Vorblatt

Ziel und Inhalt:

Der vorliegende Gesetzentwurf

- weist die Zuständigkeit zur Gesetzgebung und Vollziehung des Datenschutzes zur Gänze dem Bund zu, um die Zersplitterung dieser Materie zu beseitigen;

- fasst das Grundrecht auf Datenschutz in eine sprachlich verbesserte Form;

- enthält Bestimmungen über die Zulässigkeit von Videoüberwachung vor allem für Private (einschl. Privatwirtschaftsverwaltung) sowie begleitende Regelungen betreffend Meldepflicht, Registrierungsverfahren, Informationspflichten und Auskunftsrecht;

- verbessert den Rechtsschutz durch eine präzisere Regelung des Beschwerdeverfahrens vor der Datenschutzkommission und durch die Vermeidung von Doppelgleisigkeiten;

- schlägt eine starke Vereinfachung des Registrierungsverfahrens bei gleichzeitiger Steigerung seiner Effizienz vor;

- enthält Klarstellungen von in der Vollzugspraxis aufgetretener Rechtsfragen.

Alternativen:

Keine

Auswirkungen des Regelungsvorhabens:

- Finanzielle Auswirkungen:

Durch die teils massive Einschränkung von Prüf- bzw. Meldepflichten im Registrierungsverfahren sind Arbeitsentlastungen größeren Ausmaßes im Bereich des Datenverarbeitungsregisters und damit bei der vom Bund auszustattenden Datenschutzkommission zu erwarten, die zur Entschärfung der angespannten Personalsituation beitragen sollen. Weitere Entlastungen der Datenschutzkommission ergeben sich aus der Schaffung der Möglichkeit von für den Auftraggeber verbindlichen einseitigen Zusagen im Registrierungsverfahren sowie dem Genehmigungsverfahren im internationalen Datenverkehr.

Durch die vorgeschlagene Kompetenzbereinigung, wonach die Gesetzgebung und die Vollziehung in Angelegenheiten des Schutzes personenbezogener Daten künftig zur Gänze Bundessache sein soll, ist als Auswirkung auf andere Gebietskörperschaften eine vollständige Entlastung der Länder zu erwarten. Da bereits auf Grund der geltenden Kompetenzlage Gesetzgebung und Vollziehung weitestgehend Bundessache ist und entsprechende Strukturen bereits gegeben sind, ist andererseits für den Bund kein Kostenzuwachs zu erwarten.

- Wirtschaftspolitische Auswirkungen:

-- Auswirkungen auf die Beschäftigungslage und den Wirtschaftsstandort Österreich:

Durch die Regelung der Videoüberwachung wird die Rechtssicherheit verbessert, was zur Vermeidung frustrierten Aufwands für Videoanlagen, die sich im Nachhinein als unzulässig erweisen, führen kann. Auch durch die Verkürzung der Registrierungsverfahren steht schneller als bisher fest, ob mit einer Datenanwendung begonnen werden darf. Die neuen Sanktionen für die Vernachlässigung der Meldepflicht stellen Chancengleichheit im Wettbewerb sicher.

-- Auswirkungen auf die Verwaltungslasten für Unternehmen:

Eine marginale Belastung für Unternehmen kann dadurch entstehen, dass vom Auskunftsberechtigten irrtümlich in Anspruch genommene Dienstleister den Auftraggeber bekanntgeben müssen.

Zu marginalen Entlastungen kommt es – auch für Unternehmen - durch die Schaffung von einseitigen Zusagen gegenüber der Datenschutzkommission

- Auswirkungen in umweltpolitischer, konsumentenschutzpolitischer sowie sozialer Hinsicht:

Keine

- Geschlechtsspezifische Auswirkungen:

Keine

Verhältnis zu Rechtsvorschriften der Europäischen Union:

Die vorgesehenen Regelungen bewegen sich innerhalb des durch die Richtlinie 95/46/EG vorgegebenen Umsetzungsrahmens.

Besonderheiten des Normsetzungsverfahrens:

Der Entwurf kann gemäß Art. 44 Abs. 1 B-VG vom Nationalrat nur in Anwesenheit von mindestens der Hälfte der Mitglieder und mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen beschlossen werden und bedarf überdies gemäß Art. 44 Abs. 2 B-VG der in Anwesenheit von mindestens der Hälfte der Mitglieder und mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen zu erteilenden Zustimmung des Bundesrates.

Erläuterungen

Allgemeiner Teil

Hauptgesichtspunkte des Entwurfes:

Das DSG 2000 ist seit seinem Inkrafttreten am 1. Jänner 2000 nur zweimal punktuell novelliert worden. Der vorliegende Entwurf stellt demgegenüber die erste umfassende Novelle dar, die ihre Motivation vor allem aus den im Vollzug aufgetretenen Problemen schöpft, wie sie in Anfragen von Rechtsunterworfenen, in Entscheidungen der Datenschutzkommission, des VwGH und des VfGH sowie in den Datenschutzberichten zu Tage treten. Besonders hervorzuheben ist die aus dem Alltag fast nicht mehr wegzudenkende Videoüberwachung, der das DSG 2000 in seiner derzeitigen Fassung, die noch auf dem Konzept klassischer Datenbanken aufbaut, keine besondere Aufmerksamkeit schenkt. Ziel war in Anbetracht der stetig steigenden Belastung des Datenverarbeitungsregisters weiters eine massive Vereinfachung des Registrierungsverfahrens bei gleichzeitiger Steigerung der Qualität des Datenverarbeitungsregisters, was auch durch eine klarere Regelung der Reaktionsmöglichkeiten der Datenschutzkommission im Fall der Nichterfüllung einer Meldepflicht erreicht werden soll. Schließlich enthält die Novelle eine verständlichere Formulierung einiger Bestimmungen (ohne wesentliche Veränderung des Inhalts), insbesondere auch des Grundrechts auf Datenschutz, sowie eine Bereinigung der unübersichtlichen Kompetenzrechtslage.

Als Inkrafttretenszeitpunkt ist der 1. Jänner 2010 vorgesehen.

Finanzielle Auswirkungen:

- Auswirkungen auf andere Gebietskörperschaften:

Durch die vorgeschlagene Kompetenzbereinigung (Art. 10 Abs. 1 Z 13 B-VG), wonach die Gesetzgebung und die Vollziehung in Angelegenheiten des Schutzes personenbezogener Daten künftig zur Gänze Bundessache sein soll, ist eine vollständige Entlastung der Länder zu erwarten.

- Auswirkungen auf den Bundeshaushalt:

Für die Anschaffung einer Datenbank zur Führung des Datenverarbeitungsregisters (§ 16 Abs. 3) fallen beim Bund keine zusätzlichen Kosten an, da die Entwicklung der Software unabhängig von der DSG-Novelle im Auftrag gegeben und auch bereits gezahlt wurde, um die alte unbrauchbare Software zu ersetzen. Die Freischaltung der automatischen Registrierung ist mit keinen zusätzlichen Kosten verbunden.

Durch die Schaffung der Möglichkeit, dass der meldende Auftraggeber gegenüber der Datenschutzkommission einseitige verbindliche Zusagen abgibt, sollte die Datenschutzkommission in diesen Fällen von der Führung längerer Verfahren, die zum Ausspruch von Auflagen oder Bedingungen führen, entlastet werden. Ähnliches gilt für die Genehmigungsverfahren im internationalen Datenverkehr.

- Auswirkungen auf den Stellenplan des Bundes:

Die vorgeschlagenen Änderungen haben keine Auswirkungen auf den Stellenplan des Bundes, sie zielen vielmehr auf die Entlastung des Datenverarbeitungsregister (und damit der Datenschutzkommission) ab:

• Im Registrierungsverfahren soll eine beträchtliche Entlastung durch die Reduktion der inhaltlichen ex-ante-Prüfung von Meldungen auf Fälle vorabkontrollpflichtiger Datenanwendungen erfolgen, während sonst im Allgemeinen nur eine automationsunterstützte Kontrolle vorgenommen wird.

• Im Registrierungsverfahren für Informationsverbundsysteme (§ 50 Abs. 2 und 2a) ist durch verschiedene Maßnahmen – Übertragungsmöglichkeit der Meldepflichten mehrerer/einer Vielzahl von Auftraggebern auf den Betreiber sowie die Möglichkeit einer „Verweismeldung“ – eine Entlastung der Datenschutzkommission einschließlich des Datenverarbeitungsregisters durch eine geringere Anzahl von Meldungen und Erledigungen zu erwarten.

- Auswirkungen auf Verwaltungslasten für Unternehmen:

Vorweg ist festzuhalten, dass derzeit insgesamt nur etwa 1 500 bis 1 800 Unternehmen eine Videoüberwachung gemeldet haben. Für das gesamte Jahr 2009 kann erwartet werden, dass zwischen 700 und 800 Unternehmen eine Videoüberwachung melden werden.

Nicht näher zu beziffern sind die Verwaltungslasten, die Unternehmen durch die – gewiss sehr seltenen – Fälle entstehen, in denen sie als bloße Dienstleister einer Datenverarbeitung Auskunft über den Auftraggeber zu geben haben (§ 26 Abs. 10). Die Durchsicht der im Rechtsinformationssystem des

Bundes veröffentlichten Entscheidungen der Datenschutzkommission seit dem Jahr 2004 ergab, dass sich lediglich ein einziger Fall auf die Abgrenzung zwischen Auftraggeber und Dienstleister bezog, sodass davon auszugehen ist, dass diese neue Auskunftsverpflichtung ebenfalls keine wesentlichen Auswirkungen auf die Verwaltungslasten für Unternehmen hat und daher unter die Bagatellgrenze des § 5 Abs. 1 der Standardkostenmodell-Richtlinien, BGBl. II Nr. 233/2007, fällt.

Eine Minderung der Verwaltungslasten entsteht durch die Möglichkeit, Meldungen an das Datenverarbeitungsregister künftig online vornehmen zu können (§ 17 Abs. 1a, § 20 Abs. 1). Eine genaue Kalkulation der Berechnung soll im Zuge einer Novellierung der Datenverarbeitungsregister-Verordnung 2002, BGBl. II Nr. 24/2002, erfolgen.

Die Schaffung der Möglichkeit verbindlicher einseitiger Erklärungen entlastet in marginalem Ausmaß auch Unternehmen: Sie werden sich in vielen Fällen weitere Verfahrensschritte (Verbesserung, Äußerung im Parteiengehör) ersparen.

Durch die Melde-, Protokollierungs-, Informations- und Auskunftspflicht bei Videoüberwachung (§§ 50b bis 50e) sind gegenüber der gegenwärtigen Rechtslage keine bzw. nur unter der Bagatellgrenze liegende Änderungen an zusätzlichen Verwaltungslasten zu erwarten.

Im Detail wird durch die Protokollierungspflicht des § 50b Abs. 1 keine neue Verwaltungslast geschaffen, da die Protokollierungspflicht bei Datenverwendungen im Allgemeinen bereits auf Grund von § 14 DSG 2000 vorgesehen ist und im Hinblick auf die Verwendung einer Videoüberwachung in § 50b Abs. 1 nochmals aus systematischen Gründen wiederholt wird. Nachdem bereits nach geltender Rechtslage keine zeitlich unbegrenzte Aufbewahrung von aufgezeichneten Daten vorgesehen ist, führt die – zumeist wohl automationsunterstützt durchgeführte – Löschung von aufgezeichneten Daten zu keiner zusätzlichen Verwaltungslast für Unternehmen. Bezüglich der Möglichkeit der Stellung eines Antrages auf Festsetzung einer längeren Aufbewahrungsdauer gemäß § 50b Abs. 2 wird davon ausgegangen, dass auf Grund der Vorgabe, dass dieser Antrag „tunlichst“ mit der Meldung zu verbinden ist, allenfalls zusätzliche Verwaltungslasten unter der Bagatellgrenze zu erwarten sind.

