums die Zugänglichkeit von Daten aus dem PAD ermöglicht, ist mit § 13 Abs. 2 SPG nicht vereinbar. So betrachtet haben die Daten des Beschwerdeführers in den PAD nur deshalb Eingang gefunden, weil der PAD über eine nicht mit der gesetzlichen Grundlage vereinbare Funktion verfügt und anders – weil der Beschwerdeführer einen anderen Vornamen als der eigentliche Beschuldigte hat – niemals Eingang gefunden hätten.

Die Beschwerdegegnerin wendet sich gegen die Löschung der unstrittig nur aufgrund eines Irrtums ermittelten und verarbeiteten Daten mit dem Argument, dass die Daten für Dokumentationszwecke weiter benötigt würden. Dies vermag hier schon deshalb nicht zu überzeugen, als der Papierakt weiter besteht und in diesem der Vorgang dokumentiert ist. Die Löschungsverpflichtung betrifft also sowohl den Protokollteil wie auch den Aktenverwaltungsteil des PAD, soweit er sich auf den Beschwerdeführer bezieht. Ob die Daten darüber hinaus iSd § 63 Abs. 1 SPG unrichtig in Bezug auf den Dokumentationszweck waren, konnte die DSK dahingestellt lassen. Jedenfalls dadurch, dass die Beschwerdegegnerin dem Löschungsbegehren des Beschwerdeführers vom September 2009 nicht (vollständig) gefolgt ist, hat sie diesen in seinem Recht auf Löschung verletzt.

h. Post als Zusteller von Zahlungen des AMS (K121.638/0006-DSK/2010, 22. 10. 2010)

Sachverhalt

Der Beschwerdeführer behauptete eine Verletzung im Recht auf Geheimhaltung dadurch, dass eine Benachrichtigung der Post u. a.. Namen, Titel, Adresse, den Auftraggeber des Zahlungsbetrages (hier: ein Arbeitsmarktservice (AMS)) und damit den Zahlungsgrund und die Sozialversicherungsnummer, aus welcher das Geburtsdatum klar ersichtlich sei, enthalte. Damit würde die Post gegen das DSG 2000 verstoßen und zum Nachteil des Beschwerdeführers wesentliche personenbezogene Daten veröffentlichen.

Es wurde daher die Österreichische Post AG als Antragsgegner bezeichnet und der Antrag gestellt, die DSK möge den Rechtsträger zur Unterlassung dieser Vorgangsweise mit sofortiger Wirkung wegen Gefahr im Verzug verurteilen und den Anspruch auf Schadensersatz bestätigen, allenfalls bestimmen.

Die DSK hielt dem Beschwerdeführer vor, dass die Österreichische Post AG bei der Zustellung behördlicher Schriftstücke oder gesetzlich geregelter Geldbeträge als Dienstleister des Absenders tätig werde. Im konkreten Fall wäre daher das AMS als Auftraggeber, die Post AG jedoch lediglich als Dienstleister anzusehen. Da die auf dem Grundrecht auf Datenschutz gemäß § 1 DSG 2000 beruhenden Geheimhaltungspflichten betreffend personenbezogene Daten den Auftraggeber treffen und etwaige Verletzungen im Recht auf Geheimhaltung demzufolge nur dem Auftraggeber, nicht aber dem Dienstleister angelastet werden könnten, wäre die Beschwerde gegen die Post AG verfehlt und allenfalls Beschwerde gegen das AMS zu führen.

Der Beschwerdeführer hielt dennoch mit dem Argument, für das Ausfüllen der Formulare sei wohl die Post AG selbst ausschließlich verantwortlich, an dieser als Beschwerdegegnerin fest.

Rechtliche Würdigung

Die DSK zitierte eingangs den VfGH. Dieser hat in seinem Erkenntnis vom 6. März 2000, B 377/98, festgehalten, dass die Verwendung von rosa Abholscheinen zur Benachrichtigung vom Zurverfügungstehen des Arbeitslosengeldes beim Postamt entsprechend § 51 Abs. 2 AlVG durch Mitwirkung der Post an der Auszahlung des Arbeitslosengeldes erfolge und hoheitlicher Natur sei. Er führte dazu aus, dass »*der Anspruch auf Arbeitslosengeld – wie sich aus § 47 Abs. 1 AlVG ergibt – wonach dann, wenn der Anspruch nicht anerkannt wird, dem Antragsteller darüber ein Bescheid der zuständigen regionalen Geschäftsstelle des Arbeitsmarktservices auszufolgen ist – hoheitlicher Natur [ist].*« Darüber hinaus sei auch die Auszahlung des im Einzelfall gebührenden Arbeitslosengeldes gesetzlich näher geregelt: »*Die Auszahlung hat gemäß § 51 Abs. 2 AlVG über die Österreichische Postsparkassen Aktiengesellschaft zu erfolgen, die sich dabei gemäß § 2 Abs. 1 des Postsparkassengesetzes 1969 der PTA bedient*«. Im Hinblick darauf ging der VfGH davon aus, dass »*das Handeln sowohl der in Betracht kommenden Organe der Österreichischen Postsparkasse Aktiengesellschaft als auch der PTA nicht diesen Rechtsträgern des Privatrechtes, sondern durch die jeweils zuständige regionale Geschäftsstelle des Arbeitsmarktservice dem Bund zuzurechnen ist und die genannten Organe […] dabei auch den Weisungen dieser Behörde unterliegen.*«

Auch im vorliegenden Fall bezog sich die vom Beschwerdeführer behauptete Verletzung im Recht auf Geheimhaltung auf die Benachrichtigung der Post über die Abholbarkeit des Arbeitslosengeldes beim Postamt. Im Hinblick auf die Qualifikation dieser Handlung durch den VfGH als hoheitlich und gegenüber dem AMS weisungsabhängig, ist das AMS als datenschutzrechtlicher Auftraggeber und die Post AG lediglich als deren Dienstleister anzusehen.

Weil der Beschwerdeführer dennoch seine Beschwerde ausdrücklich gegen die Post AG gerichtet hat, war sie schon (auch wegen behaupteter Gefahr im Verzug) aus dem Grund, dass im gegebenen Zusammenhang ein etwaiges datenschutzrechtliches Fehlverhalten dieser nicht zugerechnet werden kann, als unbegründet abzuweisen. Der Beschwerdeführer hat auch selbst auf jene höchstgerichtliche Judikatur hingewiesen, wonach die Zustellung und Ausbezahlung von Arbeitslosengeld grundsätzlich eine hoheitliche Aufgabe ist. Er führt aber darüber hinausgehend aus, dass seiner Ansicht nach die Post AG die Benachrichtigungsformulare eigenverantwortlich ausfülle. Selbst wenn aber das Verhalten des Zustellers im konkreten Fall der Post AG zurechenbar wäre, so wäre die DSK nicht zuständig, weil die Post AG für das Erbringen von Postdiensten datenschutzrechtlich dem privaten Bereich zugeordnet wird (§ 1 Abs. 5 DSG 2000 und § 18 PostG). Bei Rechtsverletzungen durch Auftraggeber des privaten Bereichs wären (mit Ausnahme des Rechts auf Auskunft) zur rechtsförmlichen Entscheidung die Zivilgerichte berufen (§ 32 Abs. 1 DSG 2000), sodass in diesem Fall eine Zurückweisung der Beschwerde erfolgen müsste.

Soweit der Beschwerdeführer darüber hinaus auch beantragt, die DSK möge einen Anspruch auf Schadenersatz bestätigen, allenfalls bestimmen, so sind Ansprüche im Zusammenhang mit Schadenersatz gemäß § 33 DSG 2000 stets vor den Zivilgerichten geltend zu machen. Insoweit war die Beschwerde daher zurückzuweisen.

i. Tätigkeit eines Gerichtskommissärs (K121.634/0008-DSK/2010, 3. 12. 2010)

Sachverhalt

Die Beschwerdeführer behaupten eine Verletzung im Recht auf Geheimhaltung dadurch, dass der Beschwerdegegner (ein öffentlicher Notar) ausdrücklich »als Gerichtskommissär« in einer bestimmten Verlassenschaftssache eine »Ladung zur Errichtung der Todesfallaufnahme« an ihre

Adresse mit der Adressatenbezeichnung »An die Angehörigen der verstorbenen XY« zustellen habe lassen. Damit habe er »den sensiblen Inhalt des Schreibens bereits in der Briefanschrift verlautbart«. Die Zuständigkeit der DSK gründe sich darauf, dass der Beschwerdegegner bei dieser Zustellung in Vollziehung der Gesetze tätig gewesen sei.

Rechtliche Würdigung:

Die DSK sah sich zur Entscheidung über diese Beschwerde als unzuständig, da sich aus den Bestimmungen des § 105 JN iVm § 145 Abs. 1 AußStrG ergibt, dass die Verlassenschaftsabhandlung einschließlich der ausdrücklich geregelten Todesfallaufnahme zu den gerichtlichen Geschäften und damit zu den »Akten der Gerichtsbarkeit« gemäß § 1 Abs. 5 DSG 2000 gehört.

Aus dem Langtitel des Gerichtskommissärsgesetzes »Bundesgesetz vom 11. November 1970 über die Tätigkeit der Notare als Beauftragte des Gerichtes im Verfahren außer Streitsachen (Gerichtskommissärsgesetz – GKG)« ergibt sich, dass das Gericht in den in diesem Gesetz geregelten Fällen durch Notare als seine Beauftragten, eben »Gerichtskommissäre« tätig wird.

Der Beschwerdegegner als Notar war daher u. a. bei der in § 1 Abs. 1 Z 1 lit a) GKG ausdrücklich aufgezählten und ausdrücklich als »Amtshandlung« bezeichneten Todesfallaufnahme Organ des betreffenden Bezirksgerichts und damit »Organ im Dienste der … Gerichtsbarkeit« gemäß § 31 Abs. 2 DSG 2000. Nicht zuletzt aus der durch BGBl I Nr 133/2009 eingefügten Wortfolge »im Dienste« ergibt sich, dass der Gesetzgeber nicht nur berufsmäßige oder sonst auf längere Dauer bestellte Organe, sondern auch fallweise beauftragte und wie hier mit gerichtlicher Amtsgewalt beliehene Personen in den Geltungsbereich der Bestimmung einbeziehen wollte.

Die Beschwerde wurde daher zurückgewiesen.

j. Einholung einer behördlichen Meldeauskunft für Zwecke der Zustellung eines Kündigungsschreibens (K121.667/0012-DSK/2011, 18. 5. 2011)

Sachverhalt

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass der Beschwerdegegner (Magistrat) im Juni 2009 durch Missbrauch seiner Befugnisse als »Meldebehörde« seine vollständigen, damit auch historischen, Meldedaten ermittelt und anschließend dazu benutzt habe, fehlerhafte Zustellungen an nicht mehr aktuellen Adressen vorzunehmen. Er befinde sich mit dem Beschwerdegegner wegen einer widerrechtlichen Kündigung in einem Rechtsstreit.

Im Juni 2009 veranlasste der Beschwerdegegner die Zustellung der Kündigung des Dienstverhältnisses des Beschwerdeführers an seinen beiden bekannten Adressen. Beide Schreiben wurden von der Post mit dem Vermerk »ortsabwesend« an den Absender retourniert, worauf im Juni 2009 eine Abfrage des ZMR gemäß § 16a MeldeG veranlasst wurde, die den Gesamtdatensatz und damit auch historische Meldedaten (Wechsel von Haupt- und Nebenwohnsitz) umfasste, jedoch keine weiteren Abgabestellen (Meldeadressen) ergab. Darauf wurde die neuerliche, diesmal wirksame Zustellung an den bekannten Abgabestellen veranlasst.

Rechtliche Würdigung:

Aus § 16a Abs. 2 und 10 MeldeG ergibt sich, dass die Gesamtheit der aktuellen und historischen, für jeweils 30 Jahre gespeicherten Meldedaten den Gesamtdatensatz eines Menschen im ZMR bildet. Bei einer Abfrage dieser Daten durch den Magistrat, der sowohl Geschäftsapparat der Meldebehörde (Bürgermeister) als auch gemäß §§ 65 und 66 Abs. 1 Wr VBO 1995 Personalverwaltung der Stadt als Gebietskörperschaft ist, für Zwecke der Personalverwaltung, liegt eine Übermittlung durch Zweckänderung vor (§ 4 Z 12 dritter Halbsatz DSG 2000). Gemäß § 16a Abs. 4 MeldeG darf dieser Gesamtdatensatz von Organen einer Gebietskörperschaft ermittelt werden, »soweit dies zur Besorgung einer gesetzlich übertragenen Aufgabe erforderlich ist«.

Der gesetzlich festgelegte Verwendungszweck des Gesamtdatensatzes ist damit keineswegs auf hoheitliche Aufgaben, also die Vollziehung von Gesetzen im engeren

Sinne, beschränkt. Das Gesetz spricht von gesetzlich übertragenen Aufgaben, was die Besorgung von Aufgaben der Stadt als Trägerin von Privatrechten nicht ausschließt, sofern diese in einem Mindestumfang gesetzlich determiniert sind. § 16a Abs. 4 MeldeG eröffnet die Möglichkeit, Organen von Gebietskörperschaften, Gemeindeverbänden und Sozialversicherungsträgern eine Online-Abfrageberechtigung auf die Daten des ZMR einzuräumen und zwar dann, wenn sie diese Daten zur Besorgung einer gesetzlich übertragenen Aufgabe (Hoheits- und Privatwirtschaftsverwaltung) benötigen (Grosinger-Szirba, Das österreichische Melderecht6 [2002] 145). Diese Entscheidung des historischen Gesetzgebers ergibt sich aus den Materialien (AB, 501 BlgNR XXI. GP, Seite 2). Der mit Vorbereitung des Gesetzesbeschlusses befasste Ausschuss führt dazu wörtlich zur Begründung des Gesetzestextes aus: »*Die Beschränkung der Einräumung eines Online-Zugriffes für Organe der Gebietskörperschaften, der Gemeindeverbände und Sozialversicherungsträger auf die Besorgung der Aufgaben der Hoheitsverwaltung berücksichtigt in zu geringem Ausmaß, dass insbesondere den Gemeinden durch Gesetz Aufgaben übertragen wurden, die im Rahmen der Privatwirtschaftsverwaltung zu besorgen sind.*« Die zitierte Bestimmung entspricht damit sinngemäß § 8 Abs. 3 Z 1 DSG 2000.

Die Gründe für eine Beendigung eines Dienstvertrages durch Kündigung sind in den … geregelt, die entsprechenden Aufgaben sind durch … dem Magistrat übertragen. Bei der Verwaltung privatrechtlicher Dienstverhältnisse handelt es sich daher um eine dem Magistrat gesetzlich übertragene Aufgabe.

Aus dem festgestellten Sachverhalt wiederum ergibt sich, dass wegen eines Zustellanstandes bei der Zustellung eines Kündigungsschreibens auch ein konkreter Bedarf für die Prüfung des Gesamtdatensatzes auf Daten zu weiteren in Frage kommenden Abgabestellen gegeben war. Wie an dieser Stelle nochmals zu betonen ist, wurden bei dieser Gelegenheit ohnedies keine Daten (zu postalischen Abgabestellen) übermittelt, die dem Beschwerdegegner nicht bereits bekannt waren. Es lagen daher Gründe gemäß § 7 Abs. 1, Abs. 2 Z 1 und Abs. 3 DSG 2000 iVm § 16a Abs. 4 MeldeG vor, den melderechtlichen Gesamtdatensatz des Beschwerdeführers zu ermitteln bzw. diese Daten zu übermitteln. Die Beschwerde war daher als unbegründet abzuweisen.

k. Gemeinde und Krankenfürsorgeanstalt sind zu trennen (K121.678/0009-DSK/2011, 18. 5. 2011)

Sachverhalt

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung durch drei Fakten, die sämtliche seinen (verlängerten) Krankenstand und eine mögliche Ruhestandsversetzung betreffen:

I. Gemäß einem Aktenvermerk habe die Personalamtschefin der Erstbeschwerdegegnerin (Gemeinde) beim Chefarzt der Zweitbeschwerdegegnerin (Krankenfürsorgeanstalt) telefonisch Daten zum Gesundheitszustand des Beschwerdeführers ermittelt.
II. Dieselbe Personalamtschefin habe in einer E-Mail an den Stadtamtsdirektor angefragt, ob mit der Zweitbeschwerdegegnerin Kontakt aufgenommen werden solle, um einen möglichst raschen Rehabilitationsaufenthalt des Beschwerdeführers zu arrangieren; auch hier sei die dem Krankenstand zugrunde liegende Diagnose erwähnt worden, die nur von der Zweitbeschwerdegegnerin stammen könne.
III. Der sozialversicherungsrechtliche Antrag auf Genehmigung eines Kur- und Rehabilitationsaufenthalts sei an die Erstbeschwerdegegnerin (wiederum das Personalamt) übermittelt worden.

Der Beschwerdeführer steht als Beamter in einem öffentlich-rechtlichen Dienstverhältnis zur Erstbeschwerdegegnerin, ein Verfahren zur Ruhestandsversetzung ist seit Jahren anhängig. Er befand sich in einem längeren Krankenstand und unterzog sich währenddessen mehreren Untersuchungen und

einem gefäßchirurgischen Eingriff. Noch im Krankenhaus stellte der Beschwerdeführer einen Antrag auf Genehmigung eines Rehabilitationsaufenthalts an den für ihn zuständigen Sozialversicherungsträger, die Zweitbeschwerdegegnerin. Dieser Antrag war mit einer befürwortenden ärztlichen Stellungnahme des Krankenhauses mit Diagnose und Befunden versehen. Er enthielt Gesundheitsdaten des Beschwerdeführers wie Angaben zur gesundheitlichen Vorgeschichte, die antragsrelevante Diagnose, die aktuelle Medikation sowie die vorgeschlagene Rehabilitationseinrichtung.

Dieser Antrag langte im Jänner 2008 bei der Zweitbeschwerdegegnerin ein und wurde einige Tage später durch Fertigung der Genehmigung auf dem Antragsformular bewilligt.

Zu Faktum I. wurde festgestellt, dass der handschriftliche Aktenvermerk der Leiterin der Personalabteilung der Erstbeschwerdegegnerin nur so erklärt werden kann, dass sie sich telefonisch beim ärztlichen Sachverständigen (Chefarzt der Zweitbeschwerdegegnerin) erkundigte, was unter einem bestimmten ärztlichen Sprachgebrauch zu verstehen sei, und dieser die im Aktenvermerk wiedergegebene Vermutung (»angebl.«) geäußert hat.

Zu Faktum II. wurde festgestellt, dass sich aus dem Aktenvermerk der Leiterin der Personalabteilung der Erstbeschwerdegegnerin ergebe, dass sich der Beschwerdeführer in einem Telefonat selbst über seinen bevorstehenden Rehabilitationsaufenthalt informiert hat.

Zu Faktum III wurde festgestellt, dass die Zweitbeschwerdegegnerin der Erstbeschwerdegegnerin zu einem nicht näher bekannten Zeitpunkt im Jänner 2008 eine Kopie des Antrags auf Genehmigung eines Rehabilitationsaufenthalts des Beschwerdeführers (noch ohne Genehmigungsvermerk) übermittelte.

Rechtliche Würdigung

Aus datenschutzrechtlicher Sicht besteht kein rechtlich zwingender Grund, dass Mitarbeiter der Erstbeschwerdegegnerin nicht auch für die Zweitbeschwerdegegnerin tätig sein können, obwohl dies natürlich bedeutet, dass das Wissen um bestimmte, der Geheimhaltung unterliegende Tatsachen (bzw. Daten) im Gedächtnis der handelnden Personen auch bei Tätigkeit für den jeweils anderen Auftraggeber präsent bleibt.

Hinsichtlich der Fakten I. und II. war die Beschwerde nicht berechtigt. Der festgestellte Sachverhalt zu Faktum I. ergibt, dass die Leiterin der Personalabteilung der Erstbeschwerdegegnerin auf Grundlage einer vorliegenden ärztlichen Bescheinigung einen medizinischen Sachverständigen um Erläuterung eines Fachausdrucks gebeten, dabei dessen Vermutung zur Behandlung des Beschwerdeführers erfahren und diese in einem Aktenvermerk festgehalten hat. Faktum II. wiederum beruht auf der Tatsache, dass dieselbe Beamtin der Erstbeschwerdegegnerin eine ihr mündlich von einem Beamten der Gemeinde weitergeleitete verlängerte Krankenstandsmeldung des Beschwerdeführers entgegengenommen und aktenkundig gemacht hat, in der dieser offenbar selbst einen beantragten Rehabilitationsaufenthalt erwähnt hat. Gemäß § 35 Abs. 1 NÖ GBDO ist der Dienstgeber berechtigt, den Grund einer Dienstverhinderung zu erfahren. Aus § 34 NÖ GBDO ist wiederum der Schluss zulässig, dass die Dienstbehörde berechtigt und verpflichtet ist, den Grund einer Dienstverhinderung und die körperliche wie geistige Eignung zur Dienstverrichtung zu ermitteln, d. h. ein entsprechendes Ermittlungsverfahren einzuleiten und Sachverständigengutachten einzuholen. Somit besteht kein grundsätzliches Verbot für die Erstbeschwerdegegnerin, gesundheitsbezogene Daten des Beschwerdeführers für dienstrechtliche Zwecke zu ermitteln (vgl. auch § 9 Z 11 DSG 2000).

Hinsichtlich des Faktums III. und der Zweitbeschwerdegegnerin war die Beschwerde berechtigt. Die Zweitbeschwerdegegnerin ist verpflichtet, den Geheimhaltungsanspruch der Betroffenen, im Wesentlichen also der bei ihr krankenversicherten Personen, auch und gerade gegenüber der Erstbeschwerdegegnerin zu wahren. Die wirtschaftlich vorteilhafte »Personalunion« von Organen der Gemeinde und der Kran-

kenfürsorge verpflichtet letztere etwa im Hinblick auf die gemäß § 14 DSG 2000 gebotenen Datensicherheitsmaßnahmen zu einer Abgrenzung zwischen Krankenfürsorge- und Gemeindeangelegenheiten bei der Verwendung gesundheitsbezogener Daten. Für Verletzungen des Geheimhaltungsschutzes trifft sie daher im gegebenen Zusammenhang die Verantwortung.

Die Problematik des Eingriffs liegt hier nicht darin, dass die Erstbeschwerdegegnerin als Dienstgeberin des Beschwerdeführers von dessen vorgesehenem Rehabilitationsaufenthalt erfuhr, sondern dass ihr die im Antrag enthaltene medizinische Diagnose, demnach sensible Daten, übermittelt worden sind. Eine Berechtigung zur Übermittlung dieser Daten für die Zweitbeschwerdegegnerin in zumindest sinngemäßer Anwendung des § 9 DSG 2000 war nicht ersichtlich.

Da die Erstbeschwerdegegnerin grundsätzlich berechtigt war, Gesundheitsdaten des Beschwerdeführers zu ermitteln, soweit es für das Dienstverhältnis gesetzlich vorgesehen bzw. von Belang ist, fällt ihr dagegen keine Verletzung im Recht auf Geheimhaltung (»Ermittlungsschutz«) zur Last. Freilich wäre sie aber gehalten gewesen, die ihr unberechtigt ohne ihr Zutun übermittelten Daten unverzüglich zu löschen, sobald ihr die Unzulässigkeit der Verarbeitung von Daten bekannt geworden ist (§ 27 Abs. 1 Z 1 DSG 2000). Eine Verletzung im Recht auf Löschung durch die Erstbeschwerdegegnerin hat der Beschwerdeführer aber nicht geltend gemacht.

I. Erkennungsdienstliche Behandlung (K121.681/0006-DSK/2011, 18. 5. 2011)

Sachverhalt

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass ihn die Beschwerdegegnerin (eine Bundespolizeidirektion) nach Sicherstellung von ca. 70 Hanfpflanzen und ca. 1 kg getrockneter Cannabisblüten in seiner Wohnung im Februar 2010 erkennungsdienstlich behandelt habe (Lichtbilder, Fingerabdrücke und DNA-Probe). Der Beschwerdeführer sei unbescholten gewesen, habe sich nicht zum Tatverdacht geäußert, und es seien außer den sichergestellten Pflanzen und Pflanzenteilen keine konkreten Anhaltspunkte dafür vorgelegen, dass der Beschwerdeführer (über möglichen Eigenbedarf hinaus) Cannabis in Verkehr gesetzt habe oder in Verkehr bringen würde. Ein Schluss dahingehend, dass konkreter Bedarf an den Daten zwecks Prävention weiterer gefährlicher Angriffe des Beschwerdeführers bestünde, sei daher nicht zulässig gewesen.

Eine Abfrage der EKIS-Personeninformationen (PI) ergab, dass der Beschwerdeführer im Juli 2009 von der Kriminalpolizei wegen des Verdachts des Konsums, Erwerbs, und Besitzes von Cannabiskraut für den Eigengebrauch (§ 27 Abs. 2 SMG) bei der Staatsanwaltschaft zur Anzeige gebracht worden war.

Rechtliche Würdigung

Die Beschwerde war nicht berechtigt. Der VwGH hat seine Rechtsprechung zur Verarbeitung erkennungsdienstlicher Daten wie folgt geändert: »*Im Hinblick auf den geänderten Gesetzestext und die Absicht des (historischen) Gesetzgebers (Hinweis EB zur RV 272 BlgNR 23. GP 8 f) vermag der Verwaltungsgerichtshof seine bisherige, zur früheren Rechtslage ergangene Rechtsprechung nicht aufrecht zu erhalten. Der Verwaltungsgerichtshof geht daher davon aus, dass im zweiten Fall des § 65 Abs. 1 SPG bereits eine abstrakte Form von Wahrscheinlichkeit, die an der verwirklichten Tat anknüpft, für die Annahme ausreicht, die erkennungsdienstliche Behandlung sei zur Vorbeugung weiterer gefährlicher Angriffe erforderlich*« (*Erkenntnis des VwGH vom 1. April 2010, Zl 2010/17/0065*).

Der Beschwerdeführer war des Suchtgifthandels verdächtig, also einer Vorsatztat, die gemäß § 16 Abs. 2 SPG als »gefährlicher Angriff« zu qualifizieren war (die Ausnahme gemäß dem letzten Halbsatz dieser Bestimmung kommt hier nicht zur Anwendung, da nicht Erwerb und Besitz, sondern Erzeugung eines Suchtmittels zum Tatbild der Anlasstat gehörten). Die sichergestellte Suchtgiftmenge überstieg die genannte Grenzmenge

i. S. des § 28b SMG und begründete damit den Verdacht des Verbrechens nach § 28a Abs. 1 SMG. Dies wurde zwar erst durch die kriminaltechnische Laboruntersuchung beweiskräftig festgestellt, doch ist den ermittelnden und entsprechend geschulten Exekutivbeamten zuzubilligen, anhand der Zahl und Größe der sichergestellten Cannabispflanzen die für die nach § 65 Abs. 1 SPG gebotene begründete Einschätzung der Tat und des Täters notwendigen Schlüsse auch anhand eines Augenscheins zu ziehen. Die aufgefundenen 70 Hanfpflanzen stellen jedenfalls eine deutlich größere Menge dar, als sie üblicherweise in Wohnräumen oder im Freien für den Suchtgift-Eigenkonsum einer Einzelperson angebaut wird.