§ 50c hält fest, dass Videoüberwachungen grundsätzlich der Vorabkontrolle (§ 18 Abs. 2) unterliegen. Damit wird in dem für die Videoüberwachung neu vorgesehenen Abschnitt 9a bloß die derzeit ohnehin bereits geltende Rechtslage auf Grund der thematischen Zugehörigkeit nochmals wiedergegeben. § 96a des Arbeitsverfassungsgesetzes 1974, BGBl. Nr. 22, legt in der geltenden Fassung zudem bereits fest, dass die Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen, zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrates bedürfen. Eine Zustimmung ist nicht erforderlich, soweit die tatsächliche oder vorgesehene Verwendung dieser Daten über die Erfüllung von Verpflichtungen nicht hinausgeht, die sich aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag ergeben. Der Hinweis auf die Notwendigkeit des Abschlusses einer Betriebsvereinbarung in § 50c dient nur der Klarstellung und ergibt sich sohin bereits aus geltenden Rechtsnormen. Ebenfalls wird bereits nach geltendem Recht bei der Erstattung einer Meldung die Glaubhaftmachung bestimmter Tatsachen vorausgesetzt (zB durch Vorlage von statistischem Zahlenmaterial), weshalb sich aus § 50c Abs. 1 keine neuen Verwaltungslasten der Unternehmen ergeben. Darüber hinaus ist festzuhalten, dass auf Grund der geltenden Rechtslage schon bestehende Verwaltungslasten im Zusammenhang mit der Meldung einer Datenanwendung dem § 4 der Datenverarbeitungsregister-Verordnung 2002, BGBl. II Nr. 24/2002, zugerechnet werden, da diese Regelung konkret festlegt, dass der Auftraggeber einer Datenanwendung der Datenschutzkommission gemäß §§ 17 und 19 DSG 2000 die in Z 1 bis 6 angeführten Datenarten zu melden hat.

Zu § 50d ist anzumerken, dass dem Auftraggeber die geeignete Kennzeichnung einer Videoüberwachung bereits nach geltendem Recht in der Form von Auflagen aufgetragen wird. Dass darüber hinaus die Kennzeichnung in der Art zu erfolgen hat, dass der potentiell Betroffene „tunlichst“ die Möglichkeit hat, der Videoüberwachung auszuweichen, verursacht für Unternehmer allenfalls eine zusätzliche Verwaltungslast unter der Bagatellgrenze.

§ 50e Abs. 1 sieht bei Videoüberwachungen, abweichend von dem in § 26 Abs. 1 DSG 2000 geregelten Auskunftsrecht, die Übersendung einer Kopie bzw. alternativ eine Einsichtsnahme auf Lesegeräten des Auftraggebers sowie im Fall des § 50e Abs. 2 eine schriftlich Beschreibung bzw. alternativ die Einsichtnahme unter Unkenntlichmachung der betroffenen „Dritten“ vor. Vorweg ist festzuhalten, dass die Auskunftserteilung bei Videoüberwachung relativ selten zu Verwaltungslasten bei Unternehmen führen wird, da diese Daten im Regelfall des § 50b Abs. 2 bereits nach 48 Stunden zu löschen sind und davon auszugehen ist, dass nur eine sehr geringe Anzahl von Auskunftsbegehren innerhalb von 48 Stunden nach der Videoaufnahme gestellt werden wird. Im Besonderen wird auch darauf hingewiesen,

dass in den Fällen der Echtzeitüberwachung ein Auskunftsrecht ausgeschlossen ist. Aus diesen Gründen ist anzunehmen, dass das in § 50e Abs. 1 und 2 vorgesehene Auskunftsbegehren für Unternehmen keine über die Bagatellgrenzen hinausgehenden zusätzlichen Verwaltungslasten verursachen wird.

Zur in Art. 3 vorgesehenen Rechtsgrundlage für die Echtzeitüberwachung durch Sicherheitsbehörden ist zu bemerken, dass allfällige Zusatzaufwendungen bei den Sicherheitsbehörden im Zusammenhang mit der Anschaffung und dem Betrieb der Echtzeitbildübertragungsanlagen im Budgetrahmen des Bundesministeriums für Inneres ihre Bedeckung finden.

Kompetenzgrundlage:

Der vorliegende Entwurf stützt sich hinsichtlich der Verfassungsbestimmungen auf Art. 10 Abs. 1 Z 1 B-VG („Bundesverfassung“), im Übrigen auf den vorgeschlagenen Kompetenztatbestand „Schutz personenbezogener Daten“ (Art. 10 Abs. 1 Z 13 B-VG).

Besonderheiten des Normerzeugungsverfahrens:

Art. 1 sowie Art. 2 Z 8, 10, 11, 12, 13, 14, 15, 66 und 93 sind Verfassungsbestimmungen und können gemäß Art. 44 Abs. 1 B-VG vom Nationalrat nur in Anwesenheit von mindestens der Hälfte der Mitglieder und mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen beschlossen werden. Da durch Art. 1 Z 1 iVm Art. 2 Z 12 überdies die Zuständigkeit der Länder eingeschränkt wird, ist gemäß Art. 44 Abs. 2 B-VG auch die in Anwesenheit von mindestens der Hälfte der Mitglieder und mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen zu erteilende Zustimmung des Bundesrates erforderlich.

Besonderer Teil

Zu Art. 1 (Änderung des Bundes-Verfassungsgesetzes) sowie Art. 2 Z 12 (Entfall von § 2 DSG 2000):

Im Sinne des Kodifikationsgedankens sollen die derzeit in § 2 DSG 2000 enthaltenen kompetenzrechtlichen Regelungen in das B-VG integriert werden.

Die bisherige Kompetenzrechtslage auf dem Gebiet des Datenschutzes erwies sich vor allem seit Inkrafttreten der Richtlinie 95/46/EG, die sowohl für automationsunterstützt als auch für konventionell (manuell) in einer Datei geführte Datenanwendungen gilt, als unzweckmäßig. Infolge der zwischen Bund und Ländern geteilten Gesetzgebungskompetenz musste diese Richtlinie durch das DSG 2000 und eigene Datenschutzgesetze der Länder umgesetzt werden, wobei der den Ländern – zufolge der Vorgaben der Richtlinie und des Grundrechts auf Datenschutz gemäß § 1 DSG 2000 – verbliebene Gestaltungsspielraum äußerst gering war.

Durch den vorgeschlagenen Kompetenztatbestand entfällt die bislang in § 2 Abs. 1 DSG 2000 enthaltene Einschränkung der Gesetzgebungszuständigkeit des Bundes auf den Schutz personenbezogener Daten im automationsunterstützten Datenverkehr. Dadurch soll der Bund in die Lage versetzt werden, die Richtlinie 95/46/EG vollständig, also auch hinsichtlich manueller Daten umzusetzen.

Von der (umfassenden) Zuständigkeit des Bundes für den Datenschutz unberührt bleibt die Zuständigkeit zur Erlassung von auf einen bestimmten Gegenstand bezogenen Regelungen über die Daten*verwendung*; sie folgt der Zuständigkeit zur Regelung der jeweiligen Materie. Nicht zum Kompetenztatbestand Datenschutz zählt auch die Regelung der Zuständigkeit der Verwaltungsstrafbehörden (vgl. § 52 Abs. 5 DSG 2000); solche Regelungen gründen sich auf die Bedarfskompetenz „Verwaltungsstrafverfahren“ (Art. 11 Abs. 2 B-VG; vgl. *Thienel*, Das Verfahren der Verwaltungssenate, 2. Aufl. [1992] 205 ff).

Gleichzeitig treten die landesrechtlichen Vorschriften in den Angelegenheiten des Datenschutzes außer Kraft. Es sind dies die im Kärntner Gesetz über Auskunftspflicht, Datenschutz und Statistik – K-ISG, im Oberösterreichischem Auskunftspflicht-, Datenschutz- und Informationsweiterverwendungsgesetz und im Salzburger Gesetz über Auskunftspflicht, Datenschutz und Landesstatistik enthaltenen Datenschutzregelungen sowie das Niederösterreichische Datenschutzgesetz – NÖ DSG, das Steiermärkische Datenschutzgesetz – StDSG, das Vorarlberger Landes-Datenschutzgesetz, das Wiener Datenschutzgesetz – WrDSG, das Tiroler Datenschutzgesetz – TDSG und das Burgenländische Datenschutzgesetz – Bgld DSG.

Die den Ländern gemäß § 2 Abs. 2 zweiter Satz DSG 2000 vorbehaltene Zuständigkeit zur Vollziehung stand unter dem Vorbehalt, dass bundesgesetzlich nicht die Vollziehung durch die Datenschutzkommission, den Datenschutzrat oder die Gerichte, also eine Vollziehung durch Bundesorgane vorgesehen war. Darüber hinaus war die Landeszuständigkeit durch § 1 Abs. 5 DSG 2000 beschränkt, sodass für die Vollziehung des DSG 2000 durch die Länder ohnedies nur ein „Restbereich“ blieb (vgl. *Duschanek*, § 2 DSG, in: Korinek/Holoubek, Bundesverfassungsrecht, 5. Lfg [2005] Rz 21).

Nunmehr soll auch die Vollziehung des Datenschutzrechts zur Gänze beim Bund liegen und von diesem in unmittelbarer Bundesverwaltung (Art. 102 Abs. 2 B-VG) vollzogen werden können.

Keine Vollziehung des Datenschutzrechts stellt die Verwendung von personenbezogenen Daten durch Länder und Gemeinden als Auftraggeber dar.

Zu Art. 2 (Änderung des Datenschutzgesetzes 2000):

Zu Art. 2 Z 8 und 16 (Aufhebung der Überschrift „Artikel 1 (Verfassungsbestimmung)“ und der Überschrift „Artikel 2“)

Die im DSG 2000 enthaltene Gliederung in einen als Verfassungsbestimmung erlassenen Art. 1 und einen die einfachgesetzlichen (aber auch vereinzelte verfassungsgesetzliche) Bestimmungen enthaltenden Art. 2 soll aus gesetzessystematischen Gründen aufgehoben werden.

Zu Art. 2 Z 10 und 11 (§ 1):

Durch die vorgeschlagene Änderung soll das Grundrecht auf Datenschutz verständlicher formuliert werden. Die bisher in § 1 Abs. 1 enthaltene Einschränkung „soweit ein schutzwürdiges Interesse daran besteht“ stammt aus dem „alten“ DSG (1978) und war seit Inkrafttreten des DSG 2000 richtlinienkonform dahingehend zu interpretieren, dass alle personenbezogene Daten als schutzwürdig zu betrachten waren, es sei denn, dass sie allgemein verfügbar waren. Die Richtlinie 95/46/EG kennt nämlich diese Einschränkung nicht. Sie bezieht sich grundsätzlich auf alle personenbezogenen Daten und legt in der Folge Tatbestände fest, bei deren Vorliegen personenbezogene Daten verwendet werden dürfen (s. dazu insbesondere die Art. 6 ff der Richtlinie). Diesem System folgend sind die Eingriffstatbestände in das Grundrecht auf Datenschutz in Abs. 2 iVm den einfachgesetzlichen Bestimmungen der §§ 6 ff DSG 2000 geregelt. Für eine „doppelte Abwägung“ nach schutzwürdigen Interessen besteht demnach kein Spielraum. Weiters scheint selbstverständlich, dass Daten nur dann personenbezogen sein können und unter den Grundrechtstatbestand fallen, wenn eine Rückführbarkeit auf den Betroffenen möglich ist, wie das im Übrigen auch bei indirekt personenbezogenen Daten der Fall ist (vgl. *Wiederin*, Privatsphäre und Überwachungsstaat [2003] 59 f); auch diese Einschränkung kann daher entfallen. Wie inzwischen auch durch die Judikatur des EuGH (Urteil vom 16. Dezember 2008 in der Rechtssache C-73/07) klargestellt wurde, fallen auch veröffentlichte personenbezogene Daten in den Anwendungsbereich der RL 95/46/EG. Auch das in Art. 7 der EU-Grundrechtecharta verankerte Recht auf Datenschutz kennt keine Ausnahme für veröffentlichte Daten. Daher entfällt die verfassungsrechtliche Ausnahme für veröffentlichte Daten; eine diesbezügliche Neuregelung findet sich im einfachgesetzlichen Teil des Gesetzesentwurfes (§ 8 Abs. 2).

In Abs. 5 wird zum einen klargestellt, dass sich die Zuständigkeit der Datenschutzkommission nach der funktionalen Zuordnung des handelnden Organs zu einer Staatsgewalt richtet. Weiters wird – der langjährigen Praxis entsprechend – ausdrücklich bestimmt, dass die Datenschutzkommission für alle Fälle des Registrierungsverfahrens (auch etwa jener der Gerichte, der Staatsanwälte oder eines parlamentarischen Organs) zuständig ist. Andernfalls müsste auf Grund der RL 95/46/EG ein eigenes Register bei den nach den §§ 83 ff GOG für den Rechtsschutz zuständigen Gerichten eingerichtet werden, wodurch dem Bund zusätzliche Kosten erwachsen würden.

Zu Art. 2 Z 13 bis 15 (§ 3 Abs. 1 und 2 und Entfall des § 3 Abs. 4):

Der Verfassungsrang des § 3 Abs. 1 bis 3 über den räumlichen Anwendungsbereich des DSG 2000 ist nach geltendem Bundesverfassungsrecht entbehrlich; diese Bestimmung soll daher in Hinkunft als einfache bundesgesetzliche Bestimmung gelten (vgl. die Aufhebung der Überschrift „Artikel 1 (Verfassungsbestimmung)“). Da der Bund nunmehr zur vollständigen Umsetzung der Richtlinie 95/46/EG zuständig ist, ist die im bisherigen § 3 Abs. 4 vorgesehene Bindung (auch) der Landesgesetzgebung, im Anwendungsbereich der Richtlinie 95/46/EG keine abweichenden Regelungen über den räumlichen Anwendungsbereich zu treffen, obsolet. Diese Bestimmung kann daher entfallen.

Die Ausweitung des in § 3 Abs. 1 und 2 geregelten Sitzstaatsprinzips auf EWR-Vertragsstaaten erfolgt in Umsetzung von Art. 4 der Richtlinie 95/46/EG, die für alle EWR-Staaten gilt.

Zu Art. 2 Z 17 und 26 (§ 4) sowie zu Z 92 (Aufhebung von § 58):

Derzeit ist in § 4 durch das Anknüpfen der übrigen Begriffsbestimmungen an jene der (automationsunterstützen) Datenanwendung (§ 4 Z 7 der geltenden Fassung) der Anwendungsbereich des DSG 2000 mitgeregelt. Nunmehr sollen die Begriffsbestimmungen vom Anwendungsbereich entflochten und in zwei Absätzen geregelt werden. Dies entspricht auch dem Zugang der Richtlinie 95/46/EG (s. deren Art. 2 und 3).

Abs. 1 soll die Begriffsbestimmungen enthalten, wobei die Bezugnahme auf die Datenanwendung (Z 7) in den meisten Begriffen entfällt. Abs. 2 legt den bisherigen Regelungsgegenstand fest und erweitert ihn

auf alle manuellen Dateien, wobei – entsprechend der neuen Kompetenzrechtslage (vgl. den vorgeschlagenen Art. 10 Abs. 1 Z 13 B-VG) – die in § 58 enthaltene Einschränkung auf manuelle Dateien, die für Zwecke der Bundesgesetzgebung bestehen, entfällt. Dadurch werden alle manuellen Dateien in die Regelungen des DSG 2000 einbezogen. Die in § 58 enthaltene Beschränkung jener manuellen Dateien, die der Meldepflicht unterliegen, bleibt bestehen, soll allerdings aus systematischen Gründen bei den Bestimmungen über die Meldepflicht geregelt werden (vgl. den vorgeschlagenen § 17 Abs. 1).

Durch den dritten Satz des Abs. 2 sollen auch manuelle Daten, die nicht in Dateiform (§ 4 Abs. 1 Z 6) bestehen, in das DSG 2000 einbezogen werden. Unter „manuellen Daten“ sind grundsätzlich schriftlich festgehaltene Daten, wie Notizen oder nicht-elektronische Akten, die nicht dem Dateibegriff entsprechen, zu verstehen. Das bloße „Wahrnehmen“, das kein gezieltes „Beobachten“ darstellt, stellt kein „Ermitteln von Daten“ dar; es werden dabei keine Daten iSd Gesetzes (auch nicht bloß manuelle) gewonnen. Allerdings sollen für „manuelle“ Daten lediglich ausgewählte Grundsätze der Verwendung (§ 6 Abs. 1 Z 1 bis 3 und Abs. 2) und die §§ 7 bis 9 über die Zulässigkeit der Verwendung sowie die Bestimmungen des 6. Abschnittes über den Rechtsschutz (§§ 30 bis 34) sinngemäß zur Anwendung gelangen. Die Betroffenenrechte auf Auskunftserteilung, Richtigstellung und Löschung bestehen hingegen nur bei jenen manuellen Daten, die in Form einer Datei verarbeitet werden. Keiner sinngemäßen Anwendung zugänglich wird etwa der vorgeschlagene § 30 Abs. 6a sein, der ausdrücklich an eine (automationsunterstützte) „Datenanwendung“ (§ 4 Abs. 1 Z 7) anknüpft.

Zu Art. 2 Z 18 (§ 4 Abs. 1 Z 4):

Durch den vorgeschlagenen § 4 Abs. 1 Z 4 soll der für die Praxis des Datenschutzes zentrale Begriff des Auftraggebers sprachlich gestrafft und leichter verständlich formuliert werden, ohne dass es zu inhaltlichen Änderungen kommt. Klargestellt soll lediglich werden, dass die Auftraggebereigenschaft nicht nur dann erhalten bleibt, wenn der Dienstleister (Z 5) zur Herstellung des ihm aufgetragenen Werkes Daten verwendet, die ihm vom Auftraggeber überlassen werden, sondern auch dann, wenn er für die Zwecke seines Auftrages Daten bei Dritten ermittelt (sog. Ermittlungsdienstleister). Dass es nunmehr „verwenden“ anstatt bisher „verarbeiten“ lautet, soll lediglich eine Zurechnung sowohl von Verarbeitungs- als auch von Übermittlungsschritten zum Auftraggeber verdeutlichen, was dem umfassenden Begriff des Art. 2 lit. d der Richtlinie 95/46/EG entspricht. Unverändert bleibt auch die Auftraggebereigenschaft jener beauftragten Berufsgruppen, die aufgrund von Rechtsvorschriften eigenverantwortlich über die Verwendung von Daten entscheiden (vgl. die beispielhafte Aufzählung der Rechtsanwälte, Wirtschaftstreuhänder und Ziviltechniker in den Erläuterungen zur Regierungsvorlage 1613 der Beilagen XX. GP, 37, zur Stammfassung).

Zu Art. 2 Z 19 (§ 4 Abs. 1 Z 5):

Der vorgeschlagene § 4 Abs. 1 Z 5 enthält die schon beim Auftraggeberbegriff vorgenommene Klarstellung hinsichtlich der sog. Ermittlungsdienstleister. Nicht als Dienstleister anzusehen werden aber folgende Fälle sein:

- ein mit der Herstellung eines Werkes Betrauter, der für die zu diesem Zweck überlassenen Daten ein Entgelt leistet (anders noch DSK 13. Dezember 2006, GZ K121.217/0021-DSK/2006); oder

- ein mit der Herstellung eines Werkes Betrauter, der Daten verschiedener Aufträge verknüpft; oder

- der Empfänger von Daten, der über die Verwendung von Daten entgegen einer Anordnung dessen entscheiden kann, welcher ihm die Daten weitergegeben hat.

Durch die Einfügung des Wortes „nur“ soll klargestellt werden, dass der mit der Herstellung eines Werkes Beauftragte nur dann als Dienstleister qualifiziert werden kann, wenn er ihm überlassene bzw. von ihm ermittelte Daten ausschließlich für den Zweck der Werkherstellung und nicht (auch) für einen anderen Zweck verwendet (vgl. in diesem Sinn schon DSK 20. Oktober 2006, GZ K121.155/0015-DSK/2006).

Zu Art. 2 Z 20 (§ 4 Abs. 1 Z 7):

Der Klammerausdruck „(früher „Datenverarbeitung“)“, der sich noch auf das „alte“ DSG (1978) bezog, soll nunmehr entfallen.

Zu Art. 2 Z 21 und Z 25 (§ 4 Abs. 1 Z 8 und Z 12):

In diesen Bestimmungen entfällt die Bezugnahme auf die „Datenanwendung“ (s. die Erläuterungen zu § 4).

Zu Art. 2 Z 22 und 23 (§ 4 Abs. 1 Z 9, Entfall der Z 10):

In Z 9 wird ebenfalls die Bezugnahme auf die „Datenanwendung“ beseitigt. Die bisherige Definition des Begriffs „Ermitteln“ in Z 10 (Umschreibung mit „Erheben“) scheint – auch im Hinblick auf die Richtlinie 95/46/EG – entbehrlich.

Zu Art. 2 Z 24 (§ 4 Abs. 1 Z 11):

Die Neuformulierung des „Überlassens“ soll klarstellen, dass unter diesen Begriff auch der Datenfluss vom Dienstleister zum Auftraggeber fallen kann (zB im Fall eines „Ermittlungsdienstleisters“, s. dazu die Erläuterungen zu § 4 Abs. 1 Z 5).

Zu Art. 2 Z 27 (§ 8 Abs. 1):

Diese Änderung ist aufgrund der Neufassung des § 1 Abs. 1 notwendig. Dementsprechend wird der Verweis auf diese Bestimmung gestrichen.

Zu Art. 2 Z 28 (§ 8 Abs. 2):

Sofern bei der Veröffentlichung von Daten eindeutig ein bestimmter Zweck erkennbar ist, dürfen diese nur zu einem mit dem ursprünglichen Zweck vereinbaren Zweck verwendet werden. So etwa dürfen die Daten von Subventionsempfängern, die zu Transparenz- und Kontrollzwecken veröffentlicht werden, nicht für unvereinbare Zwecke wie Marketing udgl. verwendet werden. Die in Materiengesetzen vorgesehenen besonderen Bestimmungen über die Zulässigkeit der Verwendung von allgemein zugänglichen Daten bleiben unberührt (vgl. zB SPG und GewO). Im Umkehrschluss zum ersten Satz des Abs. 2 dürfen Daten, deren Veröffentlichung zu keinen eindeutigen Zwecken erfolgt, ohne die genannte Einschränkung verwendet werden (dies gilt zB für öffentlich zugängliche Daten aus Telefonbuch, Melderegister, Firmenbuch, Gewerberegister und Grundbuch). Während gegen die Verwendung zulässigerweise veröffentlichter Daten ein Widerspruchtsrecht besteht, wäre ein Widerspruchsrecht gegen die Verwendung indirekt personenbezogener Daten sinnwidrig und besteht auch nach § 29 nicht.

Zu Art. 2 Z 29 (§ 8 Abs. 4):

Die bisherige Regelung über die Verwendung von strafrechtsrelevanten Daten scheint insofern ergänzungsbedürftig, als der hier genannte Fall der Anzeigeerstattung (insbesondere im Verwaltungsstrafverfahren) unter keinen der dort genannten Tatbestände eindeutig subsumierbar scheint. Sofern besondere gesetzliche Vorschriften bestehen, die etwa eine bestimmte Vorgangsweise bei der Anzeigenerstattung vorsehen (wie das Suchtmittelgesetz) oder einer Anzeigeerstattung entgegenstehen, gehen diese Bestimmungen dem § 8 Abs. 4 Z 4 vor.

Zu Art. 2 Z 30 (§ 12 Abs. 1):

Die Ausweitung auf EWR-Vertragsstaaten resultiert aus der Tatsache, dass diese, auch wenn sie nicht der EU angehören, ebenfalls die Richtlinie 95/46/EG umzusetzen haben und damit denselben datenschutzrechtlichen Standard aufweisen müssen wie EU-Mitgliedstaaten.

Zu Art. 2 Z 31 (§ 13 Abs. 2):

Zum einen wird nunmehr klargestellt, dass auch einseitige Zusagen des Antragstellers für die Datenverwendung im Ausland für eine Genehmigung der Datenschutzkommission relevant sein können. In diesem Fall wird sich der Antragsteller seinerseits wohl (vertraglich) beim Empfänger rückversichern müssen, dass dieser die Daten ordnungsgemäß verwenden wird. Um der Datenschutzkommission diesfalls weitere Auflagenbescheide zu ersparen, sollen nunmehr derartige Zusagen mit der Registrierung rechtsverbindlich werden (vgl. auch § 19 Abs. 2).

Zu Art. 2 Z 32 (Entfall von § 13 Abs. 3):

Die Parteistellung von Auftraggebern des öffentlichen Bereichs ist nunmehr in § 40 Abs. 2 allgemein vorgesehen.

Zu Art. 2 Z 33 (§ 16 Abs. 1):

Die Regelung hat klarstellenden Charakter und entspricht der derzeitigen Praxis der Registerführung: Das Datenverarbeitungsregister ist schon heute ein Register der Auftraggeber, denen die von ihnen betriebenen Datenanwendungen zugeordnet werden. Die bisher erwähnte „Kontrolle der Rechtmäßigkeit“ erfolgt vor – bzw. nach dem nunmehrigen Konzept vielfach auch erst nach – der Registrierung.

Zu Art. 2 Z 34 (§ 16 Abs. 3):

Die Regelung betreffend elektronische Eingaben findet sich nunmehr in § 17 Abs. 1a.

Zu Art. 2 Z 35 (§ 17 Abs. 1):

Mit der Einführung des Terminus „Änderungsmeldung“ soll die Verpflichtung, den Stand des Datenverarbeitungsregisters durch Meldung jeder relevanten Änderung stets aktuell zu halten, verdeutlicht werden. Der dritte Satz übernimmt den Inhalt des bisherigen § 58 zweiter Satz.