Die im Zeitpunkt der erkennungsdienstlichen Behandlung vorliegenden Ergebnisse des Ermittlungsverfahrens ließen den Schluss zu, dass der Beschwerdeführer den Entschluss gefasst hatte, Suchtgift in großer Menge zu erzeugen und damit das Tatbild des Suchtgifthandels zu erfüllen. Ein wesentlicher Gesichtspunkt zur Beurteilung des Präventionsbedarfes gemäß § 65 Abs. 1 SPG ist der abstrakte Gefahrengrad der verwirklichten Tat für die öffentliche Sicherheit, ohne dass es einer besonderen Berücksichtigung der Person des Beschuldigten bedarf (arg »wegen der Art oder Ausführung der Tat oder der Persönlichkeit des Betroffenen«). Bereits die Art der zur Last gelegten Tat selbst – Suchtgifthandel, beinhaltend den Verdacht der Suchtgifterzeugung in großer Menge – weist im sicherheitspolizeilichen Sinn einen erhöhten Gefährlichkeitsgrad auf, da die Tat als Dauerdelikt mit der Eignung, andere Personen durch den Vorsatz zur Weitergabe des erzeugten Cannabis zu gefährden, zu qualifizieren ist. Hierauf konnte im Zeitpunkt der erkennungsdienstlichen Behandlung die nachvollziehbare und zulässige Prognoseentscheidung gestützt werden, der Beschwerdeführer müsse durch eine erkennungsdienstliche Behandlung gemäß § 65 Abs. 1 SPG von weiteren gefährlichen Angriffen abgehalten werden.

Auch die strengeren gesetzlichen Bedingungen für die Ermittlung von DNA-Daten gemäß § 67 Abs. 1 SPG waren erfüllt. Aus der Verdachtslage, der Beschwerdeführer habe bereits den Entschluss gefasst, das Suchtgift in Verkehr zu bringen, durfte der Schluss gezogen werden, der Beschwerdeführer werde als Täter Spuren hinterlassen (z. B. bei der Verpackung von Suchtgift), die seine Wiedererkennung aufgrund der ermittelten genetischen Information ermöglichen würden.

m. Verwendung eines Gutachtens im Ermittlungsverfahren (K121.683/0009-DSK/2011, 17. 6. 2011)

Sachverhalt

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass die Beschwerdegegnerin (eine Sicherheitsdirektion) ein im Zuge eines Pensionierungsverfahrens erstelltes Gutachten eines Facharztes für Psychiatrie und eines klinischen Gesundheitspsychologen der Versicherungsanstalt öffentlich Bediensteter (BVA) zum Gesundheitszustand des Beschwerdeführers auch für Zwecke kriminalpolizeilicher Ermittlungen verwendet habe.

Tatsächlich ist ein in einem Verfahren zur vorzeitigen Versetzung in den Ruhestand wegen eines länger andauernden, psychisch bedingten Krankenstands durch einen Sachverständigen der BVA erstelltes Gutachten an die Beschwerdegegnerin weitergeleitet worden. Darin wurde verfügt: »Hinsichtlich der behaupteten Anschuldigungen des … sind Stellungnahmen bis spätestens … vorzulegen. Einem Abschlussbericht wird entgegengesehen.« Die Beschwerdegegnerin informierte das intern für strafprozessuale Ermittlungen gegen Beamte des eigenen Dienststandes zuständige »Büro für besondere Ermittlungsmaßnahmen« (BBE) in einer zusammenfassenden Darstellung vom Sachverhalt und übermittelte in weiterer Folge über dessen Wunsch auch jene Seite aus dem Gutachten, auf der Vorwürfe des Beschwerdeführers gegen Kollegen wiedergegeben werden.

Rechtliche Würdigung

Die Beschwerde war nicht begründet. Zunächst stellte die DSK klar, dass die

Begutachtung durch einen medizinischen Sachverständigen kein in besonderem Umfang geschütztes Arzt-Patientenverhältnis darstellt. Es bestand kein Behandlungsvertrag, der Beschwerdeführer ist nicht freiwillig zwecks Behandlung, sondern aufgrund dienstrechtlicher Pflichten vor Sachverständigen erschienen. Der Sachverständige war nicht behandelnder Arzt bzw. Psychologe, sondern aufgrund speziellen Fachwissens als Sachverständiger Mitwirkender an einem dienstrechtlichen Ermittlungsverfahren mit dem Auftrag, die Tatsachen festzustellen, die Voraussetzung für eine Ruhestandsversetzung gemäß § 14 Abs. 1 und 3 BDG sind. Das Ergebnis seiner Tätigkeit (Befund und Gutachten), das im Regelfall sensible Daten des Betroffenen enthalten wird, hatte er der zuständigen Dienstbehörde zu übermitteln. Dies fällt unter die Ausnahme gemäß § 54 Abs. 2 Z 2 ÄrzteG 1998. Eine Entbindung von der ärztlichen Schweigepflicht durch den Betroffenen wird hiefür nicht benötigt.

Im Fall der BVA ist deren Rolle als medizinische »Begutachtungsstelle« durch das Gesetz (§ 14 Abs. 4 BDG) zwingend festgelegt. § 7 Abs. 4a SPG iVm § 2 Abs. 1 Z 1 DPÜ-VO 2005 legt die für die Ruhestandsversetzung zuständige Dienstbehörde fest. Diese war daher jedenfalls berechtigt, das BVA-Gesamtgutachten zu erhalten und für diesen Zweck als Beweismittel zu verwerten. Die damit verbundene Datenermittlung war gemäß § 7 Abs. 1 DSG 2000 gesetzlich gedeckt und nicht offenkundig überschießend.

Als Sicherheitsbehörde war die Beschwerdegegnerin aber auch von Amts wegen verpflichtet, gemäß §§ 4 Abs. 2, 22 Abs. 3 SPG sowie §§ 18 Abs. 1 und 2, 78 Abs. 1 und 99 Abs. 1 StPO ein amtswegiges kriminalpolizeiliches Ermittlungsverfahren einzuleiten. In einem solchen kriminalpolizeilichen Ermittlungsverfahren bestand in sinngemäßer Anwendung des § 79 StPO hier kein Recht der Beschwerdegegnerin, Akten des dienstrechtlichen Ruhestandsversetzungsverfahrens, einschließlich Gesundheitsdaten enthaltender Gutachten, die für den Verfahrensgegenstand (»Aufklärung einer Straftat einer bestimmten Person«) relevant waren, geheim zu halten. Der Inhalt des Gutachtens, d. h. die vom Beschwerdeführer gegenüber den Sachverständigen gemachten Äußerungen (Misshandlung einer Person durch einen Beamten des fremdenpolizeilichen Büros), war nämlich für die Aufklärung des Verdachts von strafbaren Handlungen (etwa eines Missbrauchs der Amtsgewalt, einer gefährlichen Drohung oder einer Körperverletzung) erkennbar von Relevanz. Über den Kreis der mit den entsprechenden gesetzmäßigen Verfahren befassten Stellen und Personen hinaus sind die im Verfahren zur Ruhestandsversetzung ermittelten Tatsachen (Daten) zwar nicht durch die ärztliche Schweigepflicht, jedoch durch die Amtsverschwiegenheit und das Datengeheimnis geschützt.

n. Ermittlung von IP-Adressen (K121.697/0008-DSK/2011, 20. 7. 2011)

Sachverhalt

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass die Beschwerdegegnerin (eine Bundespolizeidirektion) Verkehrsdaten, nämlich die ihm zugewiesene IP-Adresse, ohne richterlichen Beschluss ermittelt hätte.

Der Beschwerdeführer war mit seinem privaten PC im November 2009 unter Benützung einer bestimmten IP-Adresse, die ihm von seinem Zugangsprovider zugewiesen wurde, in einem Chatroom einer Webseite eingeloggt. Es handelt sich beim Inhaber der URL und Diensteanbieter um ein Unternehmen, das seinen Usern u. a. Schreibforen und Chatrooms zur Vereinbarung sexueller Kontakte sowie zum Austausch einschlägiger Informationen und Fantasien zur Verfügung stellt. Im Chat erweckte der Beschwerdeführer unter Benützung eines Nicknames den Eindruck, er wäre bereit, sexuelle Handlungen mit Unmündigen zu vermitteln. Der unbekannte Chatpartner verstand dies als Angebot verbotener und strafbarer sexueller Handlungen, worauf die Polizei verständigt wurde.

Die Beamten der Beschwerdegegnerin sahen aufgrund der Schilderung eine drohende Gefahr für die Sicherheit Minderjäh-

riger als gegeben. Es wurde daher zunächst eine Whois-Abfrage für die Webseite vorgenommen. Sodann wurde in einem Telefax an den in der Whois-Auskunft angegebenen technischen Dienstleister unter Angabe des Nicknames und der URL sowie unter Berufung auf § 53 Abs. 3a Z 3 SPG Auskunft über »die Daten des Users bzw dessen IP Adresse« verlangt. Dies wurde zunächst mit der rechtlichen Begründung abgelehnt, es fehle die Angabe einer IP-Adresse und eines Zeitpunkts, zu dem ein Name und eine (Post-) Adresse der IP-Adresse zugeordnet werden könnten. Die ermittelnden Beamten nahmen sodann mit dem Domaininhaber der Webseite bzw dem technischen Betreiber (Host) des Chatservers Kontakt auf. Von Letzterem wurden auf Anfrage gemäß § 53 Abs. 3a Z 3 SPG mit Telefax die Daten IP-Adresse und Login-Zeitpunkt für den User »Nickname« übermittelt. Eine weitere Whois-Abfrage öffentlich zugänglicher Daten ergab, dass der entsprechende Block von IP-Adressen einem bestimmten Unternehmen zugewiesen ist. An dieses wurde daraufhin per Telefax eine weitere Anfrage gemäß § 53 Abs. 3a Z 3 SPG nach dem Inhaber der IP-Adresse zum bestimmten Zeitpunkt gerichtet. Daraufhin wurden die Kunden-Stammdaten Name und Adresse des Beschwerdeführers übermittelt.

Rechtliche Würdigung

Die DSK betonte zunächst, dass das von ihr zu wahrende verfassungsgesetzlich gewährleistete Recht auf Geheimhaltung personenbezogener Daten gemäß § 1 Abs. 1 DSG 2000 gemäß Abs. 2 leg cit. – im Gegensatz zum Fernmeldegeheimnis – nicht unter Richtervorbehalt steht. Der Beschwerdeführer bestritt weder das Vorliegen einer konkreten, sicherheitspolizeilich relevanten Gefahrensituation, noch die Möglichkeit, für diesen Zweck einen Grundrechtseingriff vorzunehmen. Er berief sich allein auf das seiner Ansicht nach verfassungsgesetzlich zwingend vorgegebene Element eines richterlichen Beschlusses, der nicht eingeholt wurde.

In der Beschwerdesache Zl K121.279 der DSK (Bescheid vom 3. Oktober 2007, GZ K121.279/0017-DSK/2007, bestätigt vom VwGH, Erkenntnis vom 27. Mai 2009, Zl 2007/05/0280), in dem der Beschwerde stattgegeben wurde, war eine nahezu idente Sachlage gegeben, doch war in jenem Fall noch § 53 SPG in der Fassung vor BGBl I Nr 114/2007 anzuwenden. Durch Art. I Z 4 des in letzterem BGBl kundgemachten Bundesgesetzes wurde § 53 Abs. 3a SPG neu gefasst und wurden die sicherheitspolizeilichen Ermittlungsbefugnisse im Internet-Verkehr deutlich erweitert, sodass gerade derartige Ermittlungen gedeckt sind.

Die Prüfung dieser einfachgesetzlichen Ermächtigungen zu Eingriffen in das Grundrecht auf Datenschutz auf ihre Verfassungskonformität lag außerhalb der Befugnisse der DSK. Eine vom Beschwerdeführer angeregte verfassungskonforme, einschränkende Auslegung war aufgrund des klaren Wortlauts und des klaren historischen Zusammenhangs, der diesen Gesetzgebungsakt als »Antwort« auf die oben zitierte Entscheidung der DSK erscheinen ließ, nicht möglich. Es war die klare Absicht des Gesetzgebers, derartige Datenermittlungen der Sicherheitsbehörden auch ohne Gerichtsbeschluss zuzulassen.

In der Rechtsprechung des OGH wird überdies bestritten, dass eine IP-Adresse zu dem unter den Richtervorbehalt fallenden Kern des Fernmeldegeheimnisses zählt:

»Stammdaten unterliegen nicht dem im Art. 10a StGG verankerten Grundrecht des Kommunikationsgeheimnisses (§ 93 Abs. 1 Satz 1 TKG 2003 e contrario). Selbst bei dynamischen IP-Adressen erfordert die Übermittlung der zugehörigen Stammdaten an ein rite ermittelndes Gericht – der das Grundrecht auf Datenschutz nicht entgegensteht (§ 7 Abs. 2 DSG) – keine Feststellung, welche Teilnehmeranschlüsse Ursprung einer Telekommunikation waren (§ 149a Abs. 1 Z 1 lit b StPO). Die Erhebung des Namens und der Wohnadresse eines Internetbenutzers, dem eine bestimmte – sei es statische, sei es dynamische – Internetadresse zugewiesen ist oder war, ist unter keinen der Eingriffstatbestände des § 149a Abs. 1 Z 1 StPO zu subsumieren; eine planwidrige Gesetzeslücke diesbezüglich ist

weder nach dem Regelungsplan des StRÄG 2002 noch des Strafprozessreformgesetzes zu erkennen. Die Stammdaten des Namens und der Wohnanschrift des Inhabers eines bereits individualisierten Teilnehmeranschlusses können gemäß § 103 Abs. 4 TKG 2003 formlos bekannt gegeben oder durch formelle Vernehmung einer physischen Person des Access-Providers als Zeugen ermittelt werden, was im Bedarfsfall durch die entsprechenden Zwangsmaßnahmen der Strafprozessordnung durchzusetzen ist.« (OGH, 26. 7. 2005, 11 Os 57/05z, RS0120087)

Dies wurde erst jüngst, unter Berücksichtigung der inzwischen wirksamen umfassenden Änderungen der StPO, nochmals vom OGH bestätigt:

»*Die Erhebung von Name und Adresse eines Internetbenutzers, dem eine bestimmte – sei es statische, sei es dynamische – Internetadresse zugewiesen ist oder war, ist nicht als Auskunft über Daten einer Nachrichtenübermittlung iSd § 135 Abs. 2 StPO zu beurteilen. Sie unterliegt nicht dem Fernmeldegeheimnis des Art. 10a StGG, womit sie einer gerichtlichen Bewilligung nicht bedarf.*« (OGH, 13. 4. 2011, EvBl 2011/62, Leitsatz)

Es stand daher fest, dass

- der Beschwerdeführer als User mit seinem PC im Internet eingeloggt war, also eine bestimmte IP-Adresse benutzt hat,
- der Beschwerdeführer durch eigenes Verhalten zumindest den Anschein einer konkreten, innerhalb der nächsten Tage oder Stunden drohenden Gefahr für die Sicherheit Minderjähriger hervorgerufen hat, von der die Beschwerdegegnerin als Sicherheitsbehörde Kenntnis erlangt hat, und die sie gemäß § 21 Abs. 2 SPG abzuwehren verpflichtet war,
- die die Auskünfte erteilenden Unternehmen unbestritten Diensteanbieter gemäß § 92 Abs. 3 Z 1 TKG 2003 bzw § 3 Z 2 ECG waren, und
- die Beschwerdegegnerin zur Datenermittlung hinsichtlich der IP-Adresse (sowie des Namens und der Adresse des Beschwerdeführers) gemäß § 53 Abs. 3a Z 2 und 3 SPG ausdrücklich ermächtigt war.

Damit war der Eingriffstatbestand gemäß der angewendeten Gesetzesbestimmung klar erfüllt. Der Eingriff entspricht auch der generellen Ermächtigung gemäß § 8 Abs. 4 Z 1 DSG 2000.

Eine Unverhältnismäßigkeit des Eingriffs bzw. ein überschießendes Handeln oder präsente gelindere Mittel im Vergleich zur Ermittlung der IP-Adresse wurde vom Beschwerdeführer weder behauptet und aufgezeigt, noch haben sich solche Bedenken im Ermittlungsverfahren ergeben. Die Einholung einer richterlichen Genehmigung wäre dabei kein »gelinderes Mittel« im Sinne eines nach Art und Eingriffsintensität »anderen« Vorgehens gewesen. Sie hätte lediglich eine nochmalige rechtliche Prüfung durch eine unabhängige richterliche Instanz bewirkt, wobei auch der Beschwerdeführer den inhaltlichen Ausgang dieser Prüfung gar nicht in Zweifel zieht.

Auch aus diesen Blickwinkeln sah die DSK daher keine Bedenken gegen die Gesetzmäßigkeit des Vorgehens der Sicherheitsbehörde. Auch aus dem Vorbringen des Beschwerdeführers, § 53 Abs. 3a SPG habe zugunsten von § 18 Abs. 2 ECG zurückzutreten bzw. unangewendet zu bleiben, ist für seine Sache nichts zu gewinnen, wiewohl letztere Bestimmung eine richterliche Verfügung vorsieht. Denn § 18 Abs. 5 ECG ordnet an: »Sonstige Auskunfts- und Mitwirkungspflichten der Diensteanbieter gegenüber Behörden oder Gerichten bleiben unberührt.« Dem ECG ist daher keine Intention des Gesetzgebers zu entnehmen, sicherheitsbehördliche Ermittlungsermächtigungen zu beschränken. Überdies ist § 53 Abs. 3a SPG lex posterior zu § 18 Abs. 2 ECG (Inkrafttretensdatum: 1. Jänner 2002) und wäre daher letztere Bestimmung auch im Fall eines echten, interpretativ zu lösenden Normenkonflikts nur nachrangig anzuwenden.

Die Beschwerde war daher als nicht berechtigt abzuweisen.

Dieser Bescheid wurde beim Verwaltungsgerichtshof angefochten, die Beschwerde aber abgewiesen.

o. Unrechtmäßiges Übermitteln durch Vertreter? (K121.729/0008-DSK/2011, 30. 9. 2011)

Sachverhalt

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass ein Schreiben aus März 2011, das inhaltlich einer Landespersonalvertretung (Beschwerdegegnerin) zuzurechnen sei, von A mit Signatur »Büro des Zentralbetriebsrates« geschickt worden sei. Die Angelegenheit hätte aber keinen Bezug zum Zentralbetriebsrat und die Einbindung des A sei damit datenschutzrechtlich unzulässig gewesen.

Diese Stellungnahme der Beschwerdegegnerin wurde dem Beschwerdeführer per Mail in Kopie zu Handen seiner rechtsanwaltlichen Vertretung tatsächlich von A geschickt. A war an diesem Tag in Vertretung von B, dem eigentlichen Kanzleileiter der Beschwerdegegnerin, tätig. Dieses Mail trug versehentlich die Signatur »Büro des Zentralbetriebsrates«, mit dem sich die Beschwerdegegnerin eine Kanzlei teilt und dem A organisatorisch zuzurechnen ist.

Rechtliche Würdigung

Die Beschwerde war nicht berechtigt. Aus der versehentlichen Verwendung der falschen Signatur kann noch keine Verletzung im Recht auf Geheimhaltung abgeleitet werden, wenn die E-Mail dennoch von der Beschwerdegegnerin (bzw einem ihr zurechenbaren Organwalter) stammt. Die hier tätig gewordene Person (A) ist zwar organisatorisch dem Büro des Zentralbetriebsrates zuzurechnen, funktionell war sie aber aufgrund der bestehenden Vertretungsregelung bei der konkreten Verwendung für die Beschwerdegegnerin tätig. Sie war daher berechtigt, das E-Mail zu versenden und – ggf. – auch Kenntnis von dessen Inhalt zu erlangen. Nachweise für eine weitere Verwendung der Inhalte dieses Mails – etwa für Zwecke des Zentralbetriebsrates selbst – sind nicht hervorgekommen und wurden vom Beschwerdeführer auch nicht behauptet. Ein datenschutzrechtliches Übermitteln (§ 4 Z 12 DSG 2000) im Vorfeld der Versendung dieser E-Mail, welches auf seine Rechtmäßigkeit zu prüfen wäre, hat daher gar nicht stattgefunden.

p. Verwendung im lebenswichtigen Interesse (K121.723/0008-DSK/2011, 30. 9. 2011)

Sachverhalt

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Geheimhaltung dadurch, dass das Büro für Waffen- und Veranstaltungsangelegenheiten bei der Beschwerdegegnerin (einer Bundespolizeidirektion) im November 2010 dem Verkehrsamt bei der Beschwerdegegnerin intern eine Information über den Inhalt eines amtsärztlichen Gutachtens (eingeholt im Ermittlungsverfahren betreffend seine Vorstellung gegen ein durch Mandatsbescheid verhängtes Waffenverbot) übermittelt habe, worauf ein Verfahren zur Überprüfung seiner Lenkberechtigungen eingeleitet worden sei.

Dem Beschwerdeführer wurde mit Mandatsbescheid der Beschwerdegegnerin aus Juni 2010 der Besitz von Waffen und Munition verboten. Dagegen hat er Vorstellung erhoben. Im darauf folgenden Ermittlungsverfahren zur Überprüfung etwaiger medizinischer Gründe für die Verhängung des Waffenverbots hat die Amtsärztin im November 2010 Befund und Gutachten über ihn erstellt. Sie kam zu dem Schluss, dass der Beschwerdeführer an einer Depression leide und der Verdacht auf eine psychische Erkrankung aus dem schizophrenen Formenkreis bestehe. Aggressionen und Gewaltausbrüche seien aktenkundig, weshalb empfohlen wurde, auch die Eignung zum Lenken von Kfz einer Überprüfung zu unterziehen.

Nur Letzteres wurde dem Verkehrsamt der Beschwerdegegnerin mit interner Note aus November 2010 mitgeteilt, ohne nähere Angaben zum Gesundheitszustand des Beschwerdeführers zu machen. Im Jänner 2011 richtete das Verkehrsamt daher eine interne Note an den Chefärztlichen Dienst, in der die Amtsärztin um Stellungnahme ersucht wurde, welche konkreten Hinweise

sich betreffend die Erkrankung des Beschwerdeführers bzw dessen beschränkte Eignung zum Lenken von Kfz aus dem amtsärztlichen Gutachten aus November 2010 ergeben würden. Mit Antwortschreiben aus März 2011 erging die Empfehlung zur Überprüfung der gesundheitlichen Eignung zum Lenken von Kfz aus folgendem Grund: Es besteht eine Depression und der Verdacht auf eine Erkrankung aus dem schizophrenen Formenkreis. A lebt in einer Scheinwelt, es kommt immer wieder zu Gewaltdurchbrüchen vor allem im familiären Umfeld.

Das Verkehrsamt leitete darauf ein Verfahren zur Entziehung von Lenkberechtigungen wegen fehlender gesundheitlicher Eignung ein und ließ den Beschwerdeführer gem § 24 Abs. 4 FSG zu einer neuerlichen amtsärztlichen Untersuchung laden.

Rechtliche Würdigung

Der durch das Grundrecht auf Datenschutz unmittelbar eingeräumte subjektiv-öffentliche Anspruch auf Geheimhaltung personenbezogener Daten schützt sowohl vor ungerechtfertigter Ermittlung als auch Übermittlung von Daten.

Das belangte Organ konnte sich auf den Tatbestand des »lebenswichtigen Interesses« des Betroffenen gem § 1 Abs. 2 DSG 2000 stützen. Ein solcher Umstand macht, auch wenn der Eingriff durch eine staatliche Behörde erfolgt, keine ausdrückliche gesetzliche Ermächtigung erforderlich und stellt einen Typus des Eingriffs dar, der – vergleichbar etwa den Bestimmungen über Notwehr, Notstand und Nothilfe (§§ 3 und 10 StGB) – wegen der Bedeutung des bedrohten Rechtsgutes und der Notwendigkeit schnellen Handelns erlaubt ist.

Im Beschwerdefall steht fest, dass die Amtsärztin Bedenken hinsichtlich der psychischen Gesundheit des Beschwerdeführers und damit seiner Tauglichkeit zum Lenken von Kfz im Sinne von §§ 5 Abs. 1 Z 4 und 13 FSG-GV hatte. Das Lenken von Kfz stellt eine an sich gefährliche Tätigkeit dar, für die der Gesetzgeber nicht ohne Grund den Nachweis gesundheitlicher Eignung fordert. Durch Teilnahme einer geistig un- oder mindertauglichen Person als Lenker eines Kfz am Straßenverkehr wird eine Gefahr hervorgerufen, die neben der Sicherheit aller Straßenverkehrsteilnehmer auch das Leben und die körperliche Unversehrtheit des Betroffenen selbst bedroht. Damit war eine Situation gegeben, in der lebenswichtige Interessen des Betroffenen selbst die Übermittlung von Daten an die zuständige Führerscheinbehörde zulässig machten, um den noch nicht völlig klargestellten Sachverhalt zumindest einer Überprüfung unterziehen zu können.

Die Tätigkeit der Amtsärztin (Datenübermittlung von einem Aufgabenbereich der Beschwerdegegnerin in einen anderen, Zweckänderung) war im Beschwerdefall der Beschwerdegegnerin zuzurechnen, aber durch die unmittelbare grundrechtliche Ausnahmeklausel des »lebenswichtigen Interesses« gerechtfertigt. Die Beschwerde wurde abgewiesen.

q. Sachverständigengutachten im Dienstrechtsstreit (K121.732/0008-DSK/2011, 30. 9. 2011)

Sachverhalt

Der Beschwerdeführer behauptete eine Verletzung im Recht auf Geheimhaltung dadurch, dass eine Sicherheitsdirektion ein im Zuge eines Pensionierungsverfahrens erstelltes Gutachten (enthaltend Gutachten eines Facharztes für Psychiatrie und eines klinischen Gesundheitspsychologen) der BVA zum Gesundheitszustand des Beschwerdeführers auch für Zwecke kriminalpolizeilicher Ermittlungen verwendet (und dazu intern vom Personalbüro dem Büro für besondere Ermittlungen vorgelegt) habe. Dadurch habe die BVA sein Recht auf Geheimhaltung verletzt.

Wegen eines länger andauernden, psychisch bedingten Krankenstands leitete die Dienstbehörde zwecks möglicher vorzeitiger Ruhestandsversetzung ein Verfahren zur Überprüfung der Dienstfähigkeit des in einem öffentlich rechtlichen Dienstverhältnis stehenden Beschwerdeführers ein. Mit Schreiben aus Oktober 2010 (mit mehreren Beilagen, darunter Urlaubs- und Kranken-

standsblatt, Arbeitsplatzbeschreibung und Anforderungsprofil, ein Fragebogen und bereits vorliegende ärztliche Befunde und Gutachten) wurde die Beschwerdegegnerin auf »Formblatt A« um die Erstellung eines »ärztlichen Gutachtens über den Gesundheitszustand« des Beschwerdeführers ersucht.