Zu Art. 2 Z 36 (§ 17 Abs. 1a):

Das Datenverarbeitungsregister soll künftig in Form einer Datenbank geführt und Meldungen primär in automationsunterstützter Form über eine Internetanwendung (also online) erstattet werden, damit die Verwaltungsabläufe vereinfacht und beschleunigt werden können. Die Identifizierung und Authentifizierung der Meldepflichtigen kann insbesondere auch durch die Bürgerkarte erfolgen. Ausnahmen von der elektronischen Meldung sind für manuelle Dateien und für Fälle eines längeren technischen Ausfalls der Internetanwendung vorgesehen. Als längerer technischer Ausfall wird etwa ein Ausfall der Internetanwendung der Datenschutzkommission von mindestens 48 Stunden zu verstehen sein. Eine nähere Ausgestaltung hat in der Verordnung nach § 16 Abs. 3 zu erfolgen.

Zu Art. 2 Z 37 (§ 19 Abs. 1 Z 3a):

Dieser Erklärung kommt bei der nach § 20 zu treffenden Entscheidung, ob die Meldung nur automationsunterstützt zu prüfen ist, maßgebliche Bedeutung zu. Wird eine Meldung fälschlich nicht als vorabkontollpflichtig bezeichnet, so stellt dies eine nach § 52 Abs. 2 Z 1 zu ahndende Verwaltungsübertretung dar.

Zu Art. 2 Z 38 (§ 19 Abs. 2):

In dieser Bestimmung wird die Möglichkeit geschaffen, dass sich der Auftraggeber bereits im Registrierungsverfahren gegenüber der Datenschutzkommission einseitig zur Einhaltung bestimmter Auflagen, Bedingungen oder Befristungen bereit erklärt. Dies kann bestimmte Einschränkungen für ihn bedeuten (zB Verarbeitung von Daten nur mit Zustimmung der Betroffenen). Werden die einseitigen Zusagen oder Erklärungen von der Datenschutzkommission durch Registrierung akzeptiert, sind keine weiteren Auflagenbescheide notwendig, was einerseits den Verwaltungsaufwand bei der Datenschutzkommission vermindert, andererseits etwa bei vorabkontrollpflichtigen Datenanwendungen die Verfahrensdauer verkürzt. Die Zusagen müssen freilich den Anforderungen an die Bestimmtheit von bescheidmäßig ausgesprochenen Auflagen, Bedingungen oder Befristungen entsprechen, ansonsten ist eine Registrierung nicht möglich.

Zu Art. 2 Z 39 (§§ 20 bis 22 samt Überschriften):

Diese Bestimmungen bilden das „Herzstück“ der Neuregelung des Registrierungsverfahrens. Als Grundsatz gilt, dass nicht vorabkontrollpflichtige Meldungen nur mehr einen automationsunterstützten Prüfalgorithmus durchlaufen sollen, dessen Ablauf in der Verordnung nach § 16 Abs. 3 näher zu bestimmen ist. Dabei wird es sich notwendigerweise um eine vergröberte Prüfung auf Vollständigkeit und Widerspruchsfreiheit („Plausibilität“) handeln. Im Hinblick auf die Bedeutung der Erklärung nach § 19 Abs. 1 Z 3a muss der Prüfung von deren Richtigkeit im Rahmen der Plausibilitätskontrolle besondere Bedeutung zukommen. Eine bloß automationsunterstützte Prüfung wird im Register angemerkt (§ 21 Abs. 5). Sie führt zu einer sofortigen Registrierung (§ 20 Abs. 1 und § 21 Abs. 1 Z 1), von der der Auftraggeber auch sogleich im Rahmen der Internetanwendung (§ 17 Abs. 1a) nach § 21 Abs. 3 verständigt werden kann.

Nur wenn es beim automationsunterstützten Prüfverfahren zu einer Fehlermeldung (dh der Algorithmus erkennt eine Unvollständigkeit oder Unplausibilität) kommt, kann der Auftraggeber die Meldung schriftlich unter Anschluss der ausgedruckten Fehlermeldung einbringen; diesfalls findet eine vollständige Prüfung nicht vorabkontrollpflichtiger Meldungen nach § 19 Abs. 4 statt (§ 20 Abs. 2). Als vorabkontrollpflichtig bezeichnete Meldungen werden hingegen vor ihrer Registrierung stets nach § 19 Abs. 3 geprüft (§ 20 Abs. 3 iVm § 18 Abs. 2).

Die Ablehnung der Registrierung wird künftig zunächst nur mehr relativ formlos dem Auftraggeber mitgeteilt. Dieser hat freilich die Möglichkeit, eine bescheidmäßige Erledigung zu beantragen. Verspätete Verbesserungen sind künftig nicht mehr zu berücksichtigen, dh es hat dennoch eine Ablehnungsmitteilung der Datenschutzkommission zu ergehen. Dadurch sollen Verfahrensverzögerungen vermieden werden. Freilich steht es dem Auftraggeber jederzeit frei, unter Berücksichtigung des Verbesserungsauftrages eine neue Meldung einzubringen.

Für das Registrierungsverfahren gilt in allen Fällen die sechsmonatige Entscheidungsfrist des § 73 Abs. 1 AVG.

In § 22 Abs. 1 bis 3 wurden nur geringfügige Änderungen vorgenommen. Abs. 1 ordnet zunächst an, dass Änderungen für die Dauer von sieben Jahren im Register ersichtlich zu machen sind. Daher sind

insbesondere gestrichene Auftraggeber bzw. Datenanwendungen erst nach Ablauf dieser Frist zu löschen. Ein Interesse an der Publizität von Datenanwendungen besteht auch noch für eine gewisse Zeit nach deren Änderung bzw. Aufgabe.

§ 22 Abs. 2 iVm Abs. 3 ermöglicht nunmehr auch in Fällen, in denen der Datenschutzkommission bekannt wird, dass eine einzelne Datenanwendung zur Gänze und dauerhaft (dh ohne erkennbare Wiederaufnahmeabsicht) aufgegeben wurde, sowie nach Ablauf einer Befristung des Betriebes nach § 19 Abs. 2 oder § 21 Abs. 2 eine vereinfachte Streichung durch Mandatsbescheid.

Neu ist die gesetzliche Regelung der Rechtsnachfolge in Abs. 4. Sie baut auf der Idee des geltenden § 13 DVRV 2000 auf, erweitert diese jedoch dadurch, dass ein (Einzel- oder Gesamt-)Rechtsnachfolger auch bloß einzelne Datenanwendungen übernehmen kann. Wenn diese ansonsten (einschließlich der Rechtsgrundlage) unverändert bleiben, erscheint dafür die bisher erforderliche komplette Neumeldung überzogen, sodass eine bloße Erklärung ausreicht, in der aber die Nachfolge in jene Rechte, aus denen auch die Berechtigung für den Betrieb der Datenanwendung abgeleitet wird, glaubhaft zu machen ist. Diese Erklärung ist ein Spezialfall einer Änderungsmeldung, ihr wird also im Regelfall durch entsprechende Registrierung entsprochen, erforderlichenfalls ist sie nach § 20 Abs. 5 abzulehnen.

Zu Art. 2 Z 40 (§ 22a samt Überschrift):

Durch diese Bestimmung soll das bisher (im geltenden § 22 Abs. 4) nur wenig geregelte Verfahren zur Überprüfung der Meldepflicht insbesondere im Hinblick auf die Befugnisse der Datenschutzkommission neu geregelt werden. Dies stellt auch einen Ausgleich für den Entfall der Detailprüfung bei nicht vorabkontrollpflichtigen Datenanwendungen dar. Abs. 1 ermöglicht in diesem Sinn eine jederzeitige Überprüfung der Erfüllung der Meldepflicht durch die Datenschutzkommission (vgl. auch die vorgeschlagenen § 30 Abs. 2a, § 31a Abs. 1 sowie § 32 Abs. 7, die „Impulse“ für derartige Überprüfungen setzen sollen). Wenn diese „interne“ Prüfung den Verdacht einer Nichterfüllung der Meldepflicht erhärtet, so ist ein Verfahren zur Berichtigung des Datenverarbeitungsregisters durchzuführen, welches durch begründete Verfahrensanordnung (also nicht durch Bescheid) eingeleitet wird. Freilich können nicht nur Mängel innerhalb registrierter Meldungen (§ 19 Abs. 4), die in der Regel (außer die Mangelhaftigkeit tritt erst nachträglich durch Änderungen der Rechtslage ein; s. dazu die Übergangsbestimmung für Videoüberwachung in § 61 Abs. 6) eigentlich schon im Zuge des Registrierungsverfahrens hätten hervorkommen müssen (in verfahrensrechtlicher Terminologie „nova reperta“), ein solches Berichtigungsverfahren erforderlich machen, sondern auch Fälle, in denen eine Meldung zur Gänze oder teilweise unterlassen wurde, eine Datenanwendung also gar nicht oder in einer nicht (mehr) dem Echtbetrieb entsprechenden Form registriert ist. Je nachdem, welcher der beiden Fälle vorliegt, ist auch das Berichtigungsverfahren zu führen bzw. abzuschließen. Der erste Fall (Mangel nach § 19 Abs. 3), den Abs. 3 regelt, führt, sofern keine auftragsgemäße Verbesserung erfolgt, – analog der Ablehnung nach § 20 Abs. 5 – zur Streichung der Datenanwendung, im zweiten Fall (Abs. 4) wird die Datenanwendung untersagt. Eine solche Untersagung hat freilich – wie grundsätzlich jeder Bescheid (vgl. *Walter/Mayer*, Verwaltungsverfahrensrecht, [2003] 8. Aufl., Rz. 481 ff) – objektive Grenzen, nämlich den Sachverhalt und die Rechtslage, auf die sie sich bezieht. Wird also zB eine Datenanwendung, die zunächst mangels Meldung untersagt wurde, auf Grund einer nachträglich erstatteten Meldung registriert, so wird die Untersagung gegenstandslos.

Die Abs. 5 regelt den Sonderfall, dass sich als Ergebnis des Berichtigungsverfahrens bloß Mängel bei den Datensicherheitsmaßnahmen ergeben.

Bei Gefahr im Verzug ist schon während des noch anhängigen Berichtigungsverfahrens eine Bescheiderlassung nach § 30 Abs. 6a möglich.

Zu Art. 2 Z 41 (§ 24 Abs. 2a):

Hier wird eine besondere Informationsverpflichtung jener Auftraggeber geschaffen, die Kenntnis von einer systematischen und schwerwiegenden unrechtmäßigen Verwendung (Datenmissbrauch) ihrer Datenbestände erlangen. Dies soll der Vermeidung von Vermögensschäden der Betroffenen dienen. Die Information hat in geeigneter Form zu erfolgen. Dies bedeutet zunächst eine persönliche Information der Betroffenen. In bestimmten Fällen käme etwa auch eine adäquate mediale Information in Frage. Soweit einerseits nur geringfügige Schäden drohen oder andererseits die Information einen unverhältnismäßigen Aufwand für den Auftraggeber verursachen würde, kann von der Information gänzlich abgesehen werden. Angesichts der Möglichkeit der Information durch Medien wird dies jedoch eher eine in nur besonderen Fällen in Anspruch zu nehmende Ausnahme bleiben; keinesfalls muss eine Information bei Drohung eines nur geringfügigen Schadens erfolgen.

Zu Art. 2 Z 42, 43 und 44 (§ 26 Abs. 1 bis 7):

Hier erfolgt lediglich eine der Rechtsprechung der Datenschutzkommission (zB Bescheid vom 2. Februar 2007, GZ K121.220/0001-DSK/2007) entsprechende Klarstellung, dass auch in dem Fall, dass ein Auftraggeber zu einer Person keine Daten verarbeitet, eine sog. Negativauskunft zu erteilen ist. Dementsprechend wird in § 26 nunmehr im Allgemeinen von „Auskunftswerbern" gesprochen, der Begriff des Betroffenen wird nur noch im strengen Sinn des § 4 Z 3 gebraucht, dh wenn zur Person des Auskunftswerbers tatsächlich Daten vorhanden sein müssen (zB Anspruch auf Bekanntgabe von Dienstleistern in Abs. 1). Entsprechend der RL 95/46/EG hat die Auskunft über die Herkunft der Daten insoweit zu erfolgen, als diese verfügbar sind. Die in Abs. 7 vorgesehene Speicherfrist von vier Monaten verkürzt sich, wenn der Auskunftswerber gleichzeitig oder etwa gleich nach Erhalt der Auskunft ein Löschungsbegehren stellt oder Widerspruch gegen eine Datenverarbeitung erhebt. Diesfalls ist – sofern das Löschungsbegehren oder der Widerspruch berechtigt ist – unverzüglich eine Löschung der Daten vorzunehmen.

Zu Art. 2 Z 45 (§ 26 Abs. 8):

In dieser Bestimmung entfällt die sinnwidrige Einschränkung auf *öffentliche* Einsehbarkeit. Nunmehr soll es darauf ankommen, dass ein Auskunftswerber ein Recht auf Einsicht in die zu seiner Person verarbeiteten Daten hat („zumindest" bedeutet dabei bloß, dass manchmal, zB im Grundbuch, auch darüber hinaus gehende Einsichtsrechte gewährt werden). Damit wird insbesondere auch die immer häufiger werdende Führung elektronischer Verfahrensakten durch Behörden jedenfalls hinsichtlich der Verfahrensparteien umfasst (zB § 17 AVG, §§ 90 f BAO). Wenn durch das Einsichtsrecht nicht alle Bestandteile einer Auskunft nach § 26 Abs. 1 erlangt werden können, besteht darüber hinaus – soweit Informationen vorhanden sind – das Auskunftsrecht nach dem DSG 2000. Bei (teil-)öffentlichen Registern ist freilich die Bekanntgabe von Empfängerkreisen – mehr wird im Hinblick auf fehlendes Rechtsschutzbedürfnis im Regelfall nicht erforderlich sein (vgl. das Erkenntnis des VwGH vom 19. Dezember 2006, Zl. 2005/06/0111) – schon durch den dem Auskunftswerber bekannten Umstand der (teil-)öffentlichen Einsehbarkeit verwirklicht. Weiterhin nicht möglich sein soll freilich die Umgehung von Beschränkungen von Einsichtsrechten durch das Auskunftsrecht: Die für die Beschränkung maßgeblichen Gründe werden idR auch nach § 26 Abs. 2 eine Ablehnung der Auskunft ermöglichen.

Im Hinblick auf die Richtlinie 95/46/EG ist diese Ausnahme unproblematisch, weil dort die näheren Modalitäten der Auskunftserteilung nicht geregelt sind. Eine geringe Kostenpflicht ist nicht ausgeschlossen. Die Anrufbarkeit der Datenschutzkommission nach § 30 ist trotz Ausschluss des förmlichen Beschwerderechts gegeben, sodass auch die Umsetzung von Art. 28 der Richtlinie gewahrt bleibt.

Zu Art. 2 Z 46 (§ 26 Abs. 10):

Die ersten beiden Sätze wurden nur sprachlich geringfügig angepasst und bleiben inhaltlich unverändert. In den hinzugefügten neuen Sätzen erfolgt der Schluss einer Lücke im System des Auskunftsrechts: Wenn der Auskunftswerber ein Auskunftsbegehren irrtümlich an einen Dienstleister richtet, so hat dieser das Auskunftsbegehren unverzüglich an den Auftraggeber weiterzuleiten. Der Auftraggeber hat innerhalb von acht Wochen ab Einlangen des Auskunftsbegehrens beim Dienstleister dem Auskunftswerber Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, von einer Auskunftserteilung abzusehen. Wird jedoch in weiterer Folge das Ersuchen direkt an den Auftraggeber gestellt, hat dieser nach Abs. 5 vorzugehen. Der Dienstleister hat unverzüglich den Auskunftswerber darüber zu informieren, dass in seinem Auftrag keine Daten verwendet werden. Im Vorfeld dieser Mitteilung kann der Dienstleister eine Identitätsprüfung durchführen, wobei deren Ergebnis von ihm an den Auftraggeber weiterzuleiten ist. Für Dienstleister, die zugleich Betreiber von Informationsverbundsystemen sind, gilt weiterhin § 50 Abs. 1.

Zu Art. 2 Z 47 (§ 28 Abs. 2):

Durch die Verwendung des Begriffs „Datenanwendung" soll gewährleistet werden, dass auch etwa bei Internetanwendungen, bei denen über die Dateieigenschaft Unklarheit besteht, das Recht auf Widerspruch geltend gemacht werden kann.

Zu Art. 2 Z 48 (§ 28 Abs. 3):

Hier wird lediglich klargestellt, dass die Bestimmungen über die Durchsetzung des Richtigstellungs- und Löschungsrechts auch für das als Sonderfall des Löschungsrechts anzusehende Widerspruchsrecht gelten.

Zu Art. 2 Z 49 und 51 (§ 30 Abs. 2a und Abs. 6):

Auch der neue § 30 Abs. 2a soll den Entfall der inhaltlichen Prüfung von nicht vorabkontrollpflichtigen Registermeldungen im Sinn einer verwaltungseffizienten und am Rechtsschutzbedarf orientierten Lösung ausgleichen (s. schon oben zu § 22a): Anlässlich jeder zulässigen Eingabe nach § 30 Abs. 1 bzw. jedes begründeten Verdachts hat die Datenschutzkommission nunmehr den Registerstand zu überprüfen, entspricht dieser nicht dem Gesetz, sind Maßnahmen nach den §§ 22 und 22a zu ergreifen. Somit führt das Verfahren nach § 30 im Fall eines Verdachts der Nichterfüllung der Meldepflicht zu den §§ 22 und 22a. Der Ausspruch einer Empfehlung scheint in diesen Fällen wenig zweckmäßig und entfällt daher künftig. Eine Empfehlung ist weiters nicht mehr erforderlich, wenn die Datenanwendung schon wegen Gefahr im Verzug untersagt worden ist.

Zu Art. 2 Z 50 (§ 30 Abs. 5):

Hier wird eine Klarstellung getroffen: Auch die Verwertung der Ergebnisse einer Einschau nach Abs. 4 zur verbindlichen Klärung der darauf bezogenen (Datenschutz-)Rechtslage vor Gericht nach § 32 (gleich ob durch den Einschreiter oder die Datenschutzkommission) zählt zur Kontrolltätigkeit. Daher besteht gegenüber dem angerufenen Gericht hinsichtlich solcher Ergebnisse keine Verschwiegenheitspflicht. Das Gericht kann einem besonderen Geheimhaltungsinteresse des Beklagten durch Ausschluss der Öffentlichkeit auf Grundlage der ZPO Rechnung tragen. Weiters wird eine Ausdehnung jener strafbaren Handlungen, bei Verdacht auf deren Vorliegen die Datenschutzkommission Anzeige zu erstatten hat, auf bestimmte computerbezogene Delikte (widerrechtlicher Zugriff auf ein Computersystem, Verletzung des Telekommunikationsgeheimnisses, missbräuchliches Abfangen von Daten, Datenbeschädigung, Störung der Funktionsfähigkeit eines Computersystems, Missbrauch von Computerprogrammen oder Zugangsdaten, betrügerischer Datenverarbeitungsmissbrauch) vorgenommen.

Zusätzlich erfolgt noch eine Verweisanpassung an die seit 1. Jänner 2008 geltende Fassung der StPO.

Zu Art. 2 Z 52 (§ 30 Abs. 6a):

Für die Fälle der rechtswidrigen Unterlassung einer Meldung sieht § 22a Abs. 4 bereits die Untersagung einer Datenanwendung vor. Es gibt aber auch abseits von Verletzungen der Meldepflicht Fälle, in denen Datenanwendungen untersagt werden müssen, um eine Gefährdung schutzwürdiger Geheimhaltungsinteressen hintanzuhalten. Zu denken ist hier zunächst an gar nicht meldepflichtige Datenanwendungen aber auch an Fälle, in denen die Meldung zwar der Form nach korrekt ist, die Datenanwendung aber auf eine Art und Weise betrieben wird, die den Grundsätzen des § 6 Abs. 1 krass widerspricht (zB systematische Verarbeitung nicht aktueller oder im Hinblick auf den Verwendungszweck unrichtiger Daten). Da in diesen Fällen von Gefahr im Verzug auszugehen ist, erfolgt eine allfällige Untersagung mit Mandatsbescheid. Ein solcher kann, wenn die wesentliche Gefährdung vorliegt, auch während der Anhängigkeit eines Berichtigungsverfahrens nach § 22a Abs. 2 erlassen werden. Wird die Untersagung wegen Gefährdung rechtskräftig, scheint aber die Weiterführung des Berichtigungsverfahrens wenig sinnvoll.

Zu Art. 2 Z 53 (§ 31 samt Überschrift):

Die Vollzugspraxis hat zahlreiche Probleme bei der Auslegung der bisherigen spärlichen Regelungen des § 31 Abs. 1 und 2 gezeigt. Zunächst war lange nicht klar, welchen Charakter die Bescheide der Datenschutzkommission haben. Durch Rechtsprechung des VwGH ist dies nunmehr weitgehend klargestellt (vgl. vor allem die beiden Erkenntnisse vom 28. März 2006, Zl. 2004/06/0125, und vom 27. Juni 2006, Zl. 2005/06/0366). An dieser orientiert sich auch der nunmehrige § 31 Abs. 7. Demnach ist eine Rechtsverletzung jedenfalls festzustellen. Nur bei Auftraggebern des privaten Bereichs ist darüber hinaus ein – vollstreckbarer – Leistungsauftrag zu erteilen, der so zu formulieren ist, dass die festgestellte Rechtsverletzung beseitigt wird. Der Leistungsauftrag ist je nach dem Beschwerdebegehren bzw. den die Feststellung der Rechtswidrigkeit tragenden Gründen im Einzelfall zu formulieren. Es wird sich im Regelfall nicht auf ein konkret verarbeitetes Datum beziehen, weil die Datenschutzkommission die Rechtmäßigkeit der Auskunftserteilung nur ex post prüft und sie nicht an Stelle des Auftraggebers Auskunft zu erteilen hat. Somit wird der Leistungsauftrag in der Regel allgemeiner formuliert sein (zB „Der Beschwerdegegner hat innerhalb von zwei Wochen (neuerlich) Auskunft über die zur Person des Beschwerdeführers verarbeiteten Daten aus der Datenbank xy zu erteilen oder zu begründen, warum Auskunft nicht erteilt wird.“).

§ 31 vermeidet nunmehr insbesondere in den Abs. 1 und 2 die Verwendung des materiellrechtlichen Begriffs „Auftraggeber“ (ob jemandem diese Rolle zukommt, wird oft erst im Verfahren entschieden) und orientiert sich an der Formulierung von § 1 Abs. 5). Der lückenlosen Umsetzung dieser verfassungsrechtlichen Rechtsschutzbestimmung dient auch die „negative“ Abgrenzung der

Beschwerdelegitimation nach Abs. 2, bezogen auf § 32 Abs. 1. Der Organbegriff ist weiterhin funktional zu verstehen, was durch die Formulierung „im Dienste“ nunmehr auch im Text verdeutlicht werden soll.

Weiters wird nun auch eine Beschwerdemöglichkeit im Hinblick auf die Rechte auf Bekanntgabe des Ablaufs einer automatisierten Einzelentscheidung (§ 49 Abs. 3) bzw. des verantwortlichen Auftraggebers in einem Informationsverbundsystem (§ 50 Abs. 1 dritter Satz) vorgesehen. Diesbezüglich bestand bisher (jedenfalls dem Wortlaut nach) eine Rechtsschutzlücke. Weiters kann nunmehr auch gegen Dienstleister zur Durchsetzung des § 26 Abs. 10 vorgegangen werden.

Eine gewisse Formalisierung des Beschwerdeverfahrens erfolgt nach dem Vorbild des § 67c Abs. 2 AVG durch die neuen Abs. 3 und 4 des § 31. Dadurch soll es der Datenschutzkommission ermöglicht werden, Beschwerden, die nicht einmal die genannten Minimalanforderungen aufweisen, nicht inhaltlich behandeln zu müssen. Wenn diese fehlen, kann nach § 13 Abs. 3 AVG vorgegangen werden. Eine Behandlung von Anbringen, die Abs. 3 und 4 nicht genügen, kann allenfalls im Verfahren nach § 30 erfolgen. Der VwGH hat in seinem Erkenntnis vom 6. Juni 2007, Zl. 2001/12/0004, ausgesprochen, dass ein Anspruch auf Löschung stets ein entsprechendes Begehren nach § 27 Abs. 1 Z 2 voraussetzt, was wohl sinngemäß auf das Auskunftsrecht zu übertragen ist. Daher müssen Auskunfts- bzw. Löschungsverlangen ohnehin stets vorliegen, um die Rechte erfolgreich geltend zu machen.

§ 31 Abs. 5 enthält lediglich eine Klarstellung, die bisher geübter Praxis entspricht.