In der Befragung (Anamnese) durch einen Sachverständigen der Beschwerdegegnerin im November 2010 schilderte der Beschwerdeführer u. a. ihn belastende Vorkommnisse während seiner Dienstzeit im fremdenpolizeilichen Büro, darunter die Bedrohung und Misshandlung (Ohrfeigen) von einvernommenen Personen durch einen – namentlich nicht genannten – Referatsleiter. Dieses Gespräch wurde im BVA-Gesamtgutachten wiedergegeben. Es umfasste weiters ein ärztliches Sachverständigengutachten und eine zusammenfassende Stellungnahme des leitenden Arztes. Das Gesamtgutachten wurde mit Begleitschreiben an die Beschwerdegegnerin weitergeleitet.

Rechtliche Würdigung

Im gegebenen Fall war der Sachverständige nicht behandelnder Arzt bzw Psychologe, sondern Mitwirkender an einem dienstrechtlichen Ermittlungsverfahren mit dem Auftrag, jene Tatsachen festzustellen, die Voraussetzung für eine Ruhestandsversetzung des Beschwerdeführers gem § 14 Abs. 1 und 3 BDG sind. Das Ergebnis seiner Tätigkeit (Befund und Gutachten), das im Regelfall sensible Daten des Betroffenen enthalten wird, hatte er der zuständigen Dienstbehörde zu übermitteln. Dies fällt unter die Ausnahme gem § 54 Abs. 2 Z 2 ÄrzteG 1998, eine Entbindung von der ärztlichen Schweigepflicht wird hiefür nicht benötigt.

Im Fall der Beschwerdegegnerin ist deren Rolle als medizinische »Begutachtungsstelle« durch das Gesetz (§ 14 Abs. 4 BDG 1979) zwingend festgelegt. Gem § 7 Abs. 4a SPG iVm § 2 Abs. 1 Z 1 DPÜ-VO 2005 ist Sicherheitsdirektion die für die Ruhestandsversetzung des Beschwerdeführers zuständige Dienstbehörde. Sie war daher berechtigt, das BVA-Gesamtgutachten zu erhalten und für diesen Zweck als Beweismittel zu verwerten. Die damit verbundene Datenermittlung war gem § 7 Abs. 1 DSG 2000 gesetzlich gedeckt und war nicht offenkundig überschießend.

Vor dem Hintergrund, dass zwecks Überprüfung der gesundheitlichen Eignung von der Dienstbehörde regelmäßig ein ärztliches Gutachten in Auftrag gegeben wird, bringt der Beschwerdeführer nun sinngemäß vor, dass es überschießend sei, wenn seine Dienstbehörde den Inhalt der Befunde zur Kenntnis erhalten hätte, weil es vielmehr ausreichen müsse, wenn das Ergebnis des Gutachtens in Form einer zusammenfassenden Stellungnahme des leitenden Arztes (enthaltend das Kalkül »dienstfähig/bedingt dienstfähig/dauernd dienstunfähig«) an die Dienstbehörde übermittelt werde. Damit verkennt er jedoch die rechtliche Stellung eines Sachverständigen, der lediglich dem zur Entscheidung befugten behördlichen Organ seine sachverständige Meinung zur Gutachtensfrage samt den Sachargumenten zu liefern hat, die das behördliche Organ in die Lage versetzen sollen, eine logisch nachvollziehbare Entscheidung zu treffen. Zu diesem Zweck müssen dem zur Entscheidung befugten Organ auch alle zur Begründung der sachverständigen Äußerung notwendigen Informationen zur Verfügung gestellt werden, d. h. im vorliegenden Fall auch das Ergebnis der Anamnese über den Gesundheitszustand des Betroffenen. Das Vorhandensein dieser Informationen bei der Behörde ist auch im Interesse der Nachprüfbarkeit der behördlichen Entscheidung – etwa im dienstrechtlichen Verfahren – unerlässlich (siehe auch den Bescheid vom 14. April 2010, GZ K121.572/0003-DSK/2010)

Die Beschwerdegegnerin hat im vorliegenden Beschwerdefall im datenschutzrechtlichen Sinne weiters nur als Dienstleisterin der Dienstbehörde gehandelt. Sie hat dabei Weisungen erfüllt und Entscheidungen vollzogen, die die Dienstbehörde getroffen hat. Die Beschwerde war daher spruchgemäß abzuweisen.

6.1.3 Recht auf Löschung und Richtigstellung

a. Löschung von Daten eines Kunden eines Wertpapierdienstleistungsunternehmens bei der Finanzmarktaufsicht (K121.552/0002-DSK/2010, 20. 1. 2010)

Sachverhalt

Der Beschwerdeführer fühlte sich dadurch in seinem Recht auf Löschung verletzt, dass die Finanzmarktaufsicht (FMA) bei einem ihrer Aufsicht unterstehenden Wertpapierdienstleistungsunternehmen, dessen Kunde der Beschwerdeführer sei, die zu seiner Person schon rechtswidrig ermittelten Daten auf sein entsprechendes Begehren hin nicht gelöscht hat.

Die FMA führte im Jänner 2009 bei A, einer Inhaberin einer sogenannten »großen Konzession« zur gewerblichen Erbringung von Wertpapierdienstleistungen und als solche der Aufsicht der FMA unterstehend, ein sogenanntes Vor-Ort-Prüfungsverfahren mit dem Ziel durch, mittels Ziehung von repräsentativen Kundenstichproben Ansatzpunkte für spätere Detailprüfungen der gesetzeskonformen Geschäftsgebarung der A zu gewinnen. Für diesen Zweck verlangte die FMA von A eine Gesamtliste der Kunden, die auch von A an die FMA übermittelt wurde. In dieser Liste sind auch Daten des Beschwerdeführers zu folgenden Datenarten enthalten: interne Kundennummer des Beschwerdeführers bei A; Familienname; Nationalität; Produktname (= Name des/der Investmentfonds samt INSI – internationaler Wertpapierkennnummer); Abschlussdatum und investierter Geldbetrag (Investitionshöhe). Da der Beschwerdeführer nicht bei der Stichprobenziehung für weitere Prüfungen der A erfasst wurde, werden seine Daten in Form der ausgedruckten Liste im physischen Akt (Papierakt) der Vor-Ort-Prüfung aufbewahrt. Eine weitere Verarbeitung erfolgte erst in Form des Scannens (automationsunterstützten, grafischen Erfassens und Speicherns) der Liste zwecks Übermittlung an den VfGH im Zuge eines Beschwerdeverfahrens.

Die im Juni 2009 vom Beschwerdeführer mit ausführlicher rechtlicher Begründung von der FMA verlangte Löschung der Daten lehnte diese im Juli 2009 mit der Begründung ab, die »Aufbewahrung« der rechtmäßig ermittelten Daten, die als »sonstige Unterlagen und Aufzeichnungen« gem § 22 Abs. 4 FMABG zu werten seien, über einen Zeitraum von mindestens sieben Jahren sei durch die zitierte Bestimmung geboten.

Rechtliche Würdigung – Zur Rechtmäßigkeit der Datenermittlung und Aufbewahrung

Die DSK stellte zunächst fest, dass die Aufbewahrung der beschwerdegegenständlichen Daten in Form einer Liste mit vorgegebenen Datenarten als (manuelle) Datei gem § 4 Z 6 DSG 2000 zu werten ist, auf deren Ermittlung und Verarbeitung gem § 58 DSG 2000 das DSG 2000 wie bei automationsunterstützten Datenanwendungen anzuwenden ist.

Der Beschwerdeführer bestritt nun die Rechtmäßigkeit der Ermittlung und Speicherung wegen fehlender gehörig determinierter gesetzlicher Ermächtigung sowie mangels Relevanz seiner Daten als Kunde für den Zweck der von der FMA bei A durchgeführten Prüfung (fehlerhafte Interessenabwägung). Dieser Argumentation konnte die DSK aber nicht folgen:

Gemäß § 91 Abs. 3 Z 1 bis 4 WAG 2007 war und ist die FMA gesetzlich ermächtigt, in die Bücher, Schriftstücke und Datenträger der ihrer Aufsicht unterstehenden Unternehmen (wie unstrittig auch der A) Einsicht zu nehmen und Kopien von ihnen zu erhalten sowie von diesen Unternehmen und ihren Organen Auskünfte zu verlangen und gem. den Verwaltungsverfahrensgesetzen Personen vorzuladen und zu befragen, durch eigene Prüfer, Abschlussprüfer oder sonstige Sachverständige vor Ort Prüfungen durchzuführen sowie von den Unternehmen bereits existierende Aufzeichnungen von Telefongesprächen und Datenübermittlungen anzufordern. Die FMA ist weiters gem Abs. 4 Z 1 und 2 leg. cit. berechtigt, für Zwecke entsprechender Verfahren personenbezogene Daten zu verarbeiten. Diese Ermächtigung ist ausreichend präzise, um eine Eingriffser-

mächtigung gem § 8 Abs. 1 Z 1 DSG 2000 zu bilden, sodass es keiner besonderen Interessenabwägung zur Rechtfertigung des Eingriffs bedarf. Die beschwerdegegenständlichen Kundendaten gehören zweifelsfrei zu jenen Daten, die auf den in § 91 Abs. 3 Z 1 WAG 2007 erwähnten Datenträgern einer Wertpapierfirma gespeichert sein werden. Vom Gesetzgeber zu erwarten, er müsste jede denkbare Datenart und jeden möglichen Betroffenenkreis für jede infrage kommende Prüfungsaufgabe einer Behörde wie der FMA voraussehen und im Gesetz einzeln aufzählen, überspannt eine vernünftige Gesetzgebungstechnik. Die FMA hat glaubwürdig dargelegt, für ihre Überwachungsaufgaben gem § 91 Abs. 1 WAG 2007 eine Stichprobe der Kunden der A ziehen zu müssen und dafür eine Gesamtliste der Kunden samt einigen für die Auswahl relevanten Daten betreffend deren Investments zu benötigen. Die Ermittlung und Speicherung der Daten wurde daher als rechtmäßig eingestuft.

Zur Rechtmäßigkeit der weiteren Datenverarbeitung

Dem weiteren Begehren des Beschwerdeführers, nach Auswahl der Kundendaten für eine Stichprobe, spätestens aber nach seinem begründeten Löschungsbegehren, hätten die Daten, da nicht mehr benötigt, gelöscht werden müssen, steht § 22 Abs. 4 FMABG entgegen. § 22 Abs. 4 FMABG ist eine archiv- bzw dokumentationsrechtliche Rechtsvorschrift des Typs, auf den § 6 Abs. 1 Z 5 und 27 Abs. 3 DSG 2000 Bezug nehmen. Die DSK zweifelte nicht daran, dass von den »Unterlagen und Aufzeichnungen« auch manuelle Dateien wie die verfahrensgegenständliche, auf Papier ausgedruckte und in einen Papierakt (»physischen Akt«) eingereihte Kundenliste erfasst sein sollen. Die Ablehnung des Löschungsbegehrens verletzte den Beschwerdeführer daher nicht in seinen Rechten, sodass die Beschwerde insgesamt abzuweisen war.

Dieser Bescheid wurde beim Verwaltungsgerichtshof angefochten. Das Verfahren ist anhängig

b. Auftraggebereigenschaft von Unternehmen der Gebietskörperschaften (K121.598/0006-DSK/2010, 30. 7. 2010)

Sachverhalt

Die Beschwerdeführerin behauptete eine Verletzung im Recht auf Geheimhaltung und Löschung dadurch, dass der Magistrat der Stadt Wien (Beschwerdegegner) als datenschutzrechtlicher Auftraggeber für das städtische Unternehmen Stadt Wien – Wiener Wohnen Daten betreffend Mietzinsrückstände zwecks Inkasso an eine Kreditauskunftei weitergegeben habe bzw. ihrem Löschungsbegehren/Widerspruch nicht entsprochen habe. Tatsächlich bestanden aus einem früheren Mietverhältnis der Beschwerdeführerin mit der Stadt Wien Mietzinsrückstände, für die eine bis heute nicht vollständig erfüllte ratenweise Abzahlung vereinbart war. Das städtische Unternehmen »Wiener Wohnen« steht dabei in einem Vertragsverhältnis mit einer Kreditauskunftei und gab Name, Geschlecht, Geburtsdatum, Zustelladressen (einschließlich früherer Adressen und jenen der Mietobjekte) sowie die Daten des Zahlungsverkehrs betreffend die Beschwerdeführerin an jene weiter.

Die Beschwerdeführerin ist der Meinung, dass die »Eintreibung rückständiger Gemeindeabgaben (auch Mieten)« durch private Unternehmen unzulässig sei und entsprechende Weitergabe sowohl Amtsverschwiegenheit als auch Datenschutz verletzen würde. Der Beschwerdegegner ist hingegen der Ansicht, er handle konkret im Rahmen der Privatwirtschaftsverwaltung.

Rechtliche Würdigung

Die DSK befand die Rechtsansicht der Beschwerdeführerin für unrichtig: die Verwaltung der städtischen Wohnhäuser (Vermietung, Verrechnung und Einbringung des Mietzinses etc.) ist Privatwirtschaftsverwaltung einer Gebietskörperschaft gemäß Art. 17 B-VG, da dieselben Handlungsweisen jedem Privaten bei seiner Erwerbstätigkeit oder Vermögensverwaltung offen stehen. Die Unternehmung der Stadt Wien »Wiener Wohnen« hat im Rahmen der Privatautonomie die Entscheidung

getroffen, für das Inkasso ein bestimmtes Unternehmen heranzuziehen.

Dies ist in ihrem überwiegenden berechtigten Interesse, da das berechtigte Interesse des Auftraggebers, sich jedes Mittels zu bedienen, das gesetzmäßig (in der Gewerbeordnung vorgesehene, unternehmerische Dienstleistung) zur Durchsetzung von Forderungen Privaten in die Hand gegeben ist, das berechtigte Interesse der Beschwerdeführerin an der Unterlassung der Datenverwendung für Inkassozwecke überwiegt. Zu beachten ist, dass es sich bei der »Weitergabe« von Daten eines Schuldners an ein Inkassoinstitut regelmäßig um eine »Übermittlung« iSd DSG 2000 handelt. Da die Beschwerdeführerin unbestritten Schulden bei »Wiener Wohnen« hatte, war diese Übermittlung im konkreten Fall auch zulässig.

Weil die Einbringung der Mietzinsforderung noch im Gange war, die Datenverwendung daher in jedem Fall einen durch überwiegendes berechtigtes Interesse des hier belangten Auftraggebers gedeckten Zweck erfüllt, ging auch das Widerspruchsbegehren ins Leere. Die Beschwerde wurde daher abgewiesen.

c. Löschung der Dokumentation des Arbeitsmarktservices (K121.608/0014-DSK/2010, 24. 9. 2010)

Sachverhalt

Die Beschwerdeführerin behauptet in ihrer Beschwerde eine Verletzung im Recht auf Löschung und Richtigstellung dadurch, dass das Arbeitsmarktservice (Beschwerdegegner) ihrem Löschungs- und Richtigstellungsbegehren aus Februar 2010 laut Schreiben aus März 2010 nur teilweise entsprochen habe. Die Beschwerdeführerin befinde sich auf Arbeitssuche und sehe sich durch das Verhalten ihrer früheren AMS-Beraterin unrechtmäßig behandelt. Die Beraterin sei der Meinung, sie leide an psychischen Problemen und sei nicht arbeitsfähig und sollte infolgedessen um eine Pension ansuchen. Die Löschungs- und Richtigstellungsanträge bezögen sich auf die automationsunterstützt geführte Datenanwendung zur Dokumentation des Betreuungsverlaufs. Teilweise ließen die Eintragungen »Elemente des Mobbings« vermuten, seien diskriminierend und verletzend und daher geeignet, ihren Betreuungserfolg der Re-Integration in die Arbeitswelt zu gefährden.

Im Zuge der Betreuung durch die regionale Geschäftsstelle des Beschwerdegegners wurden gewisse hier strittige Eintragungen in die automationsunterstützte Dokumentation des Betreuungsvorgangs (Verlauf der Beratungsgespräche, »Beratungstagebuch«) gemacht, wie z. B. *»Kdn möchte auch NICHT in Krankenstand gehen«; »Ihre Leiden dürften zum großen Teil psychosomatische Ursachen haben«; »Sie fragt mich, so als ob sie sich noch nie irgendwo beworben hätte, wie jetzt die weitere Vorgehensweise mit dem Stellenvorschlag wohl wäre«; »Für die Kdin ist nicht einzusehen, warum sie jetzt wieder alles (Befunde, Gutachten) heraussuchen soll, wenn eh bei uns schon alles aufliegt.«*

Dem Löschungsbegehren der Beschwerdeführerin aus Februar 2010, in dem sie detailliert ausführte, warum sie bestimmte Eintragungen für unzulässig bzw unzutreffend hält, gab die Beschwerdegegnerin teilweise statt (so wurden z. B. die oben genannte 2. und 3. Passage gestrichen), die übrigen begehrten Änderungen am Datensatz wurden aber abgelehnt, da sie keine Auswirkung auf die Datenanwendung bzw die Gesamtinformation über die Betreuungsvorgänge hätten.

Rechtliche Würdigung

Die DSK hielt zunächst fest, dass der Beschwerdegegner bereits im laufenden Verfahren im Sinne von § 31 Abs. 8 DSG 2000 reagiert hat, indem er weite Teile der in Beschwerde gezogenen Dateneintragungen gelöscht hat. Eine rechtliche Bewertung der Richtigkeit der gelöschten Daten unterblieb daher, die Beschwerde war insoweit nunmehr unbegründet.

Grundsätzlich ist der Beschwerdegegner gemäß § 25 Abs. 1 Z 5 AMSG gesetzlich ermächtigt (§ 8 Abs. 1 Z 1 DSG 2000), allgemeine Daten zum Betreuungsverlauf von Arbeitsuchenden zu verarbeiten. Die

übrigen Eintragungen über die Beschwerdeführerin umfassen solche sonstigen Eintragungen über den Beratungs- und Betreuungsverlauf, die die Beschwerdeführerin als unvollständig und damit irreführend und unrichtig im Bezug auf den Verarbeitungszweck bzw als rechtswidrig ansieht, worauf sich ihre Richtigstellungs- und Löschungsbegehren gründeten.

Sie übersah jedoch, dass es sich hier auch um eine Verfahrensdokumentation im Sinne von § 27 Abs. 3 DSG 2000 handelt und die Datenrichtigkeit daher daran zu messen ist, ob die Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist. Die Beschwerdeführerin hat hier kein subjektives Recht auf Richtigstellung dahin gehend, dass sie sämtliche Angaben, die sie subjektiv für die Dokumentation von Bedeutung hält, in das gegenständliche »Beratungstagebuch« der AMS-BetreuerInnen hineinreklamiert und bestimmte Formulierungen von ihr vorgegeben werden. Vielmehr kann das die Dokumentation führende Organ des datenschutzrechtlichen Auftraggebers die Formulierungen und die Gewichtung der zu protokollierenden Ereignisse innerhalb gewisser Grenzen nach Treu und Glauben selbst gestalten. Hinzu kommt hier, dass ja viele Eintragungen auf eigenem Vorbringen der Beschwerdeführerin beruhen.

Aus der vorliegenden, nicht bereits gelöschten Dokumentation war nichts erkennbar, das auf ein Handeln des Beschwerdegegners wider Treu und Glauben schließen lassen würde. Durch die weitere Ablehnung des Löschungsbegehrens war die Beschwerdeführerin daher nicht in ihrem Recht auf Löschung und Richtigstellung eigener Daten verletzt worden.

d. Zuständigkeit bei Löschung erkennungsdienstlicher Daten – Teil 1 (K121.633/0024-DSK/2010, 3. 12. 2010)

Sachverhalt

Der Beschwerdeführer behauptet (u. a.) eine Verletzung im Recht auf Löschung dadurch, dass die Beschwerdegegnerin (eine Sicherheitsdirektion) ihn betreffende, im Dezember 2008 ermittelte erkennungsdienstliche Daten nicht gelöscht habe.

Der Beschwerdeführer wurde im Dezember 2008 während der Hauptverhandlung betreffend eine Strafsache nach dem Finanzstrafgesetz mit ihm als Beschuldigtem auf gerichtlich bewilligte Anordnung der Staatsanwaltschaft fest- und in Untersuchungshaft genommen (Verdacht der versuchten Erpressung, §§ 15 Abs. 1, 144 Abs. 1 StGB) und am selben Tag erkennungsdienstlich behandelt (Lichtbilder, genaue Personsbeschreibung, Abdrücke der Finger und Handflächen sowie ein durch Mundhöhlenabstrich (MHA) gewonnenes DNA-Profil). Der Beschwerdeführer war zu diesem Zeitpunkt nur wegen des anhängigen Abgabenstrafverfahrens bei der Sicherheitsbehörde bekannt und weder im Strafregister noch im KPA eingetragen.

Im Februar 2009 verlangte der Beschwerdeführer die Löschung der ihn betreffenden erkennungsdienstlichen Daten, die mit Bescheid vom Juni 2009 von der Beschwerdegegnerin abgewiesen wurde. Der dagegen erhobenen Berufung hat die Bundesministerin keine Folge gegeben.

Rechtliche Würdigung

§ 90 SPG räumt iVm § 31 Abs. 2 DSG 2000 dem Betroffenen grundsätzlich auch gegen sicherheitspolizeiliche Datenverwendung die gleichen Beschwerderechte wie gegen andere Datenverwendung durch Auftraggeber des öffentlichen Bereichs ein. Eine Ausnahme ist die Löschung erkennungsdienstlicher Daten auf Antrag des Betroffenen wegen *nachträglichen* Wegfalls der Ermittlungsgründe (etwa nach einem Freispruch oder einer Verfahrenseinstellung), für die die §§ 74 Abs. 1 und 76 Abs. 6 und 7 SPG ein eigenes Bescheidverfahren mit ausdrücklich geregeltem Instanzenzug vorsehen (1. Instanz: örtlich zuständige Sicherheitsdirektion, 2. Instanz: Bundesminister für Inneres).

Daraus folgt, dass die datenschutzrechtliche Beschwerde zur Durchsetzung des Rechts auf Löschung erkennungsdienstlicher Daten nur so weit zulässig bzw. die DSK in diesem Fall nur so weit zuständig ist, als über die *ursprüngliche* Zulässigkeit der Da-

tenermittlung zu erkennen ist (aus der sich eine amtswegige Löschungspflicht ergeben und welche im Fall eines Löschungsantrags nach §§ 74 ff SPG als Vorfrage von Relevanz sein kann).

Die ursprüngliche Zulässigkeit war hier zu bejahen: Anlasstat für die Ermittlung erkennungsdienstlicher Daten war der Vorwurf der versuchten Erpressung nach §§ 15, 144 Abs. 1 StGB, gemäß § 17 StGB ein Verbrechen, jedenfalls aber ein »gefährlicher Angriff« im Sinne des § 16 Abs. 2 Z 1 SPG. Dieser Verdacht stand im Zusammenhang mit dem bereits gerichtsanhängigen Vorwurf der gewerbsmäßigen Abgabenverkürzung. Da Erpressung als Tatbild zwingend die Kommunikation mit dem Tatopfer (Schreiben und Versenden von Briefen, E-Mails oder Telefaxen, Telefonanrufe etc.) umfasst, erscheint eine erkennungsdienstliche Behandlung (einschließlich DNA-Untersuchung) als geeignet, ein Wiedererkennen des Beschwerdeführers als Täter zu erleichtern und damit eine abschreckende Wirkung zu entfalten, da »seine Wiedererkennung auf Grund der ermittelten genetischen Information« (etwa durch biologische Spuren auf Briefkuverts) oder durch seine Fingerabdrücke ermöglicht wäre. Die Beschwerde war daher als unbegründet abzuweisen.

e. Löschung von Daten aus der zentralen Evidenz (BMF) (K121.641/0002-DSK/2011, 21. 1. 2011)

Sachverhalt

Die Beschwerdeführerin (ein Unternehmen aus der Baubranche) behauptet in ihrer rechtsanwaltlich eingebrachten Beschwerde eine Verletzung im Recht auf Löschung dadurch, dass der Beschwerdegegner (Bundesministerium für Finanzen, Zentrale Koordinationsstelle für die Bekämpfung illegaler Beschäftigung) ihr Löschungsbegehren betreffend zwei in der Zentralen Evidenz erfassten, jedoch schon im ordentlichen Verfahren der ersten Instanz gemäß § 45 Abs. 1 Z 2 VStG eingestellten (bestimmt bezeichneten) Verwaltungsstrafverfahren einer Bezirkshauptmannschaft zwar begründet, jedoch zu Unrecht abgelehnt habe. Da die betreffenden Vorfälle Jahre zurück lägen und für die Vollziehung des AuslBG durch die Beschwerdegegnerin nicht erforderlich seien, eine weitere Dokumentation für die Beschwerdeführerin überdies nachträglich sei, gebe es keinen Grund für die weitere Verarbeitung dieser Daten.

Der Beschwerdegegner verarbeitet in der Zentralen Evidenz verwaltungsbehördlicher Strafverfahren gemäß § 28b Abs. 3 AuslBG zur Beschwerdeführerin bestimmte Daten betreffend zwei rechtskräftig eingestellte Verwaltungsstrafverfahren, die mit Status »ruhend/aufgehoben« versehen sind. Das entsprechende Löschungsbegehren der Beschwerdeführerin lehnte der Beschwerdegegner insbesondere mit der Begründung ab, auch aus einer »freisprechenden« Entscheidung könnte sich die Notwendigkeit einer Dokumentation des Verfahrens ergeben.

Rechtliche Würdigung

Die DSK sah die Beschwerde aus folgenden Gründen als berechtigt an: Der Beschwerdegegner übersah bei seinen Ausführungen, dass hier nicht die Frage der Dokumentation eines bestimmten Verwaltungsstrafverfahrens gegenständlich ist (welche die DSK in anderem Zusammenhang – Strafverfahren – als rechtmäßig angesehen hat) – dies beträfe hier die Akten der Bezirkshauptmannschaft zu den jeweiligen Aktenzahlen –, sondern die Frage der Rechtmäßigkeit der Datenverarbeitung für Zwecke der besonderen, in einer gesetzlichen Spezialvorschrift geregelten Zentralen Evidenz. Der Sachverhalt dieses Verfahrens unterscheidet sich außerdem von jenem, der der einzigen bereits vorliegenden Entscheidung der DSK zur »Zentralen Evidenz« gemäß § 28b Abs. 3 AuslBG zugrunde lag (K121.554/0002-DSK/2010, 24. 2. 2010), da hier Daten zu nicht rechtskräftig gewordenen Bestrafungen gegenständlich sind.

Aus § 28b Abs. 4 AuslBG ergibt sich nämlich, dass nur rechtskräftige Bescheide an den Beschwerdegegner übermittelt und die daraus ermittelten Daten für Zwecke der Zentralen Evidenz verarbeitet werden dürfen. Daraus folgt, dass Daten zu nicht rechtskräftigen Bestrafungen, etwa während einer anhängigen Berufung oder nach dem

Einspruch gegen eine Strafverfügung, gar nicht Bestandteil der Datenanwendung werden dürfen. Entscheidungen, deren Rechtskraft nachträglich beseitigt wird (etwa in Folge einer erfolgreichen höchstgerichtlichen Beschwerde), sind folgerichtig aus der Zentralen Evidenz zu löschen.

Zweck der Zentralen Evidenz ist nämlich (trotz der missverständlichen Formulierung in § 28b Abs. 3 AuslBG) nicht die Dokumentation von Strafverfahren, sondern von rechtskräftigen, daher im Sinne von § 28b Abs. 1 AuslBG für die Auskunftserteilung relevanten Bestrafungen. § 28b Abs. 3 AuslBG sieht ein auf einen bestimmten Verfahrensbereich beschränktes verwaltungsstrafrechtliches Pendant zum gerichtlichen Strafregister, jedoch kein Pendant zur Evidenz gemäß § 57 Abs. 1 Z 6 SPG (»kriminalpolizeilicher Aktenindex«) vor. Dies ergibt sich aus Abs. 4 leg cit., mit welchem die Verwaltungsstrafbehörden, die allein die Möglichkeit haben, die Rechtskraft einer Bestrafung zuverlässig zu prüfen, zur Übermittlung von »Ausfertigungen rechtskräftiger Bescheide, die sie in Strafverfahren gemäß § 28 Abs. 1 Z 1 erlassen haben« angewiesen und ermächtigt werden, nicht jedoch zur Übermittlung von Daten betreffend jedes anhängige Verwaltungsstrafverfahren wegen Übertretung des AuslBG schlechthin. Jede andere Auslegung der zitierten Bestimmungen wäre im Lichte von § 1 Abs. 2 DSG 2000 mangels klarer gesetzlicher Determinierung in Bezug auf deren Grundrechtskonformität fragwürdig und nicht verfassungskonform.

Somit hätte schon die Verarbeitung der Daten zu den beiden in Beschwerde gezogenen, nicht-rechtskräftigen Strafbescheiden gemäß § 7 Abs. 1 DSG 2000 nicht erfolgen dürfen, da die Grenzen der gesetzlichen Ermächtigung nicht beachtet wurden. Jedenfalls wäre aber dem Löschungsbegehren gemäß § 27 Abs. 1 Z 2 DSG 2000 unverzüglich zu entsprechen gewesen. Im Übrigen ist auf die Tilgungsfrist gemäß § 55 Abs. 1 VStG zu verweisen, die – unbeschadet der Auskunftsregelung gemäß § 28b Abs. 2 AuslBG – auch für Zwecke der Zentralen Verwaltungsstrafevidenz zu beachten ist.

f. Zuständigkeit bei Löschung erkennungsdienstlicher Daten – Teil 2 (K121.650/0002-DSK/2011, 18. 2. 2011)

Sachverhalt

Die Beschwerdeführerin behauptet in ihrer ursprünglich an einen Unabhängigen Verwaltungssenat (UVS) gerichteten, teilweise auf die Zuständigkeit nach § 90 SPG gestützten, vom UVS diesbezüglich an die DSK weitergeleiteten, in der Folge auch verbesserten Beschwerde eine Verletzung im Recht auf Geheimhaltung dadurch, dass sie im Zuge einer kriminalpolizeilichen Amtshandlung nach Erlassung eines Ladungsbescheids, jedoch ohne vorheriges strafgerichtliches Urteil im März 2010 durch Organe der Beschwerdegegnerin (Bundespolizeidirektion) gegen ihren Willen und »passiven Widerstand« erkennungsdienstlich behandelt und so in die »Verbrecherkartei« aufgenommen worden sei. In eventu verstoße die Datenermittlung als Beweismittelgewinnung für Zwecke eines Strafverfahrens auch gegen das verfassungsrechtliche Gebot, eine Beschuldigte nicht zur Selbstbelastung zu drängen.

Im gegenständlichen Ermittlungsverfahren wegen strafrechtlicher Vorwürfe durch die Kriminalpolizei ersuchte das Landeskriminalamt die Beschwerdegegnerin, als Sicherheitsbehörde erster Instanz zuständig für den Wohnort der Beschwerdeführerin, die erkennungsdienstliche Behandlung der Beschwerdeführerin anzuordnen und durchzusetzen, da diese anlässlich ihrer Beschuldigtenvernehmung nicht zur freiwilligen Mitwirkung bereit war und auf eine bescheidmäßige Ladung bestanden hatte. Die Beschwerdegegnerin erließ daraufhin (auf dem Formular 2 zu § 19 AVG gemäß § 1 Abs. 2 VwFormV) einen als »Ladungsbescheid« bezeichneten Bescheid, in dem sie, gestützt auf die §§ 65 Abs. 1 und 4 sowie 77 Abs. 2 SPG das Erscheinen der Beschwerdeführerin zur erkennungsdienstlichen Behandlung unter Androhung sonstiger zwangsweiser Vorführung verfügte. Dieser Ladungsbescheid wurde nicht bekämpft.

Die Beschwerdeführerin erschien zum Termin und ließ sich, nach erfolgter Ankün-

digung, »passiven Widerstand« leisten zu wollen und der Ankündigung des Leiters der Amtshandlung, die Behörde sei berechtigt, die erkennungsdienstliche Behandlung auch durch angemessene Zwangsgewalt durchzusetzen, in der Weise erkennungsdienstlich behandeln, dass sie die Abnahme ihrer Sonnenbrille, das Ausziehen der getragenen Handschuhe, die Abnahme der Finger- und Handflächenabdrücke, das Fotografieren sowie die Abnahme der Körpermaße (Messung der Körpergröße) auf Aufforderung passiv duldete. Ermittelt und für Zwecke der Zentralen Informationssammlung der Sicherheitsbehörden (EKIS-EDE und AFIS) automationsunterstützt verarbeitet worden sind neben der Körpergröße und der allgemeinen Personenbeschreibung die Fingerabdrücke aller zehn Finger, Handflächenabdrücke sowie drei Lichtbilder (Profil, En Face, Halbprofil).

Rechtliche Würdigung

Die DSK hielt fest, dass hier ein Fall einer durch Bescheid auferlegten erkennungsdienstlichen Behandlung vorliegt. Da es sich um einen Ladungsbescheid gemäß § 77 Abs. 3 SPG iVm § 19 Abs. 3 und 4 AVG gehandelt hat, war dagegen ein ordentliches Rechtsmittel unzulässig. Die Vorführung der Beschwerdeführerin und die Durchsetzung der erkennungsdienstlichen Behandlung durch Zwangsgewalt wären evtl. als Vollstreckungsmaßnahme zulässig gewesen. Zwar waren Zwangsmaßnahmen wie die Anwendung von Körperkraft nicht erforderlich, die Beschwerdeführerin beugte sich der Aufforderung zur Duldung der erkennungsdienstlichen Behandlung jedoch nach eigener, unbestrittener Darstellung nur aufgrund der Ankündigung bzw. Androhung, dass die Durchsetzung der erkennungsdienstlichen Behandlung durch angemessene Zwangsausübung erfolgen könne.

Im Sinne der Judikatur des VwGH liegt hier eine Maßnahme unmittelbarer behördlicher Befehls- und Zwangsgewalt vor (vgl. etwa das Erkenntnis vom 23. 1. 2007, 2005/06/0254: »Schon der Fall, dass sich der Betroffene weigert, der Aufforderung zur Durchführung einer erkennungsdienstlichen Behandlung Folge zu leisten, und ihm darauf angedroht wird, dass er gemäß § 77 Abs. 4 SPG zu einer solchen Behandlung vorgeführt wird, stellt die Ausübung unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt dar«). Wenn also bereits die Androhung der Vorführung einen Akt der Befehls- und Zwangsgewalt bilden kann, so muss hier die Ankündigung der Ausübung von Zwang durch einen anwesenden Vertreter der Behörde nach Erlassung eines Ladungsbescheides (mit Androhung der Vorführung) und der Ankündigung der Betroffenen, »passiven Widerstand« gegen die Ihrer Meinung nach unberechtigte Maßnahme zu leisten, zumindest als Ausübung von unmittelbarer behördlicher Befehlsgewalt gedeutet werden, deren Beurteilung gemäß § 90 SPG der Zuständigkeit der DSK entzogen ist. Die Beschwerde war daher zurückzuweisen, da eine Weiterleitung gemäß § 6 Abs. 1 AVG an den unmittelbar angerufenen UVS nicht mehr infrage kommt, und die Beschwerdeführerin die Entscheidung der DSK in dieser Sache ausdrücklich beantragt hat.

g. Unterlassung einer Löschungsmitteilung (K121.705/0010-DSK/2011, 24. 8. 2011)

Sachverhalt

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Löschung dadurch, dass ihm die Beschwerdegegnerin (eine Sicherheitsdirektion) auf sein Löschungsbegehren vom Dezember 2010 hin binnen gesetzlicher Achtwochenfrist weder eine Löschungsmitteilung noch eine begründete Ablehnung seines Löschungsbegehrens übermittelt habe. Die Beschwerdegegnerin meinte dagegen, das Löschungsbegehren sei niemals bei ihr eingelangt, inhaltlich sei es auch abzulehnen.

Das in dieser Angelegenheit der Beschwerdegegnerin unterstehende Landeskriminalamt führte in den Jahren 2008 und 2009 ein Ermittlungsverfahren (u. a.) gegen den Beschwerdeführer im Zusammenhang mit dessen Pornofilmproduktion. Mit Urteil des Landesgerichts Linz im August 2009

wurde der Beschwerdeführer von allen Vorwürfen rechtskräftig freigesprochen. Betreffend seine Person und das gegenständliche Ermittlungsverfahren werden von der Beschwerdegegnerin auch keine Daten mehr in der zentralen Informationssammlung der Sicherheitsbehörden verarbeitet. Neben den Daten im PAD (z. B. Ermittlungsverfahren) besteht ein inhaltlich ergänzender Papierakt zum Ermittlungsverfahren.

Der Beschwerdeführer richtete anwaltlich vertreten im Dezember 2010 ein Löschungsbegehren an die Beschwerdegegnerin. Darin verlangte er »sämtliche zur Person des A im Zusammenhang mit den oa sicherheitsbehördlichen Ermittlungen (automationsunterstützt oder nicht automationsunterstützt) verarbeitete Daten, insb. im KPA, in den Allgemeinen Protokollen (wie PAD) und in den entsprechenden Erhebungsakten, zu löschen und den A, zu Handen seines ausgewiesenen Vertreters, hievon zu verständigen.«

Dieses Löschungsbegehren wurde am 24. Dezember 2010, 1:54 Uhr, als Telefax an die im Briefkopf der Beschwerdegegnerin angegebene Faxnummer gesendet. Die Sendung wird im Faxjournal der Kanzlei des Beschwerdeführervertreters als »fertig gestellt« ausgewiesen. Das Löschungsbegehren ist daher bei der Beschwerdegegnerin eingelangt, wurde aber in der Folge nicht beantwortet.

Rechtliche Würdigung

Die Beschwerde war teilweise berechtigt. Auch wenn das Löschungsbegehren in den frühen Morgenstunden eines für das Kanzleipersonal arbeitsfreien Tages bei der Beschwerdegegnerin eingelangt ist, so betrifft dies höchstens den Zeitpunkt des Einlangens, hat jedoch keinen Einfluss auf die Tatsache, dass der Beschwerdeführer als Absender darauf vertrauen durfte, dass die technisch übermittelte Faxsendung als Anbringen gemäß § 13 Abs. 1 AVG auch einer Erledigung gemäß § 18 Abs. 2 leg cit. zugeführt werde. Jede weitere Gebarung mit dem Eingangsstück, etwa dessen Ausdruck (bei einem papierlosen Faxeingang) und dessen Registrierung und Protokollierung, fiel in die Verantwortungssphäre der Beschwerdegegnerin. Durch die Nichtreaktion hat sie den Beschwerdeführer jedenfalls in seinem Recht gemäß § 27 Abs. 4 DSG 2000 verletzt. Ein Vorbringen im Verfahren vor der DSK nur dieser gegenüber vermag die nach § 27 Abs. 4 DSG 2000 gebotene Mitteilung von der Löschung bzw. die begründete Verweigerung der Löschung nicht zu ersetzen, auch wenn der Beschwerdeführer im Weg des Parteiengehörs davon Kenntnis erlangt.

Da die Beschwerdegegnerin den Standpunkt vertrat, (weitere) Datenlöschungen, insbesondere der PAD-Dokumentation, verweigern zu können, konnte zur Hauptfrage des Löschungsrechts von Dokumentationsdaten (Papierakt, äußere und innere PAD-Daten) auf die gesicherte Rechtsprechung der DSK (z. B. Bescheid vom 20. März 2009, GZ: K121.453/0003- DSK/2009, und vom 24. September 2010, GZ: K121.626/0016-DSK/2010), wonach die Sicherheitsbehörden im Aufgabengebiet der Kriminalpolizei im überwiegenden öffentlichen Interesse berechtigt sind, Daten zu einem Ermittlungsverfahren auch über dessen Beendigung hinaus zu dokumentieren, verwiesen werden. Hinsichtlich von Papierakten besteht überhaupt kein auf das DSG 2000 gründbares Recht auf Löschung. Die Beschwerdegegnerin konnte sich in dieser Frage aber auch zu Recht auf die §§ 74 f StPO stützen. § 75 StPO regelt als Spezialbestimmung zu den allgemeinen Vorschriften des DSG 2000 (vgl. § 74 Abs. 1 StPO) die Frage der höchstzulässigen Löschungsfristen von automationsunterstützt für Zwecke (u. a.) kriminalpolizeilicher Ermittlungsverfahren verarbeiteten Daten. Da keine der in § 75 Abs. 2 und 3 StPO festgelegten Fristen bereits abgelaufen war, hätte die Beschwerdegegnerin das Löschungsbegehren des Beschwerdeführers auch hinsichtlich der in der StPO geregelten Aspekte der PAD-Dokumentation zu Recht ablehnen können, da ein weiterhin bestehendes öffentliches Interesse an der Dokumentation des Verfahrens zu berücksichtigen war.

Dieser Bescheid wurde beim Verwaltungsgerichtshof angefochten, die Be-

schwerde aber abgewiesen. Weiters wurde dieser Bescheid beim Verfassungsgerichtshof angefochten. Das Verfahren ist anhängig.

h. Disposition über Datenverwendung im AMS (K121.722/0008-DSK/2011, 30. 9. 2011)

Sachverhalt

Die Beschwerdeführerin behauptet eine Verletzung in den Rechten auf Geheimhaltung, Richtigstellung und Löschung personenbezogener Daten durch verschiedene Ermittlungsschritte einer Regionalgeschäftsstelle (RGS) des Arbeitsmarktservice (AMS) eines Bundeslandes (Beschwerdegegner). Sie sei arbeitslos, und die RGS sperre ihr wegen des Verdachts, in einer Lebensgemeinschaft (mit ihrem Unterkunftgeber/Wohngemeinschaftspartner) zu leben, die Notstandshilfe, »nötige« sie, sich ein Kfz anzuschaffen oder in eine weniger abgelegene Gegend zu übersiedeln, um ihre Chancen bei der Jobsuche zu erhöhen, oder Kurse zu besuchen. Auch ihr Unterkunftgeber (Vermieter) sei genötigt worden, vor dem AMS auszusagen, weiters habe man von ihr die Bekanntgabe von Daten zur Bezahlung von Strom und Versicherungen (von wem, von welchem Konto?) für ihre Unterkunft verlangt. Ein Löschungs- bzw. Richtigstellungsbegehren von Daten wurde allerdings weder in der Beschwerde, noch in den verschiedenen Beilagen ausdrücklich erwähnt.

Im Jänner 2011 hat die Beschwerdeführerin der weiteren Verwendung und Übermittlung ihrer persönlichen Daten an »AMS- und Subunternehmen« und »diverse sonstige Vereine und Institutionen« widersprochen. Eine konkrete Zuweisung der Beschwerdeführerin zu Schulungs- oder Weiterbildungsmaßnahmen im Zuge der Betreuung durch den Beschwerdegegner ist nicht dokumentiert.

Anfang März 2011 wurde der Beschwerdeführerin eine Bewerbung um eine Stelle als Call Center-Mitarbeitern bei einer Firma aufgetragen, die jedoch nach einem Vorstellungstermin nicht zustande kam. Im zeitlichen Vorfeld wurde sie einmal aufgefordert, eine Übersiedlung oder die Anschaffung eines Pkw in Erwägung zu ziehen, da die schlechte Erreichbarkeit ihres Wohnorts mit öffentlichen Verkehrsmitteln ihre Vermittelbarkeit auf dem Arbeitsmarkt beschränke.

In einem behördlichen Ermittlungsverfahren in Vollziehung des AlVG überprüfte der Beschwerdegegner von Amts wegen jedenfalls seit März 2011 das Bestehen einer Lebensgemeinschaft zwischen der Beschwerdeführerin und dem an gleicher Adresse wohnhaften A. Mit Schreiben aus März 2011 wurde sie von der RGS nach Einstellung der Zahlung von Notstandshilfe aufgefordert, zwecks »Abklärung der Lebensgemeinschaft« einen Mietvertrag für ihre Unterkunft vorzulegen (laut Inhalt einer bei der RGS aufgenommenen Niederschrift aus März 2011, auf der die Beschwerdeführerin die Unterschrift nicht geleistet hat, bestehe ein Untermietvertrag, dessen Inhalt sei jedoch »vertraulich«).

Rechtliche Würdigung

Geheimhaltung: Was das Vorbringen der Beschwerdeführerin angeht, der Beschwerdegegner greife durch ein behördliches Ermittlungsverfahren betreffend Bestehen und Umfang ihrer Leistungsansprüche nach dem AlVG (Notstandshilfe) in ihr Recht auf Geheimhaltung ein, so ist darauf zu verweisen, dass datenschutzrechtliche Beschwerden nicht geeignet sind, in der Sache vor andere Behörden gehörende Rechtsfragen prüfen zu lassen. Grundsätzlich besteht ein – im Fall eines allgemeinen Verwaltungsverfahrens durch die §§ 37 und 39 Abs. 2 AVG sowie besondere Zuständigkeitsbestimmungen zum Ausdruck kommendes – berechtigtes Interesse der zuständigen Behörde an der Verwendung personenbezogener Daten, insbesondere deren Ermittlung, für Zwecke eines Verwaltungsverfahrens, welches das Interesse der Betroffenen an der Geheimhaltung ihrer personenbezogenen Daten überwiegt, sodass im Allgemeinen schon gem §§ 7 Abs. 1 und 8 Abs. 1 Z 4 DSG 2000 eine Verletzung von nach § 1 Abs. 1 leg cit. bestehenden schutzwürdigen Geheimhaltungsinteressen nicht vorliegt. Als Maßstab für eine Beurteilung der Zulässigkeit der Datenermittlung in solchen Verfahren ver-

bleibt für die DSK das Übermaßverbot als Ausdruck des in § 1 Abs. 2 und § 7 Abs. 3 DSG 2000 normierten Verhältnismäßigkeitsgrundsatzes: Wenn es denkmöglich ist, dass die von einer in der Sache zuständigen Behörde ermittelten Daten nach Art und Inhalt für die Feststellung des relevanten Sachverhalts geeignet sind, ist die Zulässigkeit der Ermittlung aus datenschutzrechtlicher Sicht gegeben (vgl. u. a. den Bescheid vom 29. November 2005, GZ: K121.046/0016-DSK/2005).

Die DSK ist auch nicht dafür zuständig, bestimmte behauptet unrechtmäßige Entscheidungen (Androhung oder tatsächliche Sperre der Notstandshilfe) zu überprüfen.

Im vorliegenden Fall ermächtigt § 25 Abs. 1 Z 3 lit a AMSG den Beschwerdegegner überdies sogar ausdrücklich, Daten zum »Familienstand (einschließlich Lebensgemeinschaft)« eines Arbeitsuchenden zu verarbeiten. Dies offenkundig unter dem teleologischen (an Ziel und Zweck des Gesetzes zu messenden) Gesichtspunkt, dass das Bestehen einer Lebensgemeinschaft einen für die Vollziehung des AlVG bedeutenden Tatbestand bildet, da gem §§ 36 Abs. 2 und Abs. 3 lit B sublit a AlVG die wirtschaftlichen Verhältnisse eines Lebensgefährten der Beschwerdeführerin in die Beurteilung der Frage, ob sie sich in einer objektiven »Notlage« befindet bzw. ob ein ungeminderter Leistungsanspruch auf Notstandshilfe besteht, einzubeziehen wären. Ausdrückliche behördliche Ermächtigungen in diesem Zusammenhang, etwa zur Ermittlung von Einkommensdaten beim Betroffenen wie bei Dritten, finden sich in § 36c AlVG. Die Beschwerde war diesbezüglich unbegründet.

Löschung/Richtigstellung von Urkunden: unabhängig davon, ob die Beschwerdeführerin ein als solches erkennbares Anbringen gem § 27 Abs. 1 Z 2 DSG 2000 überhaupt gestellt hat, war sie auf den Wortlaut der Verfassungsbestimmung § 1 Abs. 3 Z 2 DSG 2000 zu verweisen, wonach ein Richtigstellungs- und Löschungsrecht nur für automationsunterstützt oder in einer manuellen Datei verarbeitete Daten besteht, nicht jedoch für Urkundeninhalte (vgl. den Bescheid vom 10. November 2000, GZ: 120.707/7-DSK/00).

Widerspruch gegen Datenüberlassung an Dienstleister des AMS: ein solcher ist gem § 28 Abs. 1 Satz 1 DSG 2000 jedenfalls unwirksam, soweit die Verwendung der Daten gesetzlich vorgesehen ist. Die Heranziehung von Vertragspartnern, Unternehmen, Vereinen, externen Institutionen etc., für Aufgaben der Schulung, Information und Beratung von Arbeitsuchenden stellt überdies ein Dienstleisterverhältnis letzterer zum AMS gem § 32 Abs. 2 AMSG dar. Es handelt sich beim Zurverfügungstellen von Daten daher um eine Überlassung (§ 4 Z 11 DSG 2000) von personenbezogenen Daten, die den Dienstleister verpflichtet, die Daten nur für Zwecke der von ihm zu erbringenden Leistung (etwa die Organisation von Schulungskursen), nicht jedoch für eigene Zwecke zu verwenden. Gegen eine Überlassung von Daten ist kein Widerspruch möglich. Auch hier war die Rechtsverletzung nicht gegeben.

Übermittlung der Daten an potenzielle Arbeitgeber im Rahmen der Stellenvermittlung: Die Übermittlung von Daten an potenzielle Arbeitgeber, bei denen sich zu bewerben der Beschwerdeführerin aufgetragen wurde, kann sich auf die ausdrückliche Ermächtigung gem § 6 Abs. 3 AMFG stützen. Ein entgegenstehender Sperrvermerk wurde weder behauptet noch ist ein solcher im Ermittlungsverfahren hervorgekommen.

6.2 Kontrollverfahren nach § 30 DSG 2000

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

Bei vorabkontrollpflichtigen Daten-

anwendungen kann ein solches auch ohne Vorliegen einer Eingabe oder auch nur eines konkreten Verdachts durchgeführt werden. Die Durchführung eines solchen Verfahrens ist (anders als beim Beschwerdeverfahren) unabhängig vom geltend gemachten Recht (Pflicht) bzw. dem angesprochenen Auftraggeber zulässig, und zwar auch dann, wenn die DSK alternativ auch zur förmlichen Rechtsdurchsetzung zuständig wäre.

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

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

a. Google Street View (K213.051//0004-DSK/2011, 15. 4. 2011)

Sachverhalt

»Google Street View« ist ein Dienst von Google Inc., der ausgehend von »Google Maps« (Landkarten) Straßenansichten im Internet zugänglich macht. Dies soll dem Benutzer erlauben, für ausgewählte Städte durch Anklicken des Straßenzuges auf einer Straßenkarte oder Eingabe einer Adresse in »Google Maps« eine 360-Grad-Ansicht der Örtlichkeit zu erhalten. Bei den im Internet sichtbaren Bildern handelt es sich um Momentaufnahmen und nicht etwa um Bilder aufgrund einer Live-Verbindung zum dargestellten Ort. Die im Internet gezeigten Bilder müssen daher mit der jeweils aktuellen Situation am dargestellten Ort nicht übereinstimmen.

Google Inc. hat die Datenanwendung »Google Street View« zu DVR 4000437 beim Datenverarbeitungsregister am 20. März 2009 gemeldet. Aus dem öffentlichen Raum werden von mit einer speziellen Kamera ausgestatteten Fahrzeugen aus einer Höhe, die über der durchschnittlichen Körpergröße eines Menschen liegt, digitale Bildaufnahmen angefertigt. Die Fahrzeuge sind deutlich gekennzeichnet. Die Aufnahmen erfolgen zu zwei separaten Zwecken: zum Zwecke der Erstellung und Verbesserung von Kartenmaterial (u. a. für Navigationsgeräte) und zum Zwecke der Einbindung in die Funktion »Street View«. Bei der Funktion »Street View« geht es allein um die Darstellung des öffentlichen Raumes und nicht um die Abbildung von Personen oder Kraftfahrzeugen, die sich bei der Anfertigung der Aufnahmen allerdings nicht vermeiden lässt. Vor der Einbindung wird das Bildmaterial daher technisch bearbeitet. Dabei wird insbesondere eine Technologie eingesetzt, welche die Funktion hat, Gesichter von Passanten und Autokennzeichen automatisch zu erkennen und diese unkenntlich zu machen. Die Bilddaten werden erst nach Bearbeitung veröffentlicht, die zugrunde liegenden Klaraufnahmen bleiben zum Zwecke der Kartenerstellung weiter gespeichert. Sobald eine Aufbewahrung der Klaraufnahmen nicht mehr zur Erreichung dieses Zweckes erforderlich ist, werden die Gesichter und KFZ-Kennzeichen, die in den in der Funktion »Street View« veröffentlichten Aufnahmen erkennbar sind, irreversibel mittels der oben beschriebenen Technologie unkenntlich gemacht.

Zudem stellt die Auftraggeberin eine Funktion zur Verfügung, mit der Nutzer – nach Veröffentlichung – einzelne Bilder aus der Funktion »Street View« melden können, die dann nach Prüfung ggf. weiter unkenntlich gemacht werden.

Rechtliche Würdigung

Die DSK hat die Datenanwendung registriert und – neben den schon von der Auftraggeberin im Meldeverfahren zugesagten Bedingungen des Betriebs – folgende Empfehlungen gemäß § 30 Abs. 6 DSG 2000 erteilt:

a. Bei Aufnahmen von Personen in besonders sensiblen Bereichen sind jedenfalls nicht nur die Gesichter, sondern auch die Gesamtbilder der Personen

unkenntlich zu machen. Dazu zählen insbesondere die Eingangsbereiche von Kirchen, Gebetshäusern, Krankenhäusern, Frauenhäusern und Gefängnissen.

b. Bildaufnahmen privater, für einen Spaziergänger nicht einsehbarer Immobilien, wie insbesondere umzäunter Privatgärten und -höfe, sind vor einer Veröffentlichung im Internet unkenntlich zu machen.

c. Gemäß § 28 Abs. 2 DSG 2000 steht dem Betroffenen ab dem Zeitpunkt der Ermittlung der Daten ein Widerspruchsrecht zu. Um den Betroffenen auch vor Veröffentlichung der Bilddaten diese Möglichkeit zum Widerspruch gegen die Veröffentlichung von Gebäuden einzuräumen, sind geeignete Werkzeuge zur Verfügung zu stellen, die ein einfaches und unbürokratisches Geltendmachen des Widerspruchrechts ermöglichen. Auf dieses (bereits vor Veröffentlichung bestehende) Widerspruchsrecht und das Werkzeug zur Ausübung des Widerspruchsrechts ist auch auf der Website der Google Inc. hinzuweisen.