§ 31 Abs. 6 sieht aus Gründen der Verfahrensökonomie vor, dass ein Kontrollverfahren nach § 30 Abs. 1 nicht parallel zu einem Beschwerdeverfahren über denselben Gegenstand geführt werden soll. Freilich können über den Beschwerdegegenstand hinausgehende Verdachtsmomente (insbesondere im Hinblick auf Verpflichtungen, die nicht mit subjektiven Betroffenenrechten korrespondieren) von der Datenschutzkommission nach § 30 weiterverfolgt werden.

§ 31 Abs. 8 sieht eine besondere verfahrensrechtliche Regelung für den in der Praxis regelmäßig auftretenden Fall vor, dass ein Beschwerdeführer während des Auskunfts-, Richtigstellungs- oder Löschungsbeschwerdeverfahrens klaglos gestellt wird, dh die mit der Beschwerde verfolgte Auskunft erteilt oder die Löschung/Richtigstellung durchgeführt wird. Wurde die Beschwerde in einem solchen Fall nicht ausdrücklich zurückgezogen (§ 13 Abs. 7 AVG), so musste dennoch ein abweisender Bescheid erlassen werden, auch wenn auf Grund des Unterbleibens einer Stellungnahme des Beschwerdeführers im Parteiengehör zu vermuten war, dass dieser kein Interesse an der Weiterverfolgung seines Anspruches hat. Nunmehr soll es der Datenschutzkommission ermöglicht werden, in derartigen Fällen das Verfahren formlos (dh ohne Bescheiderlassung, wohl aber unter Verständigung des Beschwerdeführers) einzustellen, wenn der Beschwerdeführer nicht ausdrücklich auf einer Fortsetzung beharrt. Diese § 33 Abs. 1 VwGG nachgebildete Ergänzung des verfahrensrechtlichen Instrumentariums des AVG scheint im Hinblick auf das kontradiktorisch ausgestaltete Beschwerdeverfahren vor der Datenschutzkommission zweckmäßig. Die formlose Einstellung ist auch nicht präjudiziell, eine neue Beschwerdeerhebung innerhalb der Frist des § 34 Abs. 1 daher jederzeit möglich.

Besonders Bedacht genommen wird in der Bestimmung auch auf die immer wieder vorkommende wesentliche Änderung des Verfahrensgegenstandes (§ 13 Abs. 8 AVG) in einer derartigen Konstellation. Wenn etwa zunächst Beschwerde erhoben wurde, weil auf ein Auskunftsbegehren überhaupt nicht reagiert worden ist und während des Verfahrens eine Auskunft erteilt wird, die der Beschwerdeführer aber als unvollständig oder falsch ansieht, so ändert er bei einem entsprechenden Vorbringen den Verfahrensgegenstand wesentlich ab (s. zB den Bescheid der Datenschutzkommission vom 20. Juli 2007, GZ K121.289/0006-DSK/2007). Solche Fälle werden nunmehr entsprechend der bei *Thienel*, Verwaltungsverfahren, 3. Aufl., 112, wiedergegebenen herrschenden Ansicht, der die Datenschutzkommission in der Praxis schon bisher folgte, als (konkludente) Zurückziehung der ursprünglichen Beschwerde und gleichzeitige Einbringung einer weiteren Beschwerde mit dem geänderten Gegenstand gewertet. Damit beginnt auch die Entscheidungsfrist neu zu laufen. Zu verspäteten Äußerungen gilt das zum vorgeschlagenen § 20 Abs. 5 Gesagte sinngemäß. Die nach Abs. 3 erforderlichen Inhalte müssen sich in einem derartigen Fall schlüssig aus einer Zusammenschau von alter und neuer Beschwerde ergeben, ansonsten ist die neue Beschwerde mangelhaft.

Zu Art. 2 Z 54 (§ 31a samt Überschrift):

Zur Wahrung der Übersichtlichkeit des § 31 werden mit dem Beschwerdeverfahren zusammenhängende Instrumente nunmehr in § 31a geregelt. Zunächst wird in dessen Abs. 1 eine auf die neuen §§ 20 bis 22a abgestimmte Anordnung zur Überprüfung der Registermeldung getroffen. Der bisherige § 31 Abs. 3 (in der Praxis bedeutungslos) scheint im Hinblick darauf nicht mehr erforderlich, weil der neue § 30 Abs. 6a, auf den in Abs. 2 verwiesen wird, der Datenschutzkommission zumindest die gleichen Möglichkeiten gibt. Hinsichtlich des Bestreitungsvermerks wird nunmehr in § 31a Abs. 3 im Hinblick auf eine

Beschleunigung dieser Möglichkeit vorgesehen, dass darüber mit Mandatsbescheid entschieden werden kann.

Der bisherige § 31 Abs. 4 findet sich in § 31a Abs. 4 unverändert wieder. Es wird lediglich zusätzlich angeordnet, dass die ersten beiden Sätze im Verfahren nach § 30 sinngemäß anzuwenden sind.

Zu Art. 2 Z 55 bis 57 (§ 32 Abs. 1, 4 und 6):

Hier gilt das schon zu § 31 Ausgeführte analog: Es werden materiellrechtliche Begriffe durch prozessrechtliche ersetzt bzw. die Terminologie an § 1 Abs. 5 angeglichen. Die im Begutachtungsverfahren angeregte Klarstellung, dass bei datenschutzrechtlichen Streitigkeiten, die aus Arbeitsverhältnissen resultieren, die Arbeitsgerichte zuständig sind, scheint nicht erforderlich, da dies der herrschenden Auffassung [*Dohr/Pollirer/Weiss/Knyrim*, DSG² (9. Erg.-Lfg. 2009), Anm. 7 zu § 32 DSG 2000] entspricht.

Zu Art. 2 Z 58 (§ 32 Abs. 7):

Es liegt im freien Ermessen des Gerichtes, mit der Datenschutzkommission Kontakt aufzunehmen, um die Erfüllung der Meldepflicht im Hinblick auf eine klagsgegenständliche Datenanwendung zu überprüfen. Dies soll ebenfalls den Entfall der Prüfung nicht vorabkontrollpflichtiger Datenanwendungen ausgleichen (s. schon oben zu den §§ 20 bis 22, § 22a, § 30 Abs. 2a und § 31a). Das Ergebnis soll im Sinn der Waffengleichheit vom Gericht beiden Verfahrensparteien bekannt gegeben werden.

Zu Art. 2 Z 59 (§ 34 Abs. 1):

Die bisherige Anordnung, dass verspätete Beschwerden abzuweisen sind, entsprach nicht der üblichen verfahrensrechtlichen Terminologie. Nunmehr soll klargestellt werden, dass es sich um eine verfahrensrechtliche Frist handelt. Da keine Sachentscheidung getroffen wird, handelt es sich richtigerweise um eine Zurückweisung.

Zu Art. 2 Z 60 (§ 34 Abs. 3):

Die Bestimmung wird sprachlich vereinfacht und dadurch gleichzeitig etwas weiter gefasst, was der Intention des Art. 28 Abs. 6 der Richtlinie 95/46/EG entspricht. Zur Erweiterung auf den Europäischen Wirtschaftsraum vgl. die Erläuterungen zu § 3 Abs. 1 und 2 sowie § 12 Abs. 1. Internationale Zuständigkeitsregelungen nach § 3 werden dadurch nicht verändert.

Zu Art. 2 Z 61 (§ 34 Abs. 4):

Vgl. die Erläuterungen zu § 3 Abs. 1 und 2 sowie § 12 Abs. 1.

Zu Art. 2 Z 62 (§ 36 Abs. 3):

Fortan sollen im Hinblick auf die abnehmende Zahl von Beamtendienstverhältnissen (vgl. dazu die vom Bundeskanzleramt herausgegebene Broschüre „Der öffentliche Dienst in Österreich“, S 6 f) bzw. die im Regierungsprogramm in Aussicht genommene Schaffung einer einheitlichen Rechtsform für den Bundesdienst alle Arten von Bundesbediensteten der Datenschutzkommission angehören können.

Zu Art. 2 Z 63 (§ 36 Abs. 3a):

Hier wird klargestellt, dass die Ausübung der Funktion als Mitglied der Datenschutzkommission *neben* allfälligen sonstigen beruflichen Verpflichtungen zu erfolgen hat. Ein Anspruch auf Gewährung von Freizeit kann somit aus der Mitgliedschaft nicht abgeleitet werden. Bei Bundesbeamten liegt im Hinblick auf § 36 Abs. 9 eine bezahlte Nebentätigkeit vor (vgl. § 25 Abs. 1 und 2 GehG).

Zu Art. 2 Z 64 (§ 36 Abs. 6):

Ähnlich wie für Richter und Beamte soll auch für die Mitgliedschaft in der Datenschutzkommission eine Altersgrenze eingeführt werden. Es scheint zweckmäßig, dazu beim richterlichen Mitglied und dem Mitglied aus dem Kreis der rechtskundigen Bundesbediensteten am Ausscheiden aus den hauptberuflichen Funktionen anzuknüpfen, weil diese Voraussetzung für die Ernennung zum Mitglied war. Bei den übrigen Mitgliedern wird – da ihre Mitgliedschaft nicht auf einem Dienstverhältnis beruht – eine Altersgrenze eingeführt.

Zu Art. 2 Z 65 (§ 36 Abs. 9):

Mit der Neufassung dieser Bestimmung, die bisher nach hA nur einen Reisekostenersatzanspruch für die Anreise zu Sitzungen der Datenschutzkommission vorsah, soll dem Umstand Rechnung getragen werden, dass der Datenschutzkommission auch Aufgaben im internationalen Bereich zukommen (s. insbesondere Art. 29 der Richtlinie 95/46/EG) und daher den Mitgliedern auch Reisetätigkeit abverlangt wird. Nunmehr wird dafür explizit ein öffentlich-rechtlicher Ersatzanspruch vorgesehen.

Zu Art. 2 Z 66 (Entfall des Verfassungsrangs von § 38 Abs. 1):

Der Verfassungsrang dieser Bestimmung ist nach geltendem Bundesverfassungsrecht entbehrlich; sie soll daher in Hinkunft als einfache bundesgesetzliche Bestimmung gelten.

Zu Art. 2 Z 67 (§ 38 Abs. 1):

Mandatsbescheide können künftig auch nach § 30 Abs. 6a erlassen werden, also auch außerhalb des Registrierungsverfahrens. Die Verweise auf konkrete Bestimmungen scheinen nicht erforderlich. Darüber hinaus scheint es zweckmäßig, eine Kundmachungsform für die als Verordnung zu wertende Geschäftsordnung der Datenschutzkommission festzulegen.

Zu Art. 2 Z 68 (§ 38 Abs. 2)

Diese Bestimmung ist im Hinblick auf Art. 20 Abs. 2 letzter Satz B-VG idF BGBl. I Nr. 2/2008 erforderlich.

Zu Art. 2 Z 69 (§ 39 Abs. 5):

Durch diese Regelung wird lediglich die bisherige Praxis gesetzlich festgeschrieben.

Zu Art. 2 Z 70 (§ 40 Abs. 1 und 2):

Abs. 1 enthält lediglich eine Anpassung der Verweise.

In Abs. 2 wird nunmehr auch Auftraggebern des öffentlichen Bereichs durchwegs Parteistellung gewährt. Auch der bisherige Wortlaut wurde vom VwGH schon in diese Richtung ausgelegt (Beschluss vom 28. November 2006, Zl. 2006/06/0068). Eine Beschwerdemöglichkeit an den Verwaltungsgerichtshof im Verfahren nach § 31 bleibt aber hinsichtlich dieser Auftraggeber weiterhin einer speziellen gesetzlichen Anordnung (zB § 91 Abs. 1 Z 2 SPG) vorbehalten.

Zu Art. 2 Z 71 (§ 41 Abs. 2 Z 4a):

Hier wird klargestellt, dass der Datenschutzrat auch von der Datenschutzkommission Auskünfte einholen darf. Diese Auskünfte der Datenschutzkommission sind auf den in dieser Bestimmung genannten Zweck beschränkt und umfassen daher in der Regel keine personenbezogenen Daten von BeschwerdeführerInnen.

Zu Art. 2 Z 72 (§ 42 Abs. 1 Z 1):

Hier erfolgt eine Neuregelung, die nunmehr den Fall der Mandatsgleichheit im Hauptausschuss für alle Parteien berücksichtigt. Entscheidend ist das amtliche Endergebnis der letzten Nationalratswahl. Außerdem wird klargestellt, dass Änderungen der Parteienzugehörigkeit der Mitglieder des Hauptausschusses während dessen Funktionsperiode auf die Entsendeberechtigung in den Datenschutzrat keinen Einfluss haben.