Die Empfehlungen a. und b. sind bis spätestens zur Veröffentlichung der Daten im Internet umzusetzen, das Werkzeug sowie der Hinweis darauf gemäß Empfehlung c. sind mindestens zwölf Wochen vor Veröffentlichung der Daten im Internet zur Verfügung zu stellen.

Die in Empfehlung a. genannte »Auflage« dient dazu, den Auftraggeber zu verhalten, bei der Veröffentlichung von Bilddaten von Personen, die in den dort genannten »sensiblen« Bereichen (das sind solche Bereiche, in denen naturgemäß eine besondere Eingriffsintensität gegeben ist) aufgenommen wurden, jedenfalls eine völlige Anonymisierung zu gewährleisten. Dazu wird es notwendig sein, nicht nur eine automatische Unkenntlichmachung der Gesichter vorzusehen, sondern das gesamte Bild der Person mittels technischer Hilfsmittel unkenntlich zu machen.

Da die Auftraggeberin die Aufnahmen aus einer Höhe über der Durchschnittsgröße eines Menschen vornimmt, sind gemäß Empfehlung b. jene privaten Immobilien (z. B umzäunte private Gärten und Höfe) von einer Veröffentlichung auszunehmen, die normalerweise nicht einsehbar sind. Diesbezüglich kann nämlich nicht von einem die schutzwürdigen Interessen des Betroffenen überwiegenden Interesse der Öffentlichkeit ausgegangen werden.

Die Empfehlung c. dient der Umsetzung der sich aus § 28 Abs. 2 DSG 2000 ergebenden gesetzlichen Verpflichtung des Auftraggebers, begründungslos Widerspruchsbegehren von Betroffenen nachzukommen. Betroffen ist dabei grundsätzlich jeder, der entweder selbst als Person oder dessen Haus auf den Bilddaten zu erkennen ist. Das Widerspruchsrecht steht dabei bereits ab dem Ermittlungszeitpunkt (und nicht erst ab Veröffentlichung zu), weil die für die Datenanwendung »Google Street View« ermittelten Bilddaten (auch) der Veröffentlichung dienen, und ist (vor Veröffentlichung) auf Immobilien (Gebäude und Grundstücke) beschränkt, da ja andere personenbezogene Daten (wie Gesichter, KFZ-Kennzeichen etc.) nach den Vorgaben des Auftraggebers gar nicht Teil der öffentlich zugänglichen Datenanwendung sein sollen. In diesem Zusammenhang stellt die DSK fest, dass Immobilien, die auf deren Eigentümer, Mieter oder sonst nutzungsberechtigte Personen (sei es über das Grundbuch oder andere rechtlich zulässige Mittel) rückführbar sind, als personenbezogene Daten dieser genannten Personen zu werten sind. Auf das Widerspruchsrecht und das Werkzeug zur Geltendmachung eines Vorab-Widerspruches ist spätestens zum selben Zeitpunkt auf der Website hinzuweisen.

b. Verwendung von Bonitätsdaten

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

Häufig endeten die Fälle mit einer Löschung der Betroffenen aus einer Bonitätsdatenbank, wodurch jedenfalls ein recht-

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

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

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

c. Videoüberwachung

Eine zahlenmäßig sehr große Gruppe von Eingaben betraf Fragen der Videoüberwachung. Dies betraf die Zulässigkeit von Anlagen an sich, die Abgrenzung der überwachten Örtlichkeit (etwa im nachbarschaftlichen Bereich privater Wohnhäuser), aber auch die Erfüllung von Auftraggeberpflichten, wie der Melde- oder Kennzeichnungspflicht. Vermehrt hatte die Datenschutzkommission dazu das Instrument der Einschau in Datenanwendungen in Anspruch nehmen müssen, um etwa strittige Fragen betreffend Erfassungswinkel und Funktionsweise von Systemen zu klären. In der überwiegenden Zahl der Fälle war dabei – auch in als nicht friktionsfrei zu bezeichnenden Verhältnissen zwischen Einschreiter und Betreiber der Anlage – die Kooperationsbereitschaft der Betreiber äußerst positiv. In einigen Fällen waren Empfehlungen auszusprechen bzw. wegen Verletzung von Melde- und Kennzeichnungspflicht Verwaltungsstrafanzeigen zu erstatten.

Immer wieder hat die Datenschutzkommission in Verfahren nach § 30 DSG 2000 betreffend Videoüberwachung schwierige Auslegungsfragen betreffend die Zulässigkeit oder die Erfüllung von Auftraggeberpflichten zu lösen. So wurde etwa die Erfassung von Kennzeichen per Kamera zur Einfahrtskontrolle in Garagen als Videoüberwachung iSd § 50a Abs. 1 DSG 2000 gesehen, die nur dann registrierungsfähig ist, wenn eine konkrete Gefährdung durch so genannte gefährliche Angriffe, das sind idR gerichtlich strafbare Vorsatztaten, vorliegt. Die Einfahrtskontrolle auf diese Weise für Zwecke der reinen Besitzstörung ist nicht zulässig. Auch wurde etwa zur Kennzeichnungspflicht festgehalten, dass neben dem Informationsgedanken in der Praxis vom Auftraggeber nicht stets verlangt werden kann, dass die Kennzeichnung jedenfalls ein Ausweichen des überwachten Raumes ermöglichen muss, sondern nur, wo dies tunlich ist (vgl. dazu den Fall der Fassadenüberwachung eines Geschäftslokales mit angrenzendem/r Gehsteig oder Fußgängerzone).

d. Adressdaten

In Verfahren nach § 30 DSG 2000 war es der Datenschutzkommission auch möglich, unkompliziert und rasch die – in vielen Fällen durch den Einschreiter per direkter Korrespondenz bereits versuchten – Löschung von Adressdaten durchzusetzen. Die meist auf Basis einer früheren Zustimmungserklärung oder im Rahmen des Gewerbes des § 151 GewO (Adressverlag) erlangten Daten konnten so vor einer weiteren Verwendung bewahrt werden. In manchen Fällen hat sich hier die – gesetzlich nicht vorgesehene – Sperre gegenüber der physischen Löschung als vorteilhaft für die Betroffenen erwiesen, weil nur so sichergestellt werden konnte, dass der Auftraggeber die Daten auch bei späterer erneuter Ermittlung nicht weiter verwendet.

6.3. Genehmigungsverfahren für internationalen Datenverkehr

Im Berichtszeitraum bearbeitete die Datenschutzkommission wieder eine große Menge von Anträgen zur Erteilung von Genehmigungen für den Internationalen Datenverkehr (§ 13 DSG 2000) zu bearbeiten.

Wie im vorigen Berichtszeitraum waren die antragstellenden Unternehmen ausnahmslos Konzerngesellschaften. Die wichtigsten rechtlichen Fragen betrafen die Struktur der Konzerne. Viele Konzerne betreiben in Österreich nur sehr kleine Tochtergesellschaften, was den Wunsch nach zentraler Verwaltung von Personal- und Kundendaten durch die Konzernmutter zur Folge hat.

Ebenso organisieren viele Konzerne ihre Töchter in einer »Matrixorganisation« bei der Mitarbeiter der Töchter nicht nur ihren normalen Vorgesetzten im eigenen Unternehmen unterstellt sind, sondern auch für Vorgesetzte in anderen Tochterunternehmen im Ausland arbeiten sollen. Die Zuordnung erfolgt dabei nach den Erfordernissen für internationale Geschäftsabwicklung: Ein Mitarbeiter im Verkauf bei einer österreichischen Tochter ist dabei dem Verkaufschef der Konzernmutter in Übersee unterstellt, um Aufträge internationaler Großkunden zu bearbeiten. Die Matrixorganisation erlaubt es den Konzernen, ihre Töchter sehr viel effizienter einzusetzen als dies normalerweise der Fall wäre.

Die Matrixorganisation kann aber auch dazu führen, dass Personal- und Kundendaten weltweit verteilt werden. Dabei leiden vor allem die im Datenschutzgesetz 2000 vorgeschriebenen Prinzipien der Zweckbindung (§ 6 Abs. 1 Z 2 DSG 2000) und rechtlichen Befugnis des Empfängers (§ 7 Abs. 2 Z 2 DSG 2000). Die Rolle des Arbeitgebers als Auftraggeber für die Daten der Mitarbeiter tritt gegenüber den anderen Konzernunternehmen zurück. Dabei ist es der Arbeitgeber, der auf Grund des Arbeitsvertrages und der arbeitsrechtlichen Bestimmungen im Gesetz alle Rechte und Pflichten eines Auftraggebers gegenüber den Mitarbeitern wahrnimmt.

Das Problem, Matrixorganisationen im System des Datenschutzrechts angemessen darzustellen wird durch die Haltung mancher Konzerne, die unmittelbare Arbeitgeberrechte über die Mitarbeiter der Tochtergesellschaften ausüben wollen, nicht erleichtert, obwohl diese nur mit ihrem Arbeitgeber einen Arbeitsvertrag – und damit eine rechtliche Beziehung – haben. Rechtlich muss daher sichergestellt werden, dass auch bei der Kooperation mit anderen Konzernunternehmen, sei es bei projektbezogener Arbeit oder wie hier im Rahmen einer dauerhaften Matrixorganisation, die grundsätzlichen Rechte zur Verwendung der personenbezogenen Daten der Mitarbeiter beim Arbeitgeber verbleiben müssen.

Die Datenschutzkommission hat im Jahr 2011 eine erste Entscheidung gefällt, die speziell die Matrixorganisationen in Konzernen anspricht (Bescheid K178.414/0006-DSK/2011 vom 30. September 2011). Die Antragstellerin hat in einer Weisung an die Mitarbeiter klargestellt, dass der »funktional Vorgesetzte« innerhalb der Matrix zwar Weisungen erteilen kann, aber der Vorgesetzte in Österreich bei der Antragsstellerin immer die stärkere Befugnis hat. Auf Grund dieser Regelung wurde eine Genehmigung erteilt, aber das Thema ist noch lange nicht abgeschlossen.

6.4 Gesetzlicher Handlungsbedarf

6.4.1 Entlastung des DVR

Eines der Hauptprobleme der DSK stellt die permanente Überlastung des DVR dar. Die generelle Meldepflicht scheint insbesondere im Lichte der Vorschläge für den neuen Rechtsrahmen der EU, in denen die Meldepflicht grundsätzlich abgeschafft wird, anachronistisch und nicht zielführend. Aus Sicht der DSK ist es unbedingt notwendig, legistisch eine Entlastung des DVR vorzusehen. Da mit September 2012 DVR-Online operativ werden soll und die nicht der Vorabkontrolle unterliegenden Meldungen

dann ohnehin automatisiert erfolgen sollen, wäre vor allem eine Reduktion der vorabkontrollpflichtigen Datenanwendungen notwendig. Weiters wäre eine Lösung für die Bewältigung der Altlasten anzustreben. Im Übrigen wäre die Einführung weitere Standardanwendungen anzustreben.

6.4.2 Bonitätsinformation

Bei der DSK wurden im Berichtszeitraum einige Beschwerden bezüglich der Ermittlung und weiteren Verwendung von Kredit- und Bonitätsinformationen eingebracht. Wie bereits im letzten Datenschutzbericht angesprochen ist die DSK bei der Behandlung dieser Fälle zur Auffassung gelangt, dass in diesem Bereich, in dem nicht ordnungsgemäße Datenverwendung für die Betroffenen auch sehr wichtige wirtschaftliche Implikationen hat, gesetzlicher Handlungsbedarf besteht, soweit die anstehenden Probleme nicht durch Verhaltensregeln gemäß § 6 Abs. 4 DSG 2000 gelöst werden können: Es müssten die §§ 152 der GewO 1994 betr. »Auskunfteien über Kreditverhältnisse« und 118 über »Inkassoinstitute« – ähnlich wie dies bei § 151 GewO hinsichtlich der Adressverlage und Direktmarketingunternehmen geschehen ist – mit genaueren Regelungen über die Zulässigkeit der Ermittlung von Bonitätsdaten, insbesondere über die zulässigen Quellen, über die Pflichten der Auftraggeber zur Qualitätssicherung bei gespeicherten Bonitätsdaten, über die zulässige Speicherdauer und über die effiziente Durchsetzung der Betroffenenrechte, insbesondere Löschungsansprüche, angereichert werden. Der gegenwärtige Zustand ist jedenfalls nach wie vor von großer Rechtsunsicherheit geprägt, was zu den oben erwähnten Beschwerden an die DSK über die Datenverwendung in diesem Bereich geführt hat. Aus Sicht der DSK sollten daher die politischen Bestrebungen, hier eine entsprechende gesetzliche Regelung in Anspruch zu nehmen, (wieder) aufgenommen werden. Die DSK ist gerne bereit, ihr aus der Behandlung der Beschwerden erworbenes, spezielles Erfahrungswissen den für die Genehmigung von Verhaltensregeln bzw. für die Legistik zuständigen Ressorts zur Verfügung zu stellen.

6.4.3 Videoüberwachung

Wie bereits im vorigen Bericht erachtet es die DSK für notwendig, den Begriff der Videoüberwachung (§ 50a Abs. 1 DSG 2000) zu schärfen. Während nämlich die Materialien zur DSG-Novelle 2010, womit dieser Begriff eingeführt wurde, Einschränkungen bei der Erfüllung des Begriffes sehen, legt der Wortlaut nahe, dass unter Videoüberwachung sämtliche Bildverarbeitung bezogen auf ein Objekt bzw. eine Person zu verstehen ist, ganz unabhängig vom damit verbundenen Zweck. Da aber dem Gesetzgeber nicht unterstellt werden kann, dass er reine Infowebcams (Wetter, Disco, Christkindlmarkt etc.), aber auch Kameras, die als Mittel zum Zweck der reinen Zutrittskontrolle eingesetzt werden sollen, oder Kameras zur Produktionskontrolle in derselben Weise regeln wollte, wie Kameras, die zur Abwehr von gefährlichen Angriffen eingesetzt werden, wird angeregt, eine Zweckdefinition in der Begriff aufzunehmen. Konsequenz daraus wäre, dass Kameras, die zu dort nicht genannten Zwecken eingesetzt werden, nach den allgemeinen Regeln der §§ 6ff DSG 2000 zu beurteilen wären und nicht den Regeln des § 50a DSG 2000 unterlägen.

7 Internationale Zusammenarbeit mit anderen unabhängigen Datenschutz-Kontrollstellen

7.1 Allgemeines

Die Internationalen Datenschutzkonferenzen der letzten Jahre Jerusalem (2010) und Mexico City (2011) haben – wie schon die Konferenzen in den Vorjahren – vor allem die Globalisierung der Grundgedanken des Datenschutzes vorangetrieben. Auf der internationalen Datenschutzkonferenz in Madrid (2009) waren bereits Standards für einen weltweiten Datenschutz beschlossen worden, die allerdings »Soft law-Charakter« haben. Zugleich wies und weist der Europarat immer wieder darauf hin, dass die aus 1981 datierende Datenschutzkonvention des Europarates (ETS 108) auch Drittstaaten zum Beitritt offen steht. Dieses bereits bestehende rechtsverbindliche Instrument normiert Mindeststandards, die sukzessive auf die beitretenden Staaten ausgedehnt werden sollen.

Davon abgesehen stellte im Berichtszeitraum die Arbeit der Europäischen Kommission an einem komplett neuen Rechtsrahmen für den Datenschutz auf der Grundlage des Art. 16 AEUV ein die Datenschutzszene beherrschendes Thema dar. Am 25. Jänner 2012 wurden schließlich von der Europäischen Kommission der Öffentlichkeit Vorschläge für zwei Datenschutz-Rechtsinstrumente – eine Verordnung für den Bereich der ehemaligen »ersten Säule« und eine Richtlinie für den Bereich »Polizei und Justiz« präsentiert.

Auch der Europarat hat 2010 beschlossen, seine Datenschutzkonvention zu modernisieren und zu überarbeiten. Entsprechende Diskussionen finden im beratenden Ausschuss (sog. »T-PD«), der rechtlich auf der Konvention selbst basiert, statt.

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.

Die Art. 29 Gruppe wurde auch mit Fragen im Zusammenhang mit den neuen von der EU-Kommission entworfenen Datenschutzinstrumenten befasst.

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.

Wie oben angesprochen, wurde die Art. 29 Gruppe von der EU-Kommission im Berichtszeitraum gezielt zu verschiedenen Fragen betreffend die neuen Rechtsinstrumente um Stellungnahme gebeten, wobei diese Problembereiche (siehe dazu die »Advice papers« zu sensiblen Daten, Meldepflicht und Kooperation der Datenschutzbehörden) wiederum in Unter-Arbeitsgruppensitzungen diskutiert wurden.

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

a. Begriffe »für die Verarbeitung Verantwortlicher« und »Auftragsverarbeiter« (WP 169)
b. Werbung auf Basis von Behavioural Targeting (WP 171)
c. Grundsatz der Rechenschaftspflicht (»accountability principle« – WP 173)
d. Verhaltensregeln für FEDMA bezüglich Direktmarketing (WP 174)
e. Datenschutzniveau in der Republik Östlich des Uruguay (WP 177) und in Neuseeland (WP 182)
f. Fluggastdaten (WP 178. WP 181)
g. Anwendbares Recht (WP 179)
h. überarbeiteter Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen (WP 180)
i. Smart metering (WP 183)
j. Geolokationsdienste (WP 185)
k. Bekämpfung von Geldwäsche und Terroristenfinanzierung (WP 186)
l. Einwilligung (WP 187)
m. EASA/IAB Best Practice Empfehlung zu online-verhaltensorientierter Werbung (WP 188).

Sämtliche zitierten Arbeitspapiere können auf der Homepage der EU-Kommission nachgelesen werden.[10]

10 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_de.htm

In den Unter-Arbeitsgruppen wurden im Berichtszeitraum auch Vorarbeiten für einige wichtige Fragen geleistet, die erst 2012 – oder später – zum Abschluss gebracht werden konnten bzw. können, wie die Haltung der Art. 29 Gruppe zum grenzüberschreitenden Austausch von Gesundheitsdaten bei epSOS, zu zahlreichen technischen Themen wie cloud computing oder Sozialen Online-Netzen bzw. Themen wie biometrische Daten und E-Government. Weitere Untergruppen beschäftigen sich mit dem Datenschutz bei finanziellen Transaktionen und der Bewältigung der Globalisierung, etwa mittels verbindlicher unternehmensinterner Richtlinien (Binding Corporate Rules – BCRs) und der Entwicklung von ISO-Standards.

7.2.1 Zu einzelnen Themen von generellem Interesse

7.2.1.1 Grundsatz der Rechenschaftspflicht (»Accountability Principle«)

In dieser Stellungnahme nimmt die Art. 29-Gruppe zum so genannten »Accountability Principle« Stellung. Die Grundsätze des europäischen Datenschutzes und die damit verbundenen Verpflichtungen spiegeln sich häufig nur unzureichend in konkreten internen Maßnahmen und Praktiken wider. Wenn der Datenschutz nicht Teil der gemeinsamen Werte und Praktiken von Organisationen wird und die entsprechenden Zuständigkeiten ausdrücklich zugewiesen werden, kann eine effektive Einhaltung der Datenschutzvorschriften kaum noch gewährleistet werden und Datenschutzpannen sind weiterhin vorprogrammiert.

Wie in der Stellungnahme ausgeführt wird, müssen zur Stärkung des Datenschutzes in der Praxis im europäischen Rechtsrahmen zusätzliche Instrumente vorgesehen werden. Insbesondere wird ein »Grundsatz der Rechenschaftspflicht« vorgeschlagen, der die für die Verarbeitung Verantwortlichen (das sind die »Auftraggeber« iSd DSG 2000) verpflichten würde, angemessene und wirksame Maßnahmen zu ergreifen, um die Grundsätze und Verpflichtungen der Richtlinie umzusetzen, und dies gegenüber den Kontrollstellen auf Verlangen nachzuweisen.

Dies soll dazu beitragen, dass der Datenschutz von der Theorie zur Praxis übergeht, und die Datenschutzbehörden bei der Wahrnehmung ihrer Überwachungsaufgaben und der Durchsetzung der Rechtsvorschriften unterstützt werden. Die Stellungnahme enthält Vorschläge, wie gewährleistet werden kann, dass der Grundsatz der Rechenschaftspflicht Rechtssicherheit bietet und gleichzeitig anpassbar ist (d. h. die Festlegung der konkreten Maßnahmen je nach dem mit der Datenverarbeitung verbundenen Risiko und den Arten der verarbeiteten Daten ermöglicht). Als Maßnahmen werden z. B. die Bestellung von

Datenschutzbeauftragten, die Durchführung von Datenschutzverträglichkeitsprüfungen, interne oder externe Audits und die Aufstellung von Datenschutzstrategien genannt. Anschließend wird erörtert, wie sich dieser Grundsatz auf andere Bereiche, etwa Datenübertragungen in Drittländer, Meldepflichten, Sanktionen und letztlich auch die Entwicklung von Zertifizierungsprogrammen oder Gütesiegeln auswirken könnte.

7.2.1.2 Anwendbares Recht

In dieser Stellungnahme wird der Anwendungsbereich der Richtlinie 95/46/EG und insbesondere ihres Art. 4 präzisiert, der bestimmt, welche auf der Grundlage dieser Richtlinie erlassenen einzelstaatlichen Vorschriften auf die Verarbeitung personenbezogener Daten Anwendung finden. Des Weiteren wird auf bestimmte Bereiche eingegangen, in denen Raum für Verbesserungen besteht. Eine präzisere Bestimmung der Anwendung des EU-Rechts auf die Verarbeitung personenbezogener Daten dient auch dazu, den Anwendungsbereich des EU-Datenschutzrechts sowohl in der EU bzw. im EWR als auch im größeren internationalen Kontext zu klären. Eine klare Vorstellung davon, welches Recht zur Anwendung kommt, wird sowohl den für die Verarbeitung Verantwortlichen (= Auftraggeber iSd DSG 2000) als auch den Betroffenen und anderen Beteiligten mehr Rechtssicherheit vermitteln. Eine korrekte Auslegung der Vorschriften zum anwendbaren Recht dürfte überdies gewährleisten, dass der durch die Richtlinie 95/46 gebotene weit reichende Schutz personenbezogener Daten keine Rechtslücken oder Schlupflöcher aufweist.

Die Bezugnahme in Art. 4 Absatz 1 Buchstabe a auf »eine« Niederlassung bedeutet, dass sich das anwendbare Recht nach dem Mitgliedstaat bestimmt, in dem der für die Verarbeitung Verantwortliche eine Niederlassung besitzt; besitzt der Verantwortliche auch Niederlassungen in anderen Mitgliedstaaten, kann auch das Recht dieser Mitgliedstaaten zur Anwendung berufen werden. Für die Anwendung des nationalen Rechts kommt es darauf an, dass die Verarbeitungen im »Rahmen der Tätigkeiten« der Niederlassung ausgeführt werden. Dies bedeutet, dass die Niederlassung des für die Verarbeitung Verantwortlichen mit Tätigkeiten befasst ist, die sich auf die Verarbeitung personenbezogener Daten beziehen, wobei der Umfang dieser Verarbeitungstätigkeit, die Art der Tätigkeiten und die Notwendigkeit, einen wirksamen Datenschutz zu gewährleisten, zu berücksichtigen sind. In Bezug auf die Bestimmung in Art. 4 Absatz 1 Buchstabe c über die zum Zwecke der Datenverarbeitung verwendeten »Mittel«, die die Anwendung der Richtlinie auf Verantwortliche außerhalb der EU bzw. des EWR zur Folge haben kann, wird in der Stellungnahme präzisiert, dass diese Bestimmung in den Fällen Anwendung finden sollte, in denen es keine Niederlassung in der EU bzw. im EWR gibt, die die Anwendung von Art. 4 Absatz 1 Buchstabe a auslösen würde, oder in denen die Verarbeitung nicht im Rahmen der Tätigkeiten einer solchen Niederlassung erfolgt. Eine weite Auslegung des Begriffs »equipment«, die auch durch die Wortwahl in anderen Sprachfassungen (»Mittel« in der deutschsprachigen Fassung) gerechtfertigt ist, kann in manchen Fällen dazu führen, dass europäisches Datenschutzrecht auch dann zur Anwendung gelangt, wenn die betreffende Verarbeitung keinen konkreten Bezug zur EU bzw. zum EWR aufweist.

Die Stellungnahme gibt darüber hinaus Auslegungshinweise und Beispiele zu den anderen Bestimmungen des Art. 4, zu den Sicherheitsanforderungen nach Maßgabe des gemäß Art. 17 Absatz 3 anwendbaren Rechts sowie zu der Möglichkeit der Datenschutzbehörden, bei einem Verarbeitungsvorgang in ihrem Hoheitsgebiet ihre Untersuchungs- und Eingriffsbefugnisse auch dann auszuüben, wenn das Recht eines anderen Mitgliedstaats anwendbar ist (Art. 28 Absatz 6). In der Stellungnahme wird auch angeregt, im Rahmen einer Überarbeitung des allgemeinen Datenschutzrahmens die Richtlinie klarer zu fassen und für eine größere Kohärenz innerhalb des Art.s 4 zu sorgen. Eine Vereinfachung der Regeln zur Bestimmung des anwendbaren Rechts würde

vor diesem Hintergrund auf eine Rückkehr zum Herkunftslandprinzip hinauslaufen: Danach würden alle Niederlassungen eines für die Verarbeitung Verantwortlichen in der EU unabhängig davon, wo diese Niederlassungen jeweils angesiedelt sind, dasselbe Recht anwenden, und zwar das der Hauptniederlassung. Dies wäre jedoch nur dann akzeptabel, wenn das einzelstaatliche Recht, d.h. auch die Sicherheitspflichten, umfassend harmonisiert würde.

Wenn der für die Verarbeitung Verantwortliche außerhalb der EU niedergelassen ist, könnten zusätzliche Kriterien herangezogen werden, um eine ausreichende Verbindung zum EU-Gebiet sicherzustellen und um gleichzeitig zu vermeiden, dass in Drittländern ansässige Verantwortliche Daten im EU-Gebiet rechtswidrig verarbeiten. Hierfür in Frage kommende Kriterien wären das Anvisieren einzelner Personen (wenn sich die Verarbeitung personenbezogener Daten auf Einzelpersonen in der EU bezieht und die Anwendung des EU-Datenschutzrechts zur Folge hat) oder hilfsweise der begrenzte Rückgriff auf das »equipment«-Kriterium (Verarbeitung personenbezogener Daten durch automatisierte oder nicht automatisierte, im Hoheitsgebiet des betreffenden Mitgliedstaats gelegene Mittel) zwecks Erfassung von Grenzfällen (Daten von Drittstaatsangehörigen, Verantwortliche ohne Bezug zur EU), wenn es in der EU eine entsprechende Infrastruktur für die Datenanwendung gibt.

7.2.1.3 Datenschutzfolgenabschätzungen für RFID-Anwendungen

Am 31. März 2010 legten Branchenvertreter der Art.-29-Datenschutzgruppe einen Vorschlag für einen Rahmen für Datenschutzfolgenabschätzungen zur Prüfung vor. Wenngleich dieser Vorschlag einen guten Ansatzpunkt darstellte, erhielt er nicht die volle Zustimmung der Datenschutzgruppe, insbesondere da in dem vorgeschlagenen Rahmen wesentliche Bestandteile fehlten.

In weiterer Folge hat die Branche einen überarbeiteten Rahmen für Datenschutzfolgenabschätzungen erarbeitet, wobei sie Beiträge sowohl der Datenschutzgruppe als auch der ENISA berücksichtigte. Dieser überarbeitete Rahmen für Datenschutzfolgenabschätzungen wurde der Art.-29- Datenschutzgruppe zur Prüfung vorgelegt.

Der überarbeitete Rahmen beginnt mit einem Überblick über wichtige interne Prozeduren, die für die Durchführung der Datenschutzfolgenabschätzung relevant sind. Hierzu gehören unter anderem die Zeitplanung und Überprüfung der Datenschutzfolgenabschätzung, das Erstellen der einschlägigen Dokumentation, die Bestimmung der Personen, die innerhalb der Organisation für die Unterstützung des Prozesses der Datenschutzfolgenabschätzungen zuständig sind, die Identifizierung der Bedingungen, die in Zukunft eine Überprüfung der Datenschutzfolgenabschätzungen auslösen könnten sowie Beratungen mit den Beteiligten.

Der Prozess der Datenschutzfolgenabschätzung ist zweiphasig:

I. eine Vor-Bewertungsphase, die eine RFID-Anwendung nach einer auf einem Entscheidungsbaum basierenden Vier-Stufen-Skala klassifiziert. Anhand des Ergebnisses dieser Bewertung kann festgelegt werden, ob eine Datenschutzfolgenabschätzung erforderlich ist oder nicht und ob diese in »großem« oder »kleinem Umfang« erfolgt. Anwendungen, die RFID-Tags nutzen, die vermutlich von Personen mitgeführt werden, machen zumindest eine »Datenschutzfolgenabschätzung in kleinem Amfang« (Stufe 1) erforderlich, während Anwendungen, die die personenbezogenen Daten weiter verarbeiten, eine »Datenschutzfolgenabschätzung in großem Umfang« (Stufe 2 und 3) erfordern. Umgekehrt unterliegen Anwendungen, die keine Tags nutzen, die vermutlich von Personen mitgeführt werden und die die personenbezogenen Daten nicht weiter verarbeiten, keiner Datenschutzfolgenabschätzung.
II. eine Risikobewertungsphase, die aus vier Hauptschritten besteht:

1. Charakterisierung der Anwendung (Datentypen, Datenfluss, RFID-Technologie, Datenspeicherung, Datenübermittlung usw.)
2. Identifizierung der Risiken für personenbezogene Daten, indem Bedrohungen, ihre Wahrscheinlichkeit und ihre Auswirkung auf den Datenschutz sowie die Einhaltung der europäischen Rechtsvorschriften
3. Identifizierung und Empfehlung von Kontrollen als Reaktion auf die zuvor identifizierten Risiken
4. Dokumentation der Ergebnisse der Datenschutzfolgenabschätzung, Abfassen einer Entschließung bezüglich der Bedingungen für die Umsetzung der geprüften RFID-Anwendung sowie Informationen zu den Restrisiken.

Jeder Schritt der Risikobewertungsphase wird zusätzlich durch Elemente unterstützt, die in den Anhängen des überarbeiteten Rahmens niedergelegt sind.

Das Ergebnis der Datenschutzfolgenabschätzungen wird von dem RFID-Anwendungsbetreiber formell in einem Datenschutzfolgenabschätzungsbericht zusammengefasst, der die RFID-Anwendung beschreibt und die Einzelheiten der vorgenannten vier Risikobewertungsschritte dokumentiert.

Die Datenschutzgruppe befürwortete den überarbeiteten Rahmen, der am 12. Januar 2011 vorgelegt wurde und stellte fest, dass dieser Rahmen spätestens sechs Monate nach der Veröffentlichung dieser Stellungnahme in Kraft treten würde.

7.2.1.4 Smart Metering

Intelligente Verbrauchsmessgeräte ermöglichen die Erstellung, Übermittlung und Auswertung von Daten über die Verbraucher, und zwar in wesentlich größerem Umfang, als es mit »herkömmlichen« Messgeräten ohne »intelligente« Zusatzfunktionen möglich ist. Demzufolge können auch der Netzbetreiber (auch als Verteilungsnetzbetreiber (VNB) bezeichnet), die Energieversorger und andere Akteure detaillierte Informationen über den Energieverbrauch und die Verbrauchsmuster erstellen und anhand der Nutzungsprofile Entscheidungen über individuelle Energienutzer treffen. Zwar können derartige Entscheidungen häufig in Form von Energieeinsparungen durchaus Vorteile für die Verbraucher mit sich bringen, doch zeichnet sich auch ab, dass durch die in den Privathaushalten installierten Geräte die Möglichkeit von Eingriffen in die Privatsphäre der Bürger besteht. Außerdem kommt es dadurch zu einer grundsätzlichen Verschiebung in den Beziehungen zu den Energieversorgern, da die Verbraucher in der Vergangenheit lediglich die Lieferanten für die von diesen bezogenen Strom- und Gaslieferungen bezahlt haben. Mit dem Aufkommen intelligenter Verbrauchsmessgeräte gestaltet sich dieser Prozess insofern komplexer, als die betroffenen Personen damit den Versorgern Einblicke in ihre persönlichen Gewohnheiten geben.

Wie die Datenschutzgruppe in ihrer Stellungnahme ausführt, ist die Situation in den EU-Mitgliedstaaten sehr unterschiedlich, sowohl hinsichtlich der Fortschritte bei der Einführung als auch hinsichtlich der Energieversorgungssysteme, wodurch sich die Sachlage weiter kompliziert. Eindeutig klar ist jedoch die immense Tragweite intelligenter Verbrauchsmessungen: Vor Ende dieses Jahrzehnts dürften entsprechende Systeme in den Haushalten der überwiegenden Mehrheit der Bürger Europas installiert sein.

Egal wie die Datenverarbeitung erfolgt – ob auf ähnliche Weise wie zu den Zeiten vor Einführung intelligenter Systeme oder in völlig neuartiger Form –, der für die Datenverarbeitung Verantwortliche (= der Auftraggeber iSd DSG 2000) muss eindeutig ermittelt werden und sich der aus dem Datenschutzrecht erwachsenden Pflichten, auch in Bereichen wie »eingebautem Datenschutz« (»Privacy by Design«), Datensicherheit und Rechte der betroffenen Person, bewusst sein. Die betroffenen Personen müssen in geeigneter Form darüber unterrichtet werden, wie ihre Daten verarbeitet werden, und sich über die grundlegenden Unterschiede darin, wie ihre Daten verarbeitet werden, im Klaren sein, so dass sie ihre Einwilligung in rechtsgültiger Form geben können.

7.2.1.5 Geolokalisationsdaten auf intelligenten mobilen Geräten

Mithilfe der Geolokalisationstechnologien können intelligente mobile Geräte von allen Auftraggebern zurückverfolgt werden, etwa für Zwecke der verhaltensorientierten Werbung bis hin zur Überwachung von Kindern. .Damit können höchst private Daten der Eigentümer der Geräte gewonnen werden. Ein besonderes Problem ist die Tatsache, dass die Eigentümer der Geräte sich des Datentransfers nicht bewusst sind; insofern kann auch keine gültige Zustimmung der Betroffenen vorliegen.

Wie in der Stellungnahme der Datenschutzgruppe ausgeführt wird, bestehen drei Arten von Auftraggebern: die Auftraggeber der Geolokalisations-Infrastruktur, die Provider der Geolokalisationsservices und diejenigen, die die Betriebssysteme der mobilen Geräte entwickeln.

Als Rechtsgrundlage kommt bei derartigen Diensten zunächst die Einwilligung in Frage. Diese müsste allerdings nach einer hinreichenden Information des Betroffenen freiwillig für den konkreten Zweck erfolgen. Die Einwilligung von Arbeitnehmern und Kindern ist problematisch. Hier sind zusätzliche Garantien zum Schutz der Geheimhaltung notwendig.

Weiters sollten Lokalisationssysteme »by default« abgeschaltet sein; ein möglicher opt-out-Mechanismus wäre nicht hinreichend und stellt keine Zustimmung dar.

Im Zusammenhang mit der Zuordnung von WLAN-Zugangpunkten können Unternehmen allenfalls ein rechtliches Interesse an der Verarbeitung von MAC-Adressen und der Lokalisierung von WLAN-Zugangspunkten zum Zweck des Anbietens von Geolokalisierungsdiensten haben. Um hier eine Balance der Interessen zu finden, muss der Auftraggeber eine einfache und permanente opt-out-Lösung anbieten.

Besonderes Augenmerk ist auf eine umfassende und klare Information der Betroffenen und kurze Löschungsfristen bezüglich der angefallenen Daten zu legen.

7.2.1.6 Einwilligung

Die Stellungnahme beinhaltet eine Analyse des Konzepts der »Einwilligung« im Sinne der Datenschutzrichtlinie und der E-Privacy-Richtlinie. Es werden zahlreiche Beispiele für gültige und ungültige Einwilligungen gegeben, indem der Fokus auf die Bedeutung von Schlüsselbegriffen wie »Willensbekundung«, »ohne Zwang«, »konkret«. »ausdrücklich«, »ohne jeden Zweifel«, »in Kenntnis der Sachlage« etc. gelegt wird.

Die Einwilligung ist einer von mehreren Legitimationsgründen für die Verarbeitung von Daten. Sie spielt eine wichtige Rolle, schließt aber nicht die Möglichkeit aus, je nach Kontext andere Rechtfertigungstatbestände heranzuziehen, die aus Sicht des Auftraggebers und des Betroffenen besser geeignet sind.

Sofern das Instrument der Einwilligung korrekt genutzt wird, stellt es ein Mittel dar, das dem Betroffenen die Kontrolle über die Verwendung seiner Daten einräumt. Die Stellungnahme erging auf Anfrage der EU-Kommission im Zusammenhang mit den – damals in Vorbereitung stehenden – Vorschlägen für neue Datenschutzrechtsinstrumente. Daher werden auch Empfehlungen im Hinblick auf diese neuen Rechtsinstrumente geben.

Diese Empfehlungen beinhalten:

(i) die Klarstellung der Bedeutung von »ohne jeden Zweifel« und der Tatsache, dass nur Einwilligungen, die auf Äußerungen oder Handlungen beruhen, die Zustimmung signalisieren, gültige Einwilligungen darstellen können;
(ii) Auftraggeber zu verpflichten, Mechanismen zur Sichtbarmachung der Einwilligungen vorzusehen;
(iii) eine ausdrückliche Verpflichtung bezüglich der Qualität und Verfügbarkeit der Information vorzusehen, die die Basis für die Einwilligung bildet;
(iv) Vorschläge bezüglich der Einwilligung von Kindern und anderer nicht geschäftsfähiger Personen.

7.3 Zusammenarbeit im Rahmen der Gemeinsamen Kontrollinstanzen der ehemaligen »Dritten Säule«

7.3.1 Europol

Europol ist das Europäische Polizeiamt, das EU-weit operiert und schwerwiegende Formen internationaler Kriminalität bekämpfen soll. Dazu werden große Mengen an personenbezogenen Daten verarbeitet, die auf Grund der Zielsetzung von Europol von besonderer datenschutzrechtlicher Bedeutung sind. Aus diesem Grund sind im Europol-Beschluss, mit dem Europol eigene Rechtspersönlichkeit zuerkannt wurde, besondere Rechte der Betroffenen vorgesehen (z. B. Art. 30 – Auskunftsanspruch; Art. 31 – Berichtigung und Löschung von Daten).

Neben den nationalen Kontrollinstanzen (Art. 33), im Wesentlichen die nationalen Datenschutzbehörden, wurde eine Gemeinsame Kontrollinstanz (GKI; »Europol Joint Supervisory Body«)[11] eingesetzt (Art. 34), deren Aufgabe darin besteht, die Tätigkeit von Europol nach Maßgabe des Europol-Beschlusses 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 Inspektionen bei Europol durch, weitere Inspektionen zu Sonderfragen sind ebenfalls möglich.

Die österreichischen Mitglieder der GKI werden von der DSK entsandt. Überdies stellt die DSK ein Mitglied der Europol-Inspektionsgruppe, welche im März 2010 und im März 2011 Inspektionen bei Europol durchgeführt hat. Im Jahr 2010 lag der Schwerpunkt der Kontrolle neben der Funktionsfähigkeit des Europol-Informationssystems (EIS) (Art. 11ff) und der Rechtskonformität der verarbeiteten Daten in Analytical Work Files (AWF) – Arbeitsdateien (Art. 14) auf der technischen Sicherheitsinfrastruktur, einigen EDV-Systemen, die die Dateneinspeisung ermöglichen bzw. unterstützen sowie dem Zugang zu den Daten im Schengener Informationssystem. Im Jahr 2011 konzentrierte sich das Team zusätzlich auf die Verarbeitung der Daten der Mitarbeiter von Europol (Videoüberwachung, Telefonanlage etc.). Das Inspektionsteam erstellt einen Bericht, der – nachdem Europol die Möglichkeit zur Stellungnahme eingeräumt wurde und er in der GKI formell verabschiedet wurde – auch veröffentlicht wird.

Schwerpunkte der Sitzungsarbeit in der GKI Europol im Berichtszeitraum waren die Begutachtung von Verträgen, die Europol hinsichtlich des Datenaustausches mit Drittstaaten abgeschlossen hat, die Rolle der GKI in Zeiten des Lissabonner Vertrages (sowie eine darauf abgestimmte Strategie), eine Inspektion der Verwendung von Daten im Rahmen des TFTP-Abkommens (US-Terrorist Finance Tracking Program), ein neues Konzept bei der Ausgestaltung der AWF (Orientierung an räumlichen Kriterien anstatt Typen von Verbrechen – damit verbunden eine starke Reduzierung der Zahl der AWF und Eröffnung von Target Groups und Focal Points innerhalb eines AWF) sowie Richtlinien seitens Europol für die Beantwortung von Auskunftsersuchen betreffend dort gespeicherte personenbezogene Daten.

Im Beschwerdeausschuss Europol, der für die Behandlung der Beschwerden von Betroffenen betreffend die Datenverwendung durch Europol zuständig ist, wurden zwischen Jänner 2010 und Dezember 2011 zwei Beschwerdefälle erledigt, zwei weitere Beschwerdefälle sind anhängig.

7.3.2 Schengen

Die DSK ist nationale Kontrollinstanz im Sinne des Art. 114 Schengener Durchführungsübereinkommen von 1990 (SDÜ) zur Überwachung des nationalen Teils des Schengener Informationssystems (SIS). Als solche entsendet sie auch die Vertreter in die Gemeinsame Kontrollinstanz von Schengen.[12] Diese überwacht die Übereinstimmung der Verwendung der Daten im Schengener

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

12 Die Gemeinsame Kontrollinstanz von Schengen hat eine eigene Website: http://schengen.consilium.europa.eu/. Die Jahresberichte der GKI Schengen sind auf der Website der Datenschutzkommission www.dsk.gv.at veröffentlicht.

(Informations-)System mit dem Schengener Durchführungsübereinkommen. Dazu kontrolliert sie die technische Unterstützungseinheit des SIS, prüft Anwendungs- und Auslegungsfragen im Zusammenhang mit dem Funktionieren des SIS sowie Fragen im Zusammenhang mit den von den nationalen Kontrollinstanzen unabhängig vorgenommenen Kontrollen oder mit der Ausübung des Auskunftsrecht und erarbeitet harmonisierte Vorschläge im Hinblick auf gemeinsame Lösungen für bestehende Fragen.

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

Im Berichtszeitraum war die GKI Schengen mit folgenden wichtigen Themen konfrontiert:

- Follow-Up zur Prüfung der Ausschreibungen nach Art. 99 SDÜ (verdeckte Registrierung von Personen und Fahrzeugen) aus 2007.
- Prüfung der Ausschreibungen nach Art. 95 SDÜ (Ausschreibung von Personen zur Festnahme und Auslieferung).
- Beleuchtung der Rolle der GKI im Lichte des Lissabonner Vertrages.
- Inspektion des SIS I+4all (die »Zwischenlösung«) zum SIS II.
- Auslegung von Art. 45 SDÜ.
- Rechtsfragen im Zusammenhang mit dem Zugang von Europol zu Daten im SIS.
- Implementierung von Art. 102A SDÜ.
- Neugestaltung der Website der GKI.
- Initiierung einer Prüfung zu Fragen der Geltendmachung des Rechts auf Auskunft betreffend Daten im SIS in der Praxis.

7.3.3 Zoll

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) für den Bereich der ehemaligen 1. Säule der EU sowie des Übereinkommens aufgrund von Art. 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) für den Bereich der ehemaligen 3. Säule der EU wurde ein gemeinsames Zollinformationssystem (ZIS) eingerichtet. Dieses erlaubt es, sowohl in einer Datenbank für den Bereich der gemeinschaftsrechtlichen Zuständigkeiten wie auch in einer Datenbank, die den nicht harmonisierten Bereiche betrifft, Daten über Waren oder Transportmittel sowie über natürliche und juristische Personen zu speichern, für die es tatsächliche Anhaltspunkte gibt, dass sie im Zusammenhang mit Handlungen stehen, die der Zoll- oder der Agrarregelung zuwiderlaufen.

Die Verordnung (EG) 515/97 wurde durch die Verordnung (EG) 766/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die gegenseitige Amtshilfe zwischen Verwaltungsbehörden der Mitgliedstaaten und die Zusammenarbeit dieser Behörden mit der Kommission im Hinblick auf die ordnungsgemäße Anwendung der Zoll- und der Agrarregelung geändert.

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

Um eine adäquate datenschutzrechtliche Kontrolle zu gewährleisten, wurde durch das vorstehend zitierte Übereinkommen vom 26. Juli 1995 eine gemeinsame Aufsichtsbehörde (Gemeinsame Kontrol-

linstanz für das ZIS) eingerichtet, für die jedes EU-Mitgliedsland 2 Vertreter namhaft macht, die von der jeweiligen nationalen unabhängigen Datenschutzbehörde nominiert werden.

Schwerpunkte des Berichtszeitraumes waren eine Untersuchung zu Fragen der Informationssicherheitspolitik auf nationaler Ebene, eine Inspektion des zentralen ZIS, eine Evaluierung des FIDE-Handbuchs sowie die Zusammenarbeit mit der Koordinationsgruppe ZIS (siehe sogleich). Darüber hinaus wurde eine neue Geschäftsordnung beschlossen.

Die Verordnung (EG) 766/2008 schuf durch ihren Art. 37 eine Form der koordinierten Kontrolle durch die nationalen ZIS-Aufsichtsbehörden und den Europäischen Datenschutzbeauftragten. Die so geschaffene Koordinationsgruppe ZIS nahm ihre Arbeit im März 2010 auf.

Neben der Zusammenarbeit mit der GKI ZIS, die weitgehend dieselben Themenbereiche abzudecken hat (dort eben für den Bereich der ehemaligen 3. Säule der EU), sind im Berichtszeitraum folgende Schwerpunkte in der Tätigkeit gesetzt worden: Information über Entwicklungen im Zollbereich (u. a. ist geplant, diesen rechtlich doch sehr zersplitterten Bereich in einem Rechtsakt zu regeln), Vorabkontrolle von Datenanwendungen bei OLAF (Europäisches Amt für Betrugsbekämpfung), Überprüfung der Gruppen von Behörden, die Zugang zu ZIS und FIDE haben, sowie ein Arbeitspapier zu den Rechten der Betroffenen im Bereich Zoll.

7.4 Die »Working Party Police and Justice«

Bei der Frühjahrskonferenz der Unabhängigen Datenschutzbehörden 2007 auf Zypern wurde die Working Party Police and Justice (WPPJ) als Nachfolgegruppe der früheren Police Working Party (PWP), die als ständige Untergruppe der Frühjahrskonferenzen der Europäischen Datenschutzbehörde eingerichtet worden war, neu konstituiert. Die WPPJ hatte die Aufgabe, die wichtigsten datenschutzrechtlichen Fragen der ehemaligen 3. Säule der EU (polizeiliche und justizielle Zusammenarbeit) zu beraten, die der Zuständigkeit der Art. 29 Datenschutzgruppe entzogen waren. Sie fungierte damit auch als Pendant und/oder Bindeglied zur Art. 29 WP.

Mit Inkrafttreten des Vertrages von Lissabon und Auflösung der Säulenarchitektur der EU sind die Agenden dieser Gruppe nunmehr auch von der Art. 29 WP behandelbar, weshalb die WPPJ inhaltlich von einer neuen ständigen Untergruppe der Art. 29 WP, der Borders, Travel and Law Enforcement Subgroup (BTLE Subgroup), abgelöst wurde.

Im Berichtszeitraum hatte sich die WPPJ dennoch mit Fragen der Implementierung des Rahmenbeschlusses über den Datenschutz in der 3. Säule, des Prümer Vertrages und der Cybercrime Convention auseinander zu setzen. Die WPPJ hat außerdem eine Supervision Policy für den Polizeibereich ausgearbeitet, die allen nationalen DSB zur Unterstützung von Kontrollen zur Verfügung steht.

7.5 Eurodac

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

»Eurodac« besteht aus einer von der Kommission verwalteten Zentraleinheit, einer computergestützten Datenbank für Fingerabdrücke und elektronischen Einrichtungen für die Datenübertragung zwischen den Mitgliedstaaten und der zentralen Datenbank. Neben den Fingerabdrücken

umfassen die von den Mitgliedstaaten übermittelten Daten u. a. den Herkunftsmitgliedstaat, Ort und Zeitpunkt der Antragstellung, das Geschlecht sowie die Kennnummer (Namen werden in diesem System nicht gespeichert, es handelt sich daher um eine Sammlung von »indirekt personenbezogenen Daten« im Sinne des DSG 2000).

Im Berichtszeitraum hat sich die zur Kontrolle des Systems eingerichtete Koordinierungsgruppe, bestehend aus Vertretern der nationalen DSB und des Europäischen Datenschutzbeauftragten, mit einer Kontrolle zu Löschungsfragen aus dem Eurodac-System sowie einem Security Audit auf nationaler Ebene auseinandergesetzt. Die DSK hat, wie auch in den letzten Berichten an dieser Stelle ausgeführt, bis dato keine Beschwerde oder Anfrage zu Eurodac erhalten.

8 Das Datenverarbeitungsregister

8.1 Allgemeine Bemerkungen

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

Gemäß § 2 Abs. 3 DVRV 2002 besteht die Datenanwendung »Datenverarbeitungsregister« aus:

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

Daneben ist das »Datenverarbeitungsregister« auch jene Organisationseinheit (Referat DVR) innerhalb der Geschäftsstelle der DSK, in der die Registrierungsverfahren durchgeführt und auch die das Registrierungsverfahren betreffenden Bescheide der Kommissionsorgane vorbereitet werden.

8.2 Zum Geschäftsgang des Registers

8.2.1 Statistische Aufbereitung

Entsprechend der Gliederung des sonstigen Geschäftsgangs der Datenschutzkommission nach Halbjahren, werden auch Eingänge und Erledigungen im Datenverarbeitungsregister nach Halbjahren gegliedert dargestellt. Die statistischen Auswertungen für den Berichtszeitraum wurden über die Protokollrecherche von DVR-Online erstellt. Die Anzahl der Verbesserungsaufträge bezieht sich oft auf mehrere Datenanwendungen (z. B. mit einer Eingabe werden mehrere Datenanwendungen gemeldet, jene, die mangelhaft sind, werden in einem Verbesserungsauftrag behandelt). Die Anzahl der Enderledigungen ist nachstehend gesondert ausgewiesen.