Zu Art. 2 Z 73 (§ 42 Abs. 5):

Diese Regelung stellt sicher, dass einem geänderten politischen Kräfteverhältnis nach einer Nationalratswahl auch bei der Zusammensetzung des Datenschutzrates Rechnung getragen wird: Die Zugehörigkeit der von den politischen Parteien entsendeten Mitglieder endet mit der Neukonstituierung des Hauptausschusses, sofern diese nicht durch eine neuerliche Entsendung erneuert wird.

Zu Art. 2 Z 74 (§ 46 Abs. 1):

Die bisherige uneinheitliche Terminologie wird beseitigt und damit klargestellt, dass stets vom Auftraggeber, der die Untersuchung durchführt, die Rede ist.

Zu Art. 2 Z 75 (§ 46 Abs. 2):

Die entfallende Wortfolge ist überflüssig, weil öffentlich zugängliche Daten ohnehin in § 46 Abs. 1 Z 1 enthalten sind.

Zu Art. 2 Z 76 (§ 46 Abs. 3):

Es erfolgt eine Klarstellung der Antragslegitimation. Die Terminologie wird wie schon in Abs. 1 vereinheitlicht und aus der Perspektive des antragstellenden Auftraggebers verwendet (dies entsprach schon der bisherigen Praxis der Datenschutzkommission). Dieser *er*mittelt Daten für Zwecke der Untersuchung.

Zu Art. 2 Z 77 (§ 46 Abs. 3a):

Diese Bestimmung soll sicherstellen, dass der zivilrechtlich über die Datenbestände (zB ein Archiv oder eine Datenbank) Verfügungsbefugte mit der Datenverwendung einverstanden ist bzw. ein zivilrechtlicher Rechtsanspruch auf deren Herausgabe feststeht. Dadurch sollen sinnlose Verfahren – bei denen sich im

Nachhinein herausstellt, dass der Verfügungsbefugte die Datenbestände dem Auftraggeber nicht zugänglich machen will – vermieden werden.

Zu Art. 2 Z 78 (§ 47 Abs. 4):

Auch hier wird (vgl. auch den vorgeschlagenen § 46 Abs. 3) die Antragslegitimation klargestellt. Allerdings ist nach § 47 (anders als nach § 46) der über die Adressdaten verfügende Auftraggeber antragslegitimiert.

Zu Art. 2 Z 79 (§ 49 Abs. 3) und Z 80 (§ 50 Abs. 1 dritter Satz):

Die Einforderung des Rechts auf Bekanntgabe des Ablaufs einer automationsunterstützten Einzelentscheidung bzw. des verantwortlichen Auftraggebers in einem Informationsverbundsystem soll gleich wie beim Recht auf Auskunft erfolgen.

Zu Art. 2 Z 81 und 82 (§ 50 Abs. 2 und 2a):

Diese Bestimmungen sollen der Vereinfachung des Registrierungsverfahrens für Informationsverbundsysteme dienen. Zunächst wird in Abs. 2 klargestellt, dass dem Betreiber auch die Vornahme der Meldung (idR durch eine Vollmacht) übertragen werden kann. In diesem Fall scheint es nicht erforderlich, dass die DSK vom Betreiber Vollmachten aller Auftrageber einfordern muss, wie es § 10 des Allgemeinen Verwaltungsverfahrensgesetzes 1991, BGBl. Nr. 51 (AVG) an sich vorsehen würde. Wenn der Betreiber in der Lage ist, die Meldungen vorzunehmen, so kann das Vorliegen eines Vollmachtsverhältnisses vermutet werden. Im Zweifelsfall hat die DSK selbstverständlich die Möglichkeit, sich dieses auch nachweisen zu lassen. Die Nennung von Behörden im zweiten Satz scheint entbehrlich, sie sind idR „Dritte“. Der Datenschutzkommission als verfahrensführender Behörde wird die Pflichtenübertragung schon vor der Registrierung bekannt, daher kann sie ihr gegenüber schon mit dem Einlangen der Meldung wirksam werden.

Nach dem neuen Abs. 2a kann sich die Meldung eines Teilnehmers an einem Informationsverbundsystem hinsichtlich des Inhalts der Datenanwendung nunmehr auf einen Verweis auf eine bereits registrierte Meldung eines anderen Teilnehmers beschränken, wenn er im exakt gleichen Umfang teilnehmen will. Damit gelten für solche weiteren Meldungen im Ergebnis ähnliche Vereinfachungen wie für Musteranwendungen. Wenn sich der weitere Teilnehmer anlässlich der vereinfachten Meldung entsprechend § 19 Abs. 2 (neu) auch noch den anlässlich der „Vorbildmeldung“ bereits erteilten Auflagen unterwirft, so werden diese kraft Gesetzes mit der Registrierung für ihn ebenso wirksam, ein eigener Auflagenbescheid braucht nicht erlassen zu werden. Ein Rechtsschutzdefizit entsteht dadurch nicht, weil jedem Teilnehmer jederzeit auch die Abgabe einer gewöhnlichen Meldung offen steht und dann in der Folge über die Auflagen in Bescheidform zu entscheiden ist.

Zu Art. 2 Z 83 (9a. Abschnitt):

Allgemeines:

Durch die fortschreitende Entwicklung der Videotechnologie ist auch die Überwachung von Orten, Gegenständen und Personen durch Kameras beinahe allgegenwärtig geworden. Immer wenn dabei Personen zu sehen sind (was regelmäßig der Fall ist), fallen personenbezogene (Bild-)Daten im Sinn des DSG 2000 an – nach § 4 Z 1 genügt dafür bereits Identifizierbarkeit. Somit liegt auch ein Eingriff in das Recht auf Geheimhaltung nach § 1 Abs. 1 DSG 2000 vor, für den bisher lediglich die allgemeinen Bestimmungen des DSG 2000 über die Zulässigkeit (§§ 6 bis 9), das Registrierungsverfahren (§§ 17 ff), Informationspflichten (§ 24) und die Auskunft (§ 26) Anwendung fanden. Dies bereitete häufig Schwierigkeiten, weil diese Regelungen erkennbar nur von „klassischen“ Datenanwendungen ausgehen. Auf diese Schwierigkeiten hat der Datenschutzrat bereits wiederholt hingewiesen. Auch die Datenschutzkommission hat in ihrem jüngsten Datenschutzbericht Vollzugsprobleme aufgezeigt. Entsprechend dem Wunsch des Datenschutzrates erfolgt daher – aufbauend auf dem System der §§ 6 und 7 - nunmehr eine explizite Regelung, die Videoüberwachung durch Private in bestimmten Fällen (etwa zum Eigentumsschutz oder im Rahmen rechtlicher Sorgfaltsfristen) anerkennt. Im Hinblick auf die mannigfachen Möglichkeiten des Videoeinsatzes kann § 50a jedoch nicht den Anspruch einer abschließenden Berücksichtigung aller denkbaren Fälle erheben, in denen Videoüberwachung im Lichte von § 1 Abs. 1 und 2 zulässig sein kann. Daher gilt § 50a (ähnlich wie § 47) nur vorbehaltlich einer spezielleren Regelung in einem Materiengesetz. Die gegenständliche Regelung umfasst lediglich Bildaufnahmen und -übertragungen und keine (personenbezogenen) Tonaufnahmen oder -übertragungen. Ein „Lauschangriff“ durch Private durch Gesprächsaufzeichnungen von videoüberwachten Personen ist von der Regelung nicht erfasst. Bezüglich Tonaufzeichnungen oder -übertragungen durch öffentliche Auftraggeber ist in diesem Zusammenhang auf die ohnehin bestehenden Bestimmungen in SPG und der StPO zu verweisen.

Zu § 50a:

§ 50a Abs. 1 enthält zunächst eine Definition der Videoüberwachung. Dass dies mit „systematischer“ Erfassung von Ereignissen umschrieben wurde, soll klarstellen, dass durch eine Summe von Verwendungsschritten (vgl. § 4 Z 7) das Ergebnis „Überwachung“ verwirklicht werden soll. Aufnahmen etwa aus rein touristischen oder künstlerischen Beweggründen aber auch Filmen für ausschließlich familiäre oder persönliche Tätigkeiten (vgl. § 45, zB bei einem Kindergeburtstag) fallen damit nicht darunter, sehr wohl aber auch gezieltes Fotografieren. Überwachtes Objekt oder überwachte Person ist jene Person, Gegenstand oder Ort, auf die sich die systematische Erfassung von Ereignissen intentional richtet. Sofern Videoüberwachungen für ausschließlich persönliche und familiäre Tätigkeiten überhaupt denkbar sind (zB Bildüberwachung von Babys), fallen diese nicht unter die Bestimmungen des § 50a. Entgegen dem Judikat K600.064-001/0002-DVR/2009 der Datenschutzkommission vom 8. Mai 2009 ist aber davon auszugehen, dass der eng gefasste Wortlaut des § 45 die Überwachung von Einfamilienhäusern und dazu gehörigen Grundstücken nicht umfasst und überdies neben potenziellen Einbrechern auch andere Personen (Besucher, allfällige Hausangestellte wie etwa Reinigungspersonal) davon betroffen sein können. Derartige Datenanwendungen fallen daher unter § 50a. Was die Meldepflicht bei der Datenschutzkommission anlangt, so ist auf § 50b und die danach möglichen Ausnahmen (zB Schaffung einer Standardanwendung für bestimmte klar definierte Fälle) zu verweisen. Das in § 48 normierte „Journalistenprivileg“ bleibt unberührt.

Auch für Videoüberwachung soll das System der §§ 6 bis 9 der Struktur nach beibehalten werden. Daher ordnet § 50a Abs. 2 zunächst die Geltung der allgemeinen Bestimmungen der §§ 6 und 7 an. Hinzuweisen ist besonders auf die „gesetzliche Zuständigkeit oder rechtliche Befugnis“ nach § 7 Abs. 1 (bei den „privaten“ Überwachungstatbeständen nach Abs. 4 wird dies ein privatrechtliches Rechtsverhältnis des Auftraggebers zum überwachten Objekt oder zur überwachten Person voraussetzen) und den Verhältnismäßigkeit des § 7 Abs. 3. Dieser kommt auch in § 1 Abs 1 letzter Satz zum Ausdruck, wonach Beschränkungen nur in der gelindesten zum Ziel führenden Art vorgenommen werden dürfen. Sofern taugliche Mittel zur Zielerreichung bestehen, die weniger eingriffsintensiv sind als das Mittel der Videoüberwachung, sind diese jedenfalls einer Videoüberwachung vorzuziehen. Zu denken wäre etwa an den Einsatz von RFID-Chips an Waren in Geschäften zur Sicherung vor Diebstählen. Um dem Sicherheitsbedürfnis mancher Hauseigentümer oder Mieter Rechnung zu tragen, wäre möglicherweise die Verwendung von Sicherheitstüren, Gegensprechanlagen oder Alarmanlagen ausreichend. Grundsätzlich stellt auch der Eingriff durch Echtzeitüberwachung in das Grundrecht auf Datenschutz ein gelinderes Mittel dar als eine Speicherung der dort anfallenden Daten, wobei Echtzeitüberwachung grundsätzlich in allen in § 50a Abs. 3 und 4 genannten Fällen möglich ist. Echtzeitüberwachung wird insbesondere dann ausreichen, wenn eine Videoüberwachung ausschließlich bezweckt, das überwachte Objekt oder die überwachte Person vor einer Gefahr rechtzeitig schützen zu können bzw. bei Eintreten eines schädigenden Ereignisses (zB eines Unfalls) unverzüglich reagieren zu können.

Nach dem Verhältnismäßigkeitsgrundsatz zu beurteilen wird auch die Zulässigkeit einer Gebäudeüberwachung sein. Grundsätzlich wird davon auszugehen sein, dass die Überwachung eines Einfamilienhauses oder dessen Garten als weniger eingriffsintensiv zu beurteilen ist als etwa die Überwachung eines Hauses, in dem sich mehrere Mieter befinden. Dabei könnten sich insbesondere auch Konstellationen ergeben, in denen Rückschlüsse auf besondere sensible Daten der Hausbesucher möglich sind (etwa beim Besuch einer Arztpraxis oder eines politischen Vereines); die Zulässigkeit einer Videoüberwachung kann auch hier nur unter Bedachtnahme auf die konkrete Situation und unter sorgfältiger Abwägung der Geheimhaltungsinteressen der Betroffenen gegenüber den Interessen Dritter – unter Einhaltung des Grundsatzes des gelindesten zum Ziel führenden Mittels – beurteilt werden.

§ 50a regelt weiters die einzigen Zwecke (§ 6 Abs. 1 Z 2), für die Videoüberwachung zulässigerweise eingesetzt werden darf. Im Rahmen dieser Zwecke kann Videoüberwachung insbesondere zum Schutz von Leben, Gesundheit und Eigentumsschutz und sowie zur Erfüllung rechtlicher Sorgfaltspflichten erfolgen; diese werden in Abs. 4 Z 2 näher ausgeführt.

§ 50a Abs. 3 und 4 bestimmen - als leges speciales zu den §§ 8 und 9 – Fälle, in denen schutzwürdige Geheimhaltungsinteressen eines von Videoüberwachung Betroffenen nicht verletzt werden. Das Zustimmungsrecht des Betriebsrates nach den §§ 96 und 96a ArbVG bleibt durch sämtliche Erlaubnistatbestände (wie auch im Fall der §§ 8 und 9) unberührt.

Abs. 3 Z 1 bis 3 regeln zunächst die Fälle des § 8 Abs. 1 Z 2 und 3 bzw. § 9 Z 1 und 6 bis 8, also insbesondere jene, in denen nach § 1 Abs. 2 keine Interessenabwägung erforderlich ist. Die Zustimmung des Betroffenen (Z 2) muss grundsätzlich ausdrücklich erfolgen. Zu berücksichtigen ist allerdings, dass gewisse Verhaltensweisen insbesondere im öffentlichen Raum typischerweise darauf gerichtet sind, von jedermann wahrgenommen zu werden, und daher einem allgemein verfügbar Machen bzw. einer Zustimmung gleichzuhalten sind (Z 3). Dazu zählt etwa „Straßenkunst“ oder Auftritte im Rahmen von Veranstaltungen.

Abs. 4 Z 1, 2 und 3 gelten für den privaten Bereich (einschließlich Privatwirtschaftsverwaltung öffentlicher Auftraggeber). Videoüberwachungen im Rahmen der Hoheitsverwaltung sind in Materiengesetzen (wie insbesondere im SPG) zu regeln. Videoüberwachungen im öffentlichen Raum sind grundsätzlich den Sicherheitsbehörden vorbehalten; eine Überwachung durch Private ist in diesem Zusammenhang ausnahmsweise bei der Überwachung einer besonders gefährdeten Person (etwa durch einen privaten Sicherheitsdienst) denkbar; Ausnahmen sind weiters im Randbereich zum beschränkt öffentlichen Raum, zB wegen Verkehrssicherungspflichten, möglich. Dabei war zunächst darauf Bedacht zu nehmen, dass von einer Videoüberwachung erfasste Daten potentiell sensibel sind, weil die Bilder regelmäßig Informationen über den Gesundheitszustand oder die ethnische Zugehörigkeit (Hautfarbe) der Betroffenen liefern werden. Freilich muss auch berücksichtigt werden, dass – im Hinblick auf die Zweckvorgabe in Abs. 2 – Videoüberwachung nicht intentional auf die Gewinnung solcher Daten gerichtet sein darf, diese also nur als „Zufallsprodukt“ anfallen. Somit erfordert die Interessenabwägung verglichen mit § 8 eine einschränkendere Regelung, die freilich noch gewisse unbestimmte Rechtsbegriffe enthält („bestimmte Tatsachen“ in Z 1, die nur demonstrativ konkretisiert werden, Anknüpfen am gesamten Rechtsquellensystem für die Ermittlung von Sorgfaltspflichten in Z 2). Selbstverständlich ist auch hier der Verhältnismäßigkeitsgrundsatz stets zu beachten. Im Einzelnen ist zu den Erlaubnistatbeständen der Z 1 und 2 auszuführen:

Z 1 erlaubt die Videoüberwachung zum Schutz des überwachten Objekts oder der überwachten Person vor gefährlichen Angriffen und ermöglicht es dem Auftraggeber damit, auf konkret belegte Gefährdungssituationen zu reagieren. In dieser Bestimmung wird ein eigenständiger Begriff des „gefährlichen Angriffs“ geschaffen, der nicht mit dem des § 16 des Sicherheitspolizeigesetzes (SPG), BGBl. Nr. 566/1991 in der jeweils geltenden Fassung, gleichzusetzen ist und schon aus diesen Gründen kein Tätigwerden durch die Sicherheitsbehörden bedingt. Im Hinblick darauf, dass es sich um eine Bedrohung mit strafbaren Vorsatztaten handeln muss, ist ein überwiegendes berechtigtes Interesse des Auftraggebers anzunehmen. Dies gilt jedenfalls gegenüber dem strafrechtswidrig handelnden Angreifer, aber auch gegenüber Dritten, denen (auch im Hinblick auf § 50c) verglichen mit der tatsächlichen Verwirklichung bzw. Nichtaufklärung eines gefährlichen Angriffs eine geringfügige Beeinträchtigung ihres Geheimhaltungsanspruches zugemutet werden kann. Häufig wird es darüber hinaus so sein, dass diese Dritten direkt oder indirekt durch die Abwehr des Angriffs ebenfalls geschützt werden (zB Videoüberwachung zur Bekämpfung von Diebstählen auf einem Bahnhof). Unter Videoüberwachungen nach Abs. 4 Z 1 können auch präventive Videoüberwachungen Hinblick auf eine konkrete Gefährdung des überwachten Objekts oder der überwachten Person fallen, auch wenn noch kein gefährlicher Angriff auf dieses Objekt oder diese Person stattgefunden hat. Der Begriff des „gefährlichen Angriffs“ geht über den im Sicherheitspolizeigesetz definierten Begriff des „gefährlichen Angriffs“ hinaus: unter Z 1 können auch konkrete Gefährdungen von Geschäfts- und Betriebsgeheimnissen sowie allenfalls auch die konkrete Gefahr einer groben Verwaltungsübertretung fallen.

Beispielsweise kann es sich um einen datenschutzrechtlich zulässigen Eingriff handeln,

a) wenn das überwachte Objekt oder die überwachte Person bereits einmal Ziel oder Ort eines gefährlichen Angriffs war und eine Wiederholung wahrscheinlich ist und sich dieser gefährliche Angriff innerhalb der vergangenen zehn Jahre ereignet hat (Ist für die dem gefährlichen Angriff zu Grunde liegende gerichtlich strafbare nach § 57 des Strafgesetzbuches – (StGB), BGBl. Nr. 60/1974 in der jeweils geltenden Fassung, eine kürzere Verjährungsfrist vorgesehen, so sollen nur gefährliche Angriffe innerhalb dieser Frist relevant sein. § 58 StGB soll dabei außer Betracht zu bleiben.), oder
b) die überwachte Person einen überdurchschnittlichen Bekanntheitsgrad in der Öffentlichkeit hat oder das überwachte Objekt der Aufenthaltsort einer derartigen Person ist, oder
c) die überwachte Person/das überwachte Objekt ein verfassungsmäßiges Organ oder dessen Aufenthaltsort ist, oder
d) das überwachte Objekt ein beweglicher Gegenstand mit von erheblichem Geldwert oder ein Aufenthaltsort derartiger Gegenstände ist, oder
e) das überwachte Objekt ein Gegenstand von außergewöhnlichem überdurchschnittlichem künstlerischem Wert ist.

Aufenthaltsorte im Sinn der lit. d sind insbesondere Banken. Auch hinsichtlich anderer Geschäftslokale, wie Antiquitätengeschäfte, Juweliergeschäfte oder Tabaktrafiken, könnte man sich – soferne die Annahme besteht, dort befindliche Gegenstände könnten Ziel eines gefährlichen Angriffes werden – auf diesen Tatbestand berufen. Ebenfalls auf potentiell gefährliche Situationen, die aber nicht durch gefährliche Angriffe erzeugt sein müssen, stellt Abs. 4 Z 2 ab. Die Rechtsordnung begegnet solchen häufig mit besonderen Sorgfaltspflichten bzw. Haftungsbestimmungen, die sie bestimmten Personen mit Ingerenz für die gefährliche Situation auferlegt. Solche Bestimmungen sind über die gesamte

Rechtsordnung und auf jede ihrer Stufen verteilt (vgl. zB § 1319a ABGB, § 19 Eisenbahngesetz, §§ 6 und 8 Sbg. Veranstaltungsgesetz 1997). Um ihnen nachzukommen, soll der dadurch Verpflichtete Videoüberwachung einsetzen dürfen. Das öffentliche Interesse an der Gewährleistung des durch derartige Vorschriften intendierten Schutzes sowie das Interesse des Verpflichteten, nicht für eine Verletzung derartiger Vorschriften haften zu müssen, überwiegt – vorausgesetzt es handelt sich um ein taugliches bzw. das gelindeste Mittel – das Interesse Dritter, denen derartige Verpflichtungen nicht auferlegt sind und die auch hier regelmäßig die Nutznießer der Schutzvorschriften sein werden.

Die in Abs. 4 Z 3 geregelte Überwachung einer Person oder eines Objekts durch bloße Echtzeitwiedergabe (dh. es erfolgt keinerlei Speicherung) ist zwar eine Datenanwendung im Sinn des § 4 Z 7 und unterliegt auch der Richtlinie 95/46/EG (vgl. deren Erwägungsgrund 16 sowie Art. 2 lit. b), die Gefährdung schutzwürdiger Geheimhaltungsinteressen ist bei derartigen Systemen, jedoch deutlich herabgesetzt. Der (an sich legitime) Beweissicherungszweck kann durch sie nicht erreicht werden, möglich ist lediglich die Einleitung von (datenschutzrechtlich nicht weiter relevanten) Sofortmaßnahmen, also ein Schutzzweck. Außerdem sind sie nur zum Eigenschutz des Auftraggebers zulässig, erfolgt ein Fremdschutz durch Echtzeitüberwachung, so kann dies nicht auf diese Ziffer gestützt werden (freilich auf Z 1 oder 2). Daher kann hier typischerweise von einem Interesse des Auftraggebers ausgegangen werden, welches das Geheimhaltungsinteresse überwiegt, natürlich im Rahmen gesetzlicher Zuständigkeiten bzw. rechtlicher Befugnisse sowie unter Wahrung der Verhältnismäßigkeit (vgl. schon oben bei Abs. 2).

Videoüberwachung für Zwecke der Hoheitsverwaltung soll abgesehen von den Fällen des Abs. 3 stets nur auf besonderer gesetzlicher Grundlage stattfinden. Solche Grundlagen sind zum Teil auch schon vorhanden (vgl. zB § 54 Abs. 4 und 5 SPG).

§ 50a Abs. 5 verbietet die Durchführung von Überwachungen auf Grundlage des Abs. 4 an Orten, die dem höchstpersönlichen Lebensbereich zuzurechnen sind. Solche Orte sind etwa Privatwohnungen, Umkleide- oder WC-Kabinen. Ausdrücklich verboten ist auch die gezielte Videoüberwachung zur Kontrolle von Mitarbeiterinnen und Mitarbeitern an Arbeitsstätten, da hier davon ausgegangen werden kann, dass hier auf Grund der Eingriffstiefe stets ein gelinderes Mittel zur Kontrolle von Mitarbeiterinnen und Mitarbeitern gefunden werden kann. Dieses Verbot schließt nicht die Überwachung von Objekten an Arbeitsstätten (Überwachung von Kassenräumen, Überwachung gefährlicher Maschinen zum Schutz der Mitarbeiterinnen und Mitarbeiter) aus, da derartige Überwachungen nicht auf die Leistungskontrolle von Arbeitnehmerinnen und Arbeitnehmern gerichtet sind.

§ 50a Abs. 6 regelt den Umgang mit so genannten „Zufallstreffern“, wenn also im Rahmen einer Videoüberwachung zufällig relevante Ereignisse aufgezeichnet werden, die außerhalb des Zwecks bzw. der Zulässigkeit nach den Abs. 2 und 3 liegen. Eine Verwertung solcher Aufnahmen aus freier Entscheidung des Auftraggebers ist zum einen nur dann zulässig, wenn bei ihm der begründete (dh durch objektiv nachvollziehbare Tatsachen belegte) Verdacht entstanden ist, die gefilmten Ereignisse könnten im Zusammenhang mit von Amts wegen zu verfolgenden gerichtlich strafbaren Handlungen stehen. Zum anderen ist die Herausgabe von Daten aus einer Videoüberwachung an Sicherheitsbehörden zulässig, wenn diese die Daten gemäß § 53 Abs. 5 SPG verwenden dürfen (zB zur Abwehr eines gefährlichen Angriffs oder zur Personenfahndung). Regelmäßig wird ein derartiger begründeter Verdacht durch einen entsprechenden Hinweis Dritter entstehen.

Klargestellt wird in Abs. 6 weiters, dass der Auftraggeber gegenüber einer Behörde oder einem Gericht nicht die Herausgabe von Videodaten verweigern