Erstes Halbjahr 2010:

Eingang	Verbesserungsaufträge	Registrierungen	Einstellungen	Streichungen
Auftraggebermeldungen und gemeldete Datenanwendungen				
4355	633	3863	97	359
Monatsschnitt (auf-/abgerundet) 726	106	644	16	60

Eingang und Streichungsmeldungen (die Streichungsmeldungen werden nicht im System protokolliert, sondern über die DVR-Recherche erledigt)	**Erledigungen**
4714	4952
	Enderledigungen (Registrierungen, Einstellungen und Streichungen): 4319

Zweites Halbjahr 2010:

Eingang	Verbesserungsaufträge	Registrierungen	Einstellungen	Streichungen
Auftraggebermeldungenund gemeldete Datenanwendungen				
3214	841	2282	105	154
Monatsschnitt (auf-/abgerundet) 536	140	380	18	26

Eingang und Streichungsmeldungen (die Streichungsmeldungen werden nicht im System protokolliert, sondern über die DVR-Recherche erledigt)	**Erledigungen**
3368	3382
	Enderledigungen (Registrierungen, Einstellungen und Streichungen): 2541

Erstes Halbjahr 2011:

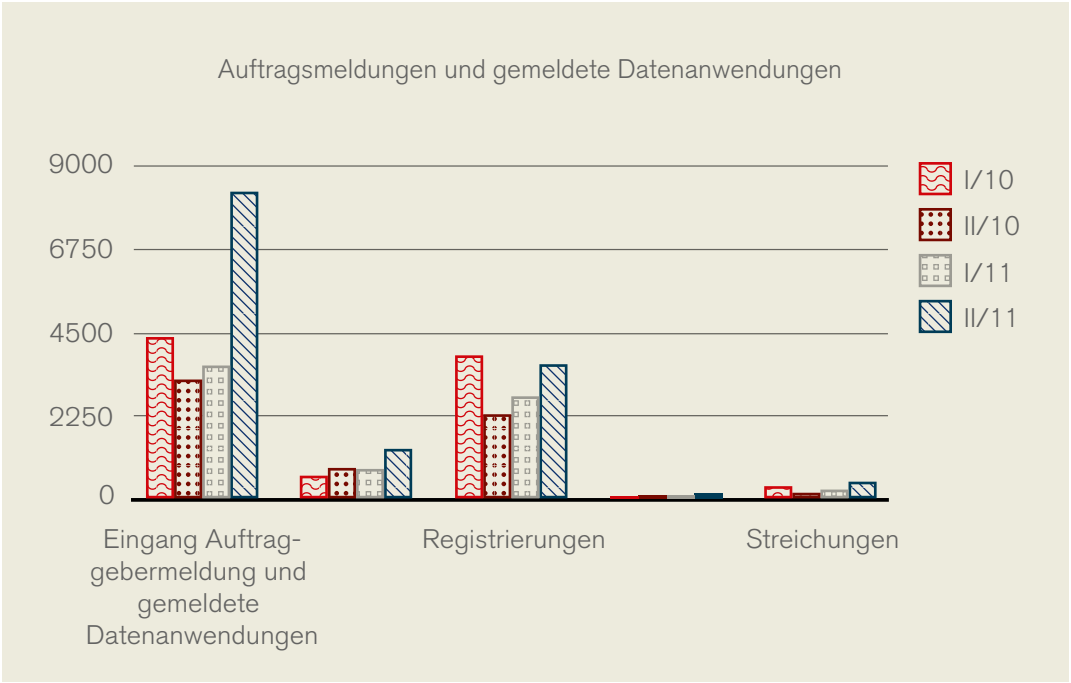
Eingang	Verbesserungsaufträge	Registrierungen	Einstellungen	Streichungen
Auftraggebermeldungen und gemeldete Datenanwendungen				
3590	814	2763	116	260
Monatsschnitt (auf-/abgerundet) 598	136	461	19	43

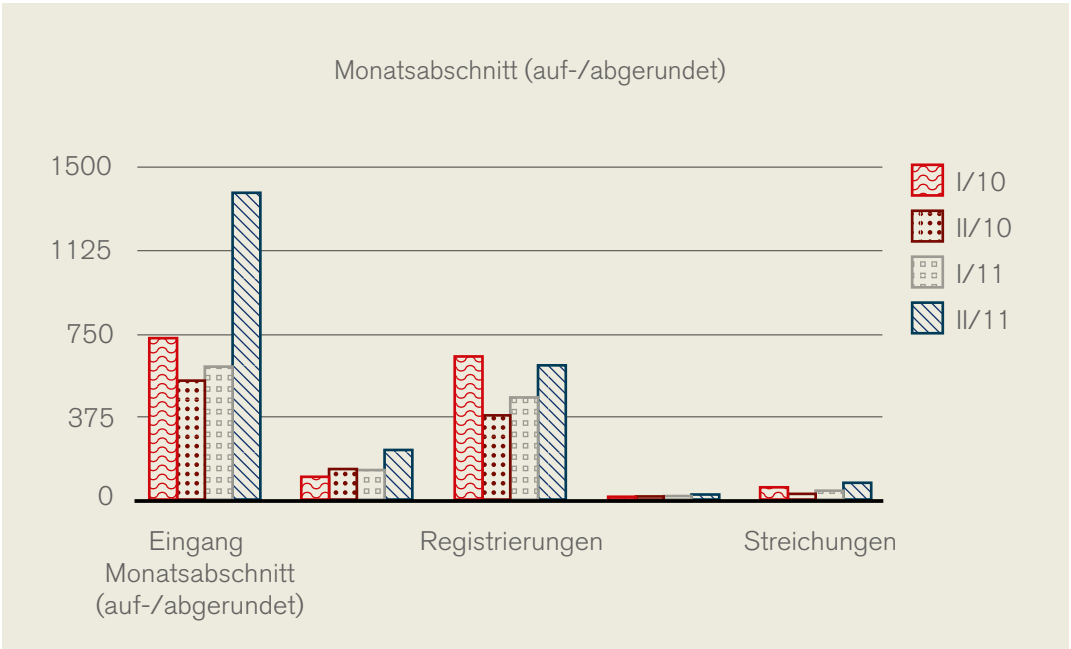
Eingang und Streichungsmeldungen (die Streichungsmeldungen werden nicht im System protokolliert, sondern über die DVR-Recherche erledigt)	**Erledigungen**
3850	3953
	Enderledigungen (Registrierungen, Einstellungen und Streichungen): 3139

Zweites Halbjahr 2011:
(ca. 3000 Meldungen waren zum Berichtszeitpunkt noch nicht protokolliert, wurden aber beim Eingang dazugezählt)

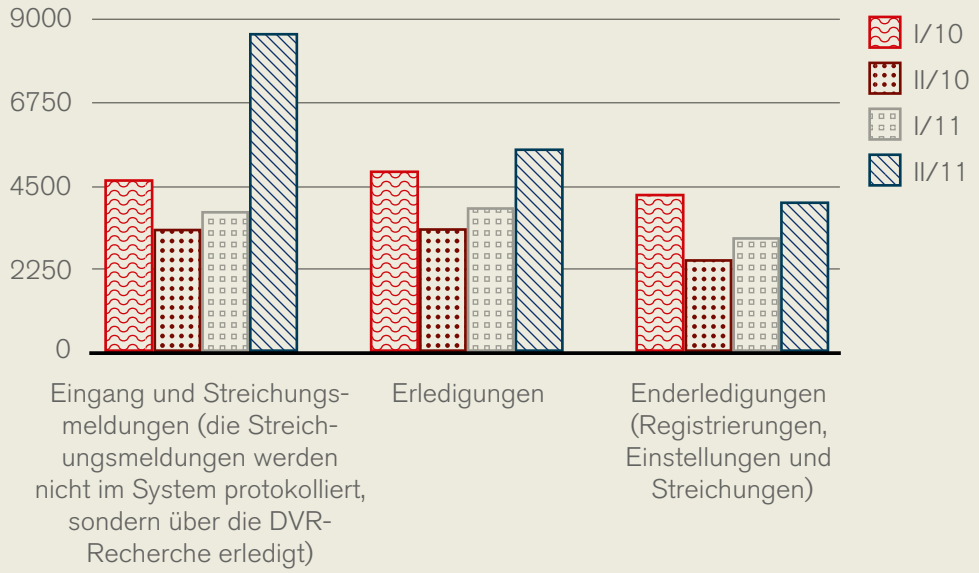
Eingang	Verbesserungsaufträge	Registrierungen	Einstellungen	Streichungen
Auftraggebermeldungen und gemeldete Datenanwendungen				
8276	1353	3625	157	416
Monatsschnitt (auf-/abgerundet) 1379	226	604	26	69

Eingang und Streichungsmeldungen (die Streichungsmeldungen werden nicht im System protokolliert, sondern über die DVR-Recherche erledigt)	**Erledigungen**
8692	5551
	Enderledigungen (Registrierungen, Einstellungen und Streichungen): 4110

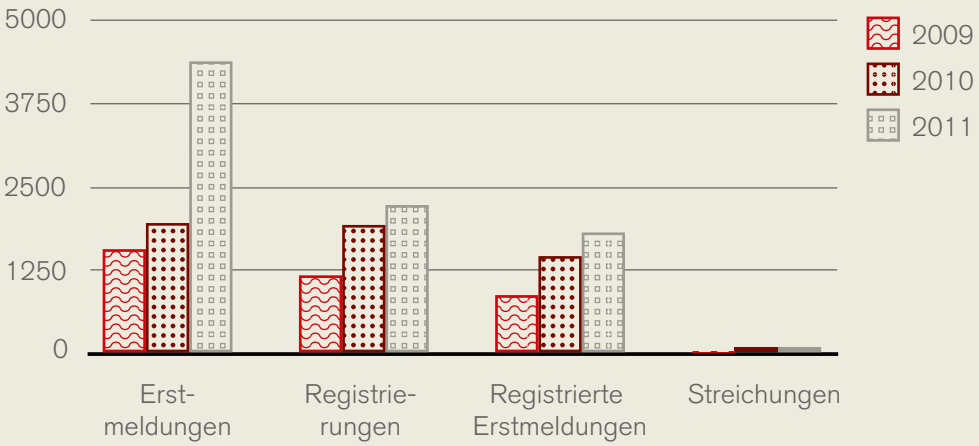

Auftragsmeldungen und gemeldete Datenanwendungen
9000
6750
4500
2250
0
I/10
II/10
I/11
II/11
Eingang Auftrag-gebermeldung und gemeldete Datenanwendungen
Registrierungen
Streichungen

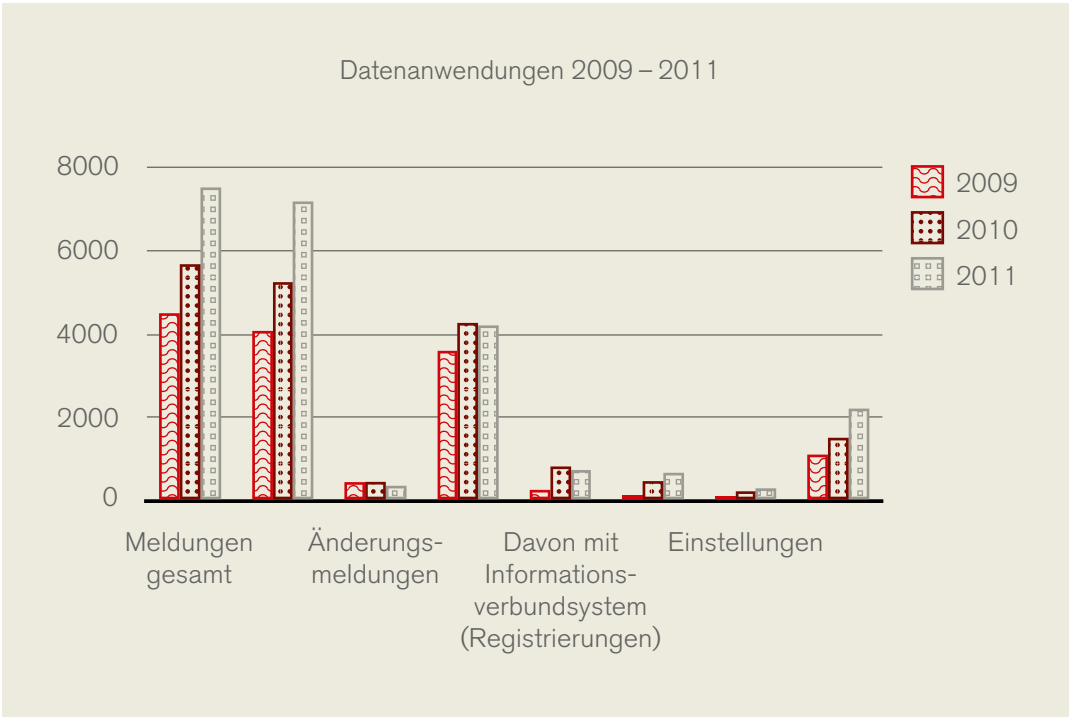

Monatsabschnitt (auf-/abgerundet)
1500
1125
750
375
0
I/10
II/10
I/11
II/11
Eingang Monatsabschnitt (auf-/abgerundet)
Registrierungen
Streichungen

Eingang und Streichungsmeldungen



Auftraggeber 2009 – 2011




Datenanwendungen 2009 – 2011
8000
6000
4000
2000
0
2009
2010
2011
Meldungen gesamt
Änderungs-meldungen
Davon mit Informations-verbundsystem (Registrierungen)
Einstellungen

ELAK:
- Bescheidentwürfe im Jahr 2010: 82
- Bescheidentwürfe im Jahr 2011: 155

E-Mail: Beantwortung von E-Mail-Anfragen
- im Jahr 2010: ca. 500;
- im Jahr 2011: ca. 500

Die vorliegende Statistik zeigt, dass es mit den vorhandenen Personalressourcen nicht möglich war, den Arbeitsanfall und die Erledigungen ins Gleichgewicht zu bringen.

Da auch noch mehrere tausende Meldungen als Rückstände einer Erledigung harren, wäre es notwendig, – allenfalls auch legistisch – Vorsorge zu treffen, um weitere Rückstände zu vermeiden.

8.2.2 Wichtige Registrierungen aus dem Berichtszeitraum

8.2.2.1 Informationsverbundsysteme (IVS)

a. aus dem Gesundheitsbereich:
– IVS E-Medikation

Bei der e-Medikation handelt es sich um zwei Informationsverbundsysteme im Sinne des § 50 DSG 2000. Als datenschutzrechtliche Auftraggeber fungieren die an e-Medikation teilnehmenden, niedergelassenen Vertragsärzte, teilnehmende Apotheken und teilnehmende Krankenanstalten.

Die »e-Medikation« wurde von ihren Initiatoren als Pilotprojekt im Rahmen der Vorarbeiten zum »Elektronischen Gesundheitsakt (ELGA)« in Österreich ins Leben gerufen. Zweck eines Pilotprojekts ist es, die Eignung einer bestimmten Vorgangsweise im Hinblick auf bestimmte Ziele zu testen. Im vorliegenden Fall sind weder Vorgangsweise noch Ziele durch Gesetz vorgegeben, es handelt sich vielmehr um eine Initiative, die von Krankenanstalten, niedergelassenen Ärzten und Apotheken, die sich zu zwei im Rahmen des Projekts »e-Medikation« durchgeführten Informationsverbundsystemen zusammengeschlossen haben. Betreiber der Informationsverbundsysteme sind einerseits die Pharmazeutische Gehaltskasse für das Informationsverbundsystem »Medikationsdatenbank (abgegebene Arzneimittelspezialitäten)« und andererseits der Hauptverband der österreichischen Sozialversicherungsträger für das Informationsverbundsystem »Verordnungsdatenbank (verordnete Arzneimittelspezialitäten)«.

Im Zuge der Teilnahme am Informationsverbundsystem »Medikationsdatenbank (abgegeben Arzneimittelspezialitäten)« werden an den Patienten von der Apotheke, vom Arzt oder von der Krankenanstalt bei der Entlassung abgegebene Arzneimittel in der Medikationsdatenbank gespeichert. Für die Dauer der Einnahme plus zusätzlich sechs Monate werden die Medikationsinformationen des Patienten für die Anzeige in der Medikationsliste zur Anzeige für Ärzte, Krankenanstalten und Apotheken bereitgestellt. Bei der Ausstellung von Verordnungen bzw. der Abgabe von Arzneimitteln kann auf Wechselwirkungen und Mehrfachverordnungen geprüft werden.

Im Zuge der Teilnahme am Informationsverbundsystem »Verordnungsdatenbank (verordnete Arzneimittelspezialitäten)« werden dem Patienten verordnete Arzneimittel beim Arzt und in Krankenanstalten gegen die bestehende Medikation sowie allfällige offene Verordnungen auf Wechselwirkungen und Mehrfachverordnungen geprüft und in der Verordnungsdatenbank als geprüft gespeichert. Die in der Verordnungsdatenbank gespeicherten Verordnungen werden entweder bei Abholung in der Apotheke oder nach Ablauf von einem Monat aus der Verordnungsdatenbank logisch gelöscht.

Als Rechtsgrundlage für die »e-Medikation« kommt – mangels eines »ELGA-Gesetzes« – derzeit prinzipiell nur die Zustimmung der Betroffenen iVm der Information gemäß § 24 Abs. 2 DSG 2000 in Frage. Hier war durch Auflagen sicherzustellen, dass eine erteilte Zustimmung allen datenschutzrechtlichen Anforderungen für ihre Gültigkeit entspricht, insbesondere auch eine ausreichende »Kenntnis der Sachlage« durch entsprechende Information vor der Zustimmungserteilung gewährleistet wird. Gemäß § 9 Z 7 DSG 2000 dürfen Daten des Betroffenen auch dann verwendet werden, wenn die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zu-

stimmung nicht rechtzeitig eingeholt werden kann. In diesen Ausnahmefällen ist daher keine Zustimmung des Betroffenen erforderlich. Was die Möglichkeiten statistischer Auswertungen und damit die Möglichkeit der Gewinnung allgemeiner Erkenntnisse über den Nutzen »e-Medikation« betrifft, gelten die Regeln des § 46 DSG 2000, wonach jeder Auftraggeber Daten, die er für einen rechtmäßigen Zweck ermittelt hat – im vorliegenden Fall für die Medikationsprüfung aufgrund der Zustimmung der Betroffenen – statistisch auswerten darf. Angesichts der besonderen Sensibilität der enthaltenen Daten, ist es angeraten, die Fragestellungen, für die statistische Auswertungen – im Auftrag jeweils der teilnehmenden Auftraggeber – durchgeführt werden dürfen, im Vorhinein festzulegen. Dass bei den Auswertungen vorgesorgt werden muss, dass die Ergebnisse nur in Form aggregierter anonymer Daten vorliegen, ergibt sich aus der Formulierung der Auflage, die ausdrücklich nur anonymisierte Auswertungen zulässt.

– IVS »ePortal MS-Netz« der Salzburger Landeskliniken

Zweck dieser Datenanwendung, die in Form eines Informationsverbundsystems geführt wird, ist die Erfassung von Untersuchungs- und Behandlungsergebnissen von »Multiple Sklerose -Patienten« zur Überwachung des Behandlungsverlaufs und Optimierung der Behandlungsmethoden sowie Vermeidung von unnötigen Doppeluntersuchungen. Die Betroffenen stimmen der Verwendung ihrer Daten ausdrücklich zu und werden gemäß § 24 Abs. 2 Z 3 DSG 2000 darüber informiert, dass ihre Daten in einem Informationsvberbundsystem verarbeitet werden.

Die Entscheidung darüber, welche Dokumente abgerufen werden können, wird vom Patienten getroffen, wobei folgende Filterkriterien mindestens zur Verfügung stehen:

- Gesundheitsdiensteanbieter (die Bezeichnung wird vom GDA-Index übernommen)
- Zeitliche Einschränkung (Dokumentenerstellungsdatum von/bis)
- Dokumententyp (Mehrfachauswahl möglich); solche Dokumententypen sind vor allem: Entlassungsdokumente (Arztbrief, Pflegebrief); Befunde; Berichte/Protokolle zu Patienten (z. B. OP-Protokoll); Medikationsblatt; Bilder (z. B. Röntgenbilder, Ct-Bilder, Endoskopiebilder ….); Patientenverfügung
- Fachrichtungen (Mehrfachauswahl möglich)

Zur Wahrung des Datenschutzes werden neben den allgemeinen Sicherheitsvorkehrungen, wie sie in § 14 DSG 2000 angeführt sind, spezielle Sicherheitsvorkehrungen eingesetzt:

a. *Die Prüfung der physischen Anwesenheit des Patienten:* Daten können aus dem Gesundheitsinformationssystem nur dann abgerufen werden, wenn durch eine automationsunterstützte Kontrollroutine nachgewiesen wird, dass der Patient innerhalb der letzten 28 Tage beim abfragenden GDA zu Behandlungszwecken physisch anwesend war. Ein typischer Sicherheitstest besteht in der Nutzung der e-card, das bedeutet, dass, erst wenn der Patient eindeutig automatisationsgestützt über die e-card identifiziert wurde, eine Abfrage überhaupt möglich ist. Andere Sicherheitstests müssen vom Sicherheitsniveau gleichwertig zum e-card Sicherheitstest sein.
b. *Prüfung, ob gültige Patientenzustimmung zur Abfrage vorliegt:* Vor einer Abfrage muss der GDA das Vorliegen der Zustimmung des Patienten – samt Datum der Zustimmung – im System bestätigen. Die Zustimmung gilt 28 Tage ab dem Zeitpunkt der Erteilung. Der Patient kann diese Zustimmung jederzeit widerrufen.

Der GDA, bei dem die Daten abgefragt werden, kann jederzeit die Vorlage der Zustimmungserklärung (auf elektronischem Weg) verlangen.

Weiters gelangen folgende Berechtigungsregeln zur Anwendung:

a. *Internes Berechtigungssystem:* Jeder Teilnehmer hat die Zugriffsmöglichkeiten seiner Mitarbeiter derart zu gestalten, wie es für die übertragenen Aufgaben notwendig ist. Jeder GDA hat dafür Sorge zu tragen, dass die abgerufenen Daten nur berechtigten Mitarbeitern zur Verfügung stehen und er hat dafür auch die Haftung zu übernehmen. (Organisatorische und technische Sicherheitsmaßnahmen sind von den jeweiligen GDA festzulegen)
b. *Behandlungszusammenhang:* Ein Zugriff ist nur gestattet, wenn die behandelnde Person in einer für die Behandlung relevanten definierten Beziehung zum Patienten steht (z. B. behandelnder Arzt).
Der Zugriff ist in dem Ausmaß gestattet, wie er für Behandlungszwecke im Rahmen des jeweiligen Aufgabengebietes der jeweiligen Rolle bzw. insbesondere für die Behandlung des Patienten notwendig ist.
c. *Patientenidentifikation:* Patientendatenabfragen dürfen nur mit eindeutig identifizierten Patienten durchgeführt werden.
d. *Sicherheitsvorkehrungen bei der Datenübermittlung*

– IVS »elektronische Gesundheitsplattform der Ordenseinrichtungen« (eGOR), »Gesundheitsnetz Oberösterreich«, »eGesundheitsplattform OÖ« und »WE.G.E 42«

Zwecke dieser Datenanwendungen sind die Abfragen von Gesundheitsdaten zur Patientenbehandlung mit Zustimmung des Betroffenen, die in der Krankengeschichte hinterlegt ist.

Teilnehmende Auftraggeber am Informationsverbundsystem sind folgende Einrichtungen:

- Rechtsträger von Krankenanstalten
- Niedergelassene Ärzte
- Rechtsträger von Pflegeheimen
- Hauskrankenpflege

Im Informationsverbund werden nur die Filter- und Verweisdaten – keine Krankengeschichten – gespeichert, anhand derer jene Dokumente gefunden werden können, die sowohl vom Teilnehmer, also dem Gesundheitsdiensteanbieter (GDA), als auch vom Patienten für die Abfrage im konkreten Behandlungsfall freigegeben sind .

Die Entscheidung darüber, welche Dokumente abgerufen werden können, wird vom Patienten getroffen, wobei folgende Filterkriterien mindestens zur Verfügung stehen:

- Gesundheitsdiensteanbieter (die Bezeichnung wird vom GDA-Index übernommen)
- Zeitliche Einschränkung (Dokumentenerstellungsdatum von/bis)
- Dokumententyp (wobei eine Mehrfachauswahl möglich ist); solche Dokumententypen sind vor allem: Entlassungsdokumente (Arztbrief, Pflegebrief); Befunde; Berichte/ Protokolle zu Patienten (z. B. OP-Protokoll); Medikationsblatt; Bilder (z. B. Röntgenbilder, Ct-Bilder, Endoskopiebilder ….); Patientenverfügung
- Fachrichtungen (wobei eine Mehrfachauswahl möglich ist)

Zur Wahrung des Datenschutzes werden neben den allgemeinen Sicherheitsvorkehrungen, wie sie in § 14 DSG 2000 angeführt sind, spezielle Sicherheitsvorkehrungen eingesetzt:

a. *Prüfung der physischen Anwesenheit des Patienten:* Daten können aus dem Gesundheitsinformationssystem nur dann abgerufen werden, wenn durch eine automatisationsunterstützte Kontrollroutine nachgewiesen wird, dass der Patient innerhalb der letzten 28 Tage beim abfragenden GDA zu Behandlungszwecken physisch anwesend war. Ein typischer Sicherheitstest besteht in der Nutzung der e-card, das bedeutet, dass, erst wenn der Patient eindeutig automatisationsgestützt über die e-card identifiziert wurde, eine Abfrage überhaupt möglich ist. Andere Sicherheitstests müssen vom Sicherheitsniveau

gleichwertig zum e-card Sicherheitstest sein.

b. *Prüfung, ob gültige Patientenzustimmung zur Abfrage vorliegt:*
Vor einer Abfrage muss der GDA das Vorliegen der Zustimmung des Patienten – samt Datum der Zustimmung – im System bestätigen.
Die Zustimmung gilt 28 Tage ab dem Zeitpunkt der Erteilung. Der Patient kann diese Zustimmung jederzeit widerrufen.
Der GDA, bei dem die Daten abgefragt werden, kann jederzeit die Vorlage der Zustimmungserklärung (auf elektronischem Weg) verlangen.

Weiters gelangen folgende Berechtigungsregeln zur Anwendung:

a. *Internes Berechtigungssystem:* Jeder Teilnehmer hat die Zugriffsmöglichkeiten seiner Mitarbeiter derart zu gestalten, wie es für die übertragenen Aufgaben notwendig ist.
Jeder GDA hat dafür Sorge zu tragen, dass die abgerufenen Daten nur berechtigten Mitarbeitern zur Verfügung stehen und er hat dafür auch die Haftung zu übernehmen. (Organisatorische und technische Sicherheitsmaßnahmen sind von den jeweiligen GDA festzulegen)

b. *Behandlungszusammenhang:* Ein Zugriff ist nur gestattet, wenn die behandelnde Person in einer für die Behandlung relevanten definierten Beziehung zum Patienten steht (z. B. behandelnder Arzt).
Der Zugriff ist in dem Ausmaß gestattet, wie er für Behandlungszwecke im Rahmen des jeweiligen Aufgabengebietes der jeweiligen Rolle bzw. insbesondere für die Behandlung des Patienten notwendig ist.

c. *Patientenidentifikation:* Patientendatenabfragen dürfen nur mit eindeutig identifizierten Patienten durchgeführt werden.

d. *Sicherheitsvorkehrungen bei der Datenübermittlung:* Die Übermittlung erfolgt nach den Vorgaben des Gesundheitstelematikgesetzes, jedoch nicht nach den Übergangsbestimmungen (wie Ausnahmen für Fax…). Es finden nur Übermittlungen in sicheren Netzwerken statt, oder Übermittlungen, die entsprechend verschlüsselt sind und wo die Identität des Absenders und des Empfängers eindeutig sind und dokumentiert werden.

e. *Verpflichtende Protokollierung:* Aus den Protokollierungsdaten muss eindeutig nachweisbar sein, welche Einzelperson auf welche Daten in welchem Behandlungszusammenhang zugegriffen hat. Aus diesen Daten muss auch die zeitliche Abfolge der Abfragen (Historisierungsfunktion) ersichtlich sein.
Minimaldatensatz:
  - Zeitpunkt des Zugriffes
  - Identifikation des Patienten
  - Namen des Zugreifenden
  - Identifikation des GDA
  - Filterkriterien bei selektierter Abfrage inklusive Ergebnisliste der Abfrage
  - Identifikation der Dokumente, die abgefragt wurden, nicht aber der Dokumentinhalt
  - Die Aufbewahrungsfrist für die Protokolldateien beträgt mindestens 11 Jahre.

f. *Kontrolle:* Pro Jahr werden je Teilnehmer im Verhältnis zur Zahl der Zugriffe Zustimmungserklärungen vom Betreiber des Informationsverbundes, der einem anderen Gremium lt. vertraglicher Grundlage anhand der elektronisch hinterlegten Zustimmungserklärungen beim GDA überprüft. Die Zustimmungserklärungen können auch gesichert auf elektronischem Weg übermittelt werden.

g. *Teilnahme am Gesundheitsinformationsverbundsystem:* Zur Regelung des Informationsverbundes besteht eine eigene vertragliche Grundlage, welche im Anhang beigefügt ist, die insbesondere auch den Haftungsaspekt im Falle eines Missbrauches regelt. Bevor ein GDA diesen Vertrag nicht unterzeichnet hat,

kann er am Informationsverbund nicht teilnehmen.
Im Vertrag ist eine Drittbegünstigungsklausel für die Patienten vorgesehen, damit diesem aus dem Datenverbund keinesfalls ein Schaden entsteht.

b. aus dem Bereich Soziales

1. *Jugendwohlfahrt* (diese Datenanwendung wird – je nach Bundesland – zur Gänze oder in Teilbereichen in Form eines Informationsverbundsystem geführt.): Zweck dieser Datenanwendung ist die Dokumentation und Verrechnung der öffentlichen Jugendwohlfahrt.
2. *Informationsverbundsystem (Soziales):* SIS-Sozialhilfe (SIS-SH)- Soziales Informationssystem zur Durchführung der Angelegenheiten der Sozialhilfe (§ 17 SSHG).
3. *Informationsverbundsysteme »Leitstelle Tirol Einsatzleitsystem« und »LSZ. Burgenland Einsatzleitsystem«:* Mit diesen Datenanwendungen, die in Form eines Informationsverbundsystems geführt werden, wird die Einleitung und Koordinierung von Hilfsmaßnahmen (beginnend mit der Alarmierung der benötigten Hilfsorganisationen), die Einsatzabwicklung, -unterstützung und – verwaltung sowie die Organisation und Koordinierung von Krankentransporten durchgeführt. Betreiber dieser Systeme sind die »Leitstelle Tirol« bzw. die »Landessicherheitszentrale Burgenland GmbH«.

c. aus dem Zuständigkeitsbereich des Bundesministeriums für Inneres

1. *Informationsverbundsystem Betreuungsinformationssystem:* Das Betreuungsinformationssystem, das in Form eines Informationsverbundsystems geführt wird, bezieht sich auf die Gewährleistung der vorübergehenden Grundversorgung für hilfs- und schutzbedürftige Fremde in Österreich (entsprechend der Grundversorgungsvereinbarung gemäß Art. 15a B-VG) Zweck: Gewährleistung der Versorgung von hilfs- und schutzbedürftigen Fremden und Abrechnung der Kosten gemäß Art. 10f der Grundversorgungsvereinbarung.
2. *Informationsverbundsystem Einsatz-Protokoll-System (EPS-WEB):* Zwecke des Einsatz-Protokoll-Systems (EPS-WEB) sind die Leitung, Administration und Koordination von sprengelübergreifenden Einsätzen (insbesondere von sicherheitspolizeilichen Schwerpunktaktionen oder Fahndungen bzw. Einsätzen aus ordnungsdienstlichen Anlässen sowie für den Personen- und Objektschutz und die Erfüllung der ersten allgemeinen Hilfeleistungspflicht)
3. *Informationsverbundsystem Sachenfahndung: Zweck* dieses Informationsverbundsystems ist die Evidenthaltung der Daten von nummerierten Sachen, die zur Fahndung ausgeschrieben wurden.
4. *Informationsverbundsystem Zentrale Gewaltschutzdatei:* Die »Zentrale Gewaltschutzdatei« dient dem Zweck, personenbezogene Daten zur Administration von Wegweisung und Betretungsverbot bei Gewalt in Wohnungen zu verwenden.

d. aus dem Zuständigkeitsbereich des Bundesministeriums für Land- und Forstwirtschaft

1. *Elektronisches Register für Anlagen und Personenstammdaten (»eRAS«) gemäß § 22 Abfallwirtschaftsgesetz 2002 (AWG 2002) und Elektronisches Register für Meldungen gem. Altfahrzeugeverordnung (»eAFZ«):* Das Elektronische Register für Anlagen- und Personenstammdaten (»eRAS«) ist ein rechnergestütztes Datenverwaltungssystem, das Stammdaten abfallwirtschaftlich relevanter Personen und Organisationen aus dem gesamten österreichischen Bundesgebiet und Stammdaten von in Österreich tätigen Abfallsammlern und -behandlern umfasst. Die Datenbank beinhaltet Angaben über natürliche und juristische Personen und über Organisationen, die aufgrund abfallwirtschaftlicher

Rechtsvorschriften registriert sein müssen. Ebenfalls in dieser Datenbank erfasst werden ausländische Personen und Organisationen, soweit dies im Zusammenhang mit der grenzüberschreitenden Verbringung von Abfällen notwendig ist.
Gemäß Altfahrzeugeverordnung sind von Herstellern, Importeuren von Kraftfahrzeugen (KFZs) sowie von Sammlern und Behandlern von Altfahrzeugen, Meldungen über die übernommenen Fahrzeuge (Marke, Type, Fahrzeugidentifikationsnummer etc.) und die Behandlung dieser Altfahrzeuge (Abfallart, Menge, Übernehmer etc.) einmal jährlich elektronisch an das BMLFUW zu übermitteln. Die Anwendung »eAFZ« ist ein Register für Bewegungsdaten gemäß § 22 Abs. 1 Z 2 AWG 2002. Die Anwendung »eAFZ« greift laufend auf die Stammdaten des »eRAS«, dem elektronischen Register für Anlagen- und Personenstammdaten zurück.

2. *Informationsverbundsystem Elektronisches Register für Anlagen- und Personenstammdaten (eRAS) iVm dem Elektronischen Register für Meldungen gem. Elektroaltgeräteverordnung (eEAG):* Gemäß Elektroaltgeräteverordnung sind von Herstellern und Importeuren von elektrischen und elektronischen Geräten sowie von Sammlern, Behandlern und Sammel- und Verwertungssystemen von Elektroaltgeräten Meldungen über die inverkehrgesetzten Geräte (quartalsweise, jährlich) und die gesammelten und behandelten Altgeräte (Kategorie, Menge, Übergeber, Übernehmer etc.) – laufend bzw. einmal jährlich – elektronisch an das BMLFUW zu übermitteln. Für diese Meldungen wurde das Bewegungsdatenregister (Anwendung) eEAG eingerichtet. Die Anwendung eEAG greift laufend auf die Stammdaten im Stammdatenregister eRAS zurück.
(Hinweis: die Abkürzung »EAG« steht für Elektro- und Elektronikgeräte bzw. für Elektro- und Elektronik-Altgeräte)

3. *Informationsverbundsystem Elektronisches Register für Anlagen- und Personenstammdaten (eRAS) – »eBilanzen (für Abfall-Input-Output-Meldungen gemäß § 41 DeponieVO)«*
Zwecke der Datenanwendung:
   1. Meldungen des Abfallinputs und Abfalloutputs für Deponien und andere Anlagen im Deponiebereich
   2. WEBGIS, öffentlicher Zugriff auf Standorte – für alle Abfallsammler und -behandler
   3. Anlagenübertragung / -zuordnung – für alle Abfallsammler und -behandler
   4. Meldung von Zusammenfassungen von Aufzeichnungen auf Verlangen gemäß § 17 Abs. 5 AWG 2002 und § 41 Abs. 5 DeponieVO 2008 an die zuständige Behörde (Hinweis: hier liegt kein Informationsverbundsystem vor).

e. sonstige IVS

1. *Informationsverbundsystem Jagd- und Fischereianwendung Tirol (JAFAT):*
Diese Datenanwendung wird zum Zweck der Überwachung der weidgerechten Ausübung der Jagd, Feststellung von Jagdgebieten, Prüfung von Jagdpachtverträgen, Prüfung eines aufrechten Haftpflichtversicherungsverhältnisses, Durchführung der Jagd-, Jagdaufseher- und Berufsjägerprüfung, Ausstellung und Verweigerung der Ausstellung von Jagdkarten, Einziehung von Jagdkarten, Genehmigung und Überwachung von Abschussplänen und Vorschreibung der Jagdabgabe sowie Ahndung von Verwaltungsübertretungen eingesetzt.
Betreiber des Informationsverbundsystems ist das Amt der Tiroler Landesregierung, teilnehmende Auftraggeber sind die Bezirkshauptmannschaften und das Amt der Tiroler Landesregierung
2. *Informationsverbundsystem Nutzung der Studienbibliothek – Bibliothekensystem ALEPH 500:*
Betreiber des Informationsverbundsystems ist die Österreichische Bibliothe-

kenverbund und Service Gesellschaft m.b.H, teilnehmende Auftraggeber sind die Mitgliedsbibliotheken des Verbundes für Bildung und Kultur.(insbesondere Pädagogische Hochschulen).

3. *Informationsverbundsystem Kundenkontaktmanager sowie damit verbundene Hilfssysteme (Betreiber ÖAMTC):*
   Dieses EDV-System wird zur umfassenden Unterstützung der stationären und mobilen Dienstleistungsabwicklung, d. h. insbesondere die Disposition, die Abwicklung, die Verrechnung und das Inkasso der Dienstleistungen des ÖAMTC eingesetzt.
   Rechtsgrundlagen sind:
   Mitgliedschaft, Vertragsbeziehung zu Kunden, Betriebsvereinbarung über den Einsatz des Kundenkontaktmanagers vom 28.05.2010, Betriebsvereinbarung über die Auswertung von mitarbeiterbezogenen Daten über mobile Dienste aus den Systemen ELOG und MAPL für Pannenhilfe und Abschleppdienst im Internen Club.
   Alle Mitglieder des ÖAMTC bzw. der Landesvereine haben Anspruch auf die angebotenen Leistungen im selben Umfang. Die Übermittlung der Daten an den Betreiber des Informationsverbundsystems Kundenkontaktmanager erfolgt zum Zwecke der umfassenden Unterstützung der stationären und mobilen Dienstleistungsabwicklung, d. h. insbesondere die Disposition, die Abwicklung, die Verrechnung und das Inkasso sämtlicher Dienstleistungen des ÖAMTC. Alle Teilnehmer des Informationsverbundsystems Kundenkontaktmanager müssen über die Art, den Inhalt und den Umfang der an die Mitglieder und Kunden erbrachten Leistungen zur gesetzeskonformen Erfüllung von Gewährleistungs- und/oder Schadenersatzansprüchen (Umtausch, Verbesserung, Rücktritt vom Vertrag, …) sowie zur Erfüllung der gesetzlichen Verpflichtungen zur Führung von Büchern und Aufzeichnungen und zur Erteilung von Auskünften gegenüber den jeweils zuständigen Behörden (§ 57a Pickerüberprüfung – Revision durch die jeweils zuständige Behörde) Kenntnis haben.
4. *Informationsverbundsystem NPO (Personen- und Vertragsverwaltung der Mitgliederdaten im Hinblick auf Mitgliedschaft und Schutzbrief):*
   Betreiber dieses Informationsverbundsystems ist der ÖAMTC.
   Teilnehmenden Auftraggeber sind insbesondere die Landesvereine des ÖAMTC sowie Tochtergesellschaften des ÖAMTC.
   Alle Mitglieder des ÖAMTC bzw. der Landesvereine haben Anspruch auf die angebotenen Leistungen im selben Umfang. Die Übermittlung der Daten an den Betreiber des Informationsverbundsystems NPO erfolgt zum Zwecke der Überprüfung der Berechtigung der Leistungsempfänger für die Inanspruchnahme von Leistungen aus Mitgliedschaft und Schutzbrief in gesamt Österreich. Dies bedeutet, dass beispielsweise ein KATC-Mitglied in Wien dieselben Leistungen aus Mitgliedschaft und Schutzbrief beanspruchen kann wie beispielsweise ein KATC-Mitglied in Kärnten. Um eine österreichweite Sicherstellung der Leistungserbringung zu ermöglichen, ist ein direkter Zugriff auf sämtliche Mitgliederdaten durch den ÖAMTC, die Landesvereine sowie die jeweiligen Tochtergesellschaften erforderlich.

8.2.2.2 Sonstige Meldungen

a. Amt der Stmk Landesregierung

LDF – Landesweite Datenbank zur Förderungsabwicklung: Zentrales Modul im Rahmen des Fördercontrollings. In diesem Modul werden die Stammdaten aller Förderungswerber verarbeitet und wenige Daten betreffend die ihnen bereits gewährten Förderungen. Auf die in diesem Modul verarbeiteten Daten können alle Förderungsstellen des Landes bei Bedarf zugreifen. Zwecke sind – insbesondere im Hinblick auf die Einhaltung von Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit – die Vermeidung von nicht beabsichtigten Mehrfachförderungen

(Förderungsmissbrauch) und Verhinderung von Überförderungen. Beides erfolgt durch eine im Einzelfall vorzunehmende Prüfung, ob für das gleiche oder ähnliche Vorhaben bereits bei einer anderen Förderstelle um eine Förderung angesucht wurde.

b. Bundesministerium für Finanzen
Kraftfahrzeugregister im Abgabeinformationssystem: Mit dieser Datenbank wird eine Kontrolle ermöglicht, dass die in Österreich zugelassenen Kraftfahrzeuge versteuert werden (Umsatzsteuer, Normverbrauchsabgabe, motorbezogene Versicherungssteuer, Kraftfahrzeugsteuer).

c. Wiener Linien GmbH & CO KG
Videoüberwachung in den Fahrzeugen zum Zwecke der Eindämmung von Vandalismusschäden, der Erhöhung des Schutzes von MitarbeiterInnen und Fahrgästen sowie zur Optimierung betrieblicher Abläufe (unbefristete Registrierung)

Bis dato durfte die oben genannte Videoüberwachung lediglich im zeitlich befristeten Probebetrieb durchgeführt werden. Aufgrund des mittlerweile vorgelegten statistischen Zahlenmaterials ist die Datenschutzkommission zur Auffassung gelangt, dass die eingesetzte Videoüberwachung einen positiven Einfluss auf die Schadensverhütung im Bereich der U-Bahn-Garnituren besitzt. Angesichts der auch in ähnlich gelagerten Fällen erwiesenen Eignung von Videoüberwachung zur Minderung von Schadensfällen beim Betrieb öffentlicher Verkehrsmittel wurde eine zeitlich unbegrenzte Registrierung der Videoüberwachung in den Fahrzeugen der Wiener Linien GmbH & Co KG für sachlich gerechtfertigt angesehen.

Die Registrierung erfolgte unter folgenden Auflagen:

- Videoüberwachungsdaten dürfen nur in verschlüsselter Form gespeichert werden.
- Die Speicherdauer darf 120 Stunden nicht überschreiten.
- Die Auswertung von Videoaufzeichnungen bei der Antragstellerin ist nur für Zwecke des Eigenschutzes oder des Verantwortungsschutzes zulässig, und zwar nur dann, wenn der begründete Verdacht besteht, dass einer der in der Registrierung festgelegten Anlassfälle für die Vornahme von Videoüberwachung eingetreten ist.
- Die Weitergabe von Videoaufzeichnungen für Zwecke des Fremdschutzes ist nur in den gesetzlich ausdrücklich vorgesehenen Fällen (insbes. §§ 110 ff StPO) zulässig.

d. Magistrat der Stadt Wien
Videoüberwachung des Wiener Krankenanstaltenverbundes in speziellen Gefährdungsbereichen in der psychiatrischen und forensischen Abteilung (Befristete Registrierung bis 31. Dezember 2014)

Die Videoüberwachung erfolgt zum Zwecke des Personenschutzes, zur Vorbeugung strafrechtsrelevanter Strafbestände sowie zum Auffinden abgängiger und zur Beobachtung gefährdeter PatientInnen und BewohnerInnen.

Es darf keine permanente Bildaufzeichnung durchgeführt werden, sondern lediglich eine Live-Bild-Überwachung mit der Möglichkeit einer Auslösung der Bildaufzeichnung im Alarmfall. Eine Bildaufzeichnung darf ausschließlich im konkreten Anlassfall zur Wahrung lebenswichtiger Interessen von PatientInnen oder von Dritten (bei unmittelbaren oder unmittelbar drohenden Gefährdungssituationen) ausgelöst werden. Jede Aufzeichnungsauslösung ist zu dokumentieren und die Bilddaten zu verschlüsseln.

e. Smart Metering für den Netzbetrieb und die Energieberatung
Automatic Meter Readout (AMR): Das System dient zur Erfassung und zur Speicherung von detaillierten Daten über den Energieverbrauch von Kundenanlagen sowie über die Netzstabilität und Versorgungssicherheit.

Zwecke des AMR-Systems:
- Sicherung und Verbesserung der Versorgungs- und Netzqualität
- Schaffung einer verlässlichen Entschei-

dungsgrundlage für Netzausbauten und Investitionsentscheidungen
- Behandlung von Kundenbeschwerden, Fehlerlokalisierung und Fehlerbehebung
- Individuelle Energieberatung

8.3 DVR-Online

8.3.1 Darstellung der bereits operationalen Verbesserungen im Verfahrensablauf durch das neue System

In den letzten Datenschutzberichten 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.

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. 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 (z. B. 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.

8.3.2 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 Betreibern von Informationsverbundsystemen folgende Funktionalitäten zur Verfügung stehen:

In der Applikation DVR-Online können Bürger ohne Authentifizierung im öffentlichen Teil des Datenverarbeitungsregisters recherchieren.

Auftraggeber und Betreiber von Informationssystemen haben nach Anmeldung mit der Bürgerkarte oder über das Unternehmensserviceportal Zugang zu DVR-Online.

Für die Authentifizierung der Benutzer werden bei Verwendung der Bürgerkarte bestehende E-Government-Strukturen genutzt. 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 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.

Auftraggeber können elektronisch

DVR-Meldungen einbringen. Nach Klick auf den Button »Versenden« wird die Meldung in den Arbeitsvorrat des DVR weitergeleitet, oder wenn die Voraussetzungen für eine automatische Registrierung vorliegen, automatisch registriert. Der betreffende Auftraggeber hat Einsicht in die von ihm eingebrachten Meldungen samt Beilagen und kann für eine Änderungsmeldung seine registrierte Datenanwendung wieder aufsuchen und die entsprechenden Änderungen im Formular vornehmen.

Betreiber von Informationsverbundsystemen haben die Möglichkeit, eine IVS-Gesamtmeldung zu erstatten. Die am Informationsverbundsystem teilnehmenden Auftraggeber können durch Klick auf den Button »Auftraggeber übernehmen« oder »Auftraggeber neu registrieren« hinzugefügt werden.

Die Erfassung der Meldungen erfolgt in Hinkunft somit grundsätzlich nicht mehr durch DVR-Bedienstete sondern durch die Auftraggeber oder die Betreiber von Informationsverbundsystemen.

Weiters ist vorgesehen, dass eine Registrierung von Verarbeitungen, die nicht vorabkontrollpflichtig sind, aufgrund einer Plausibilitätskontrolle voll automatisch möglich ist. Die Mitteilung über die Registrierung wird diesfalls elektronisch zugestellt. Als Zeithorizont für die allgemeine Nutzbarkeit von DVR-Online ist aufgrund einer gesetzlichen Regelung spätestens September 2012 vorgesehen.

9 Die Datenschutzkommission als Stammzahlenregisterbehörde

9.1 Die Funktionen der Stammzahlenregisterbehörde

9.1.1 Bereichsspezifische Personenkennzeichen

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 DSK in ihrer Funktion als Stammzahlenregisterbehörde verwaltet.

Die Stammzahlenregisterbehörde erzeugt bereichsspezifische Personenkennzeichen, stellt Anwendungen zur Erzeugung von bereichsspezifischen Kennzeichen auf Grundlage der Stammzahl zur Verfügung und stellt sicher, dass diese richtig eingesetzt werden. Zu diesem Zweck müssen Auftraggeber des öffentlichen Bereichs einen Antrag bei der Stammzahlenregisterbehörde auf Erlaubnis der Ausstattung einer Datenanwendung mit bPKs stellen. Anlässlich der Erlaubniserteilung wird von der Stammzahlenregisterbehörde festgelegt, welchem Bereich die Datenanwendung zuzurechnen ist und mit welcher Bereichskennung daher die bPKs für diese Datenanwendung zu bilden sind.

Dieses im österreichischen E-Government eingesetzte System der bereichsspezifischen Personenkennzeichen stellt sicher, dass die eindeutig erzeugten Identifikatoren für ein- und dieselbe Person in unterschiedlichen Bereichen der öffentlichen Verwaltung unterschiedlich sind, innerhalb dieses Bereiches aber eindeutig. Das erleichtert der öffentlichen Verwaltung die Zuordnung von Personen zu Verfahren, erlaubt es den betroffenen Bürgern mit einem einzigen sicheren Mechanismus immer mehr öffentliche Dienstleistungen bequem elektronisch abzuwickeln und schützt gleichzeitig die betroffenen Bürger vor einer leichteren Zusammenführbarkeit seiner Daten durch die Einführung von Personenkennzeichen. Ein bereichsspezifisches Personenkennzeichen kann weder auf die Stammzahl zurückgerechnet werden, noch – ohne zusätzliche Angaben über die Person und der Mitwirkung der Stammzahlenregisterbehörde – in ein bereichsspezifisches Personenkennzeichen eines anderen Bereichs umgerechnet werden.

Im Jahr 2010 wurden von der Stammzahlenregisterbehörde

- 26.773.000 bereichsspezifische Personenkennzeichen und
- 73.831.000 verschlüsselte bereichsspezifische Personenkennzeichen

und im Jahr 2011 wurden von der Stammzahlenregisterbehörde

- 19.882.317 bereichsspezifische Personenkennzeichen und
- 17.570.366 verschlüsselte bereichsspezifische Personenkennzeichen berechnet.

Die verschlüsselten bPKs dienen dem Verkehr zwischen Behörden unterschiedlicher Verwaltungsbereiche.

9.1.2 Ergänzungsregister

Die DSK betreibt in ihrer Funktion als Stammzahlenregisterbehörde weiters zwei Register, in die sich jene natürlichen Personen und sonstige rechtlich erhebliche Entitäten (z. B. Behörden oder ARGEs) eintragen lassen können, die in keinem der Basisregister des E-Governmentsystems (Firmenbuch, Zentrales Melderegister oder Vereinsregister) 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).

9.2 Entwicklungen

9.2.1 Bereichsspezifische Kennzeichen für die Verwendung im privaten Bereich

Die wichtigste Neuerung der Novelle zum E-Government-Gesetz (BGBl. I Nr. 7/2008) bestand 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 oder der TAC Systeme. Mit einem gemeinsamen Zugangssystem für Angebote der öffentlichen Verwaltung und der Privatwirtschaft würde auch das Problem des Merkens von unterschiedlichen Passwörtern für die unterschiedlichen Zugangssysteme erheblich entschärft werden. Von diesem Angebot haben diese Unternehmen allerdings bisher keinen Gebrauch gemacht.

9.2.2 Organisatorische und personelle Probleme

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, diese Anträge manuell zu behandeln hat, wofür ihre Personalausstattung nicht ausreicht.

Gleiches gilt auch für die aus datenschutzrechtlicher Sicht wichtigen Kontrollen von öffentlichen und privaten Einrichtungen, die bereichsspezifische Personenkennzeichen verwenden. In diesem Bereich wird daher noch nachgerüstet werden müssen, sowohl durch technische Maßnahmen, personelle Verstärkung und durch Heranziehung weiterer Dienstleister für spezielle Funktionen.

9.2.3 Volkszählung 2011

Die im Datenschutzbericht 2008-2009 beschriebene Volkszählung 2011, die als Registerzählung durchgeführt wird, konnte erfolgreich vorbereitet werden. Diese Vorbereitungen haben zu einer beschleunigten Verbreitung von bereichsspezifischen Personenkennzeichen geführt in Bereichen, die an sich nicht geplant hatten, ihre Datenanwendungen E-Government tauglich zu machen. Die sich daraus ergebenden neuen Szenarien der Verwendung von bereichsspezifischen Personenkennzeichen werden in den nächsten Jahren zusammen mit der Evaluierung der Volkszählung einer genaueren Analyse zugeführt werden müssen.

Kurz zusammengefasst wurde mit dem Registerzählungsgesetz, BGBl. I Nr. 33/2006, 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 das Register des Hauptverbandes der österreichischen Sozialversicherungsträger, die Daten des Arbeitsmarktservice und die Stammdaten der Abgabenbehörden des Bundes (nicht jedoch die Einkommensdaten). Bei der Registerzählung werden die Daten aus den teilnehmenden Registern nicht mit den Namen der Betroffenen, sondern ausschließlich mit seinem bereichsspezifischen Personenkennzeichen (bPK) an die Bundesanstalt Statistik Österreich geliefert. Da dieses bPK nicht mit dem Namen der Person verknüpft werden darf, können die

gesammelten Informationen nicht auf eine bestimmte Person zurückgeführt werden. Durch dieses neue System statistischer »Zählungen« der Bevölkerung unter verschiedensten Gesichtspunkten (Fragestellungen) wurde datenschutzrechtlich ein erheblicher Fortschritt erzielt, da anstelle von identifizierten Bürgern nur mehr nichtidentifizierte Individuen gezählt werden.

9.3 Behördenstruktur, Neuerungen und Veränderungen

9.3.1 Zusammenarbeit mit und zwischen den Dienstleistern der Stammzahlenregisterbehörde

Im Berichtszeitraum war die Stammzahlenregisterbehörde neben der Führung und Überwachung des laufenden Betriebs der verschiedenen technischen Einrichtungen und der mit der Umsetzung beauftragten Dienstleister und der Betreuung öffentlicher Auftraggeber im Zusammenhang mit der Ausstattung ihrer Datenanwendungen mit bereichsspezifischen Personenkennzeichen vor allem mit dem Aufbau einer informellen Struktur der Arbeitsabläufe und der Entwicklung technischer Hilfsmittel beschäftigt, die zur besseren Steuerung und Bewältigung dieser Aufgaben im Umfeld der besonderen personellen Struktur der Stammzahlenregisterbehörde beitragen.

Neben der DSK als verantwortlicher Behörde sind für die DSK mehrere Bundesministerien als Dienstleister wie auch private Unternehmen als Subdienstleister tätig. Der Betrieb der Datenanwendungen als auch die Steuerung der Arbeitsabläufe der Stammzahlenregisterbehörde, die sich auf viele Personen, die bei unterschiedlichen Behörden und Unternehmen beschäftigt sind, stellt daher eine ständige besondere Herausforderung dar.

In diesem Zusammenhang muss darauf hingewiesen werden, dass es unvorhersehbar umfangreiche personelle und organisatorische Veränderungen beim Dienstleister »Support Unit ZMR« gegeben hat, die kurz vor dem Ende des Berichtszeitraumes dazu geführt haben, dass ein Großteil der Mitarbeiter, die mit dem Betrieb der Anwendungen »Stammzahlenregister« (Errechnung von Stammzahlen, bereichsspezifischen Personenkennzeichen und verschlüsselten bereichsspezifischen Personenkennzeichen) und Ergänzungsregister für natürliche Personen betraut waren, die Behörde verlassen hat. Neben dem damit einhergehenden Know-how Verlust ist auch die in den vergangenen Jahren gemeinsam geschaffene Arbeitsroutine großteils verloren gegangen. Die sich daraus ergebenden Probleme werden genauer untersucht werden müssen. Die DSK wird versuchen, die sich dadurch ergebenden Verzögerungen und Betriebseinschränkungen bei den betroffenen Datenanwendungen und Serviceleistungen der Stammzahlenregisterbehörde in vertretbaren Grenzen zu halten.

9.3.2 Bürgerkartenfunktion am Mobiltelefon

Die Einführung der für den Nutzer kostenfreien Bürgerkartenfunktion mit Hilfe seines Mobiltelefons ist die im Berichtszeitraum wesentlichste Veränderung im Aufgabenbereich der Stammzahlenregisterbehörde. Der sichere Zugang zu E-Government Datenanwendungen wurde dadurch vereinfacht. Anwender müssen kein externes Lesegerät verwenden und auch keine besondere Software auf ihren Geräten installieren, sondern können sich mit ihrem Mobiltelefon eindeutig identifizieren und Dokumente signieren.

Zu diesem Zweck werden die Funktionen der Chipkarte – insbesondere das Bereithalten der Stammzahl – auf einem sicheren Server bereitgehalten. Auch wenn diese Methode sowohl den Anforderungen des E-Government-Gesetzes (BGBl. I Nr. 10/2004 idgF) als auch des Signaturgesetzes (BGBl. I Nr. 190/1999) vollständig entspricht, muss darauf hingewiesen werden, dass der Zugang mittels Karte und eines externen Lesegerätes mit Ziffernblock mehr Sicherheit bietet und daher das von der DSK empfohlene Mittel ist.

9.3.3 Ergänzungsregister für sonstige Betroffene, Unternehmensserviceportal

Im Zuge der Umsetzung des Unternehmensserviceportalgesetzes (BGBl. I Nr. 52/2009 idgF) wurde damit begonnen, das Ergänzungsregister für sonstige Betroffene (www.ersb.gv.at) zu erneuern und auf die Aufgaben vorzubereiten, die es im Zusammenhang mit der Verwaltung von Vertretungsbefugnissen für den Zugang zum Unternehmensserviceportal und den bereitgestellten Anwendungen (u. a. auch dem DVR) haben wird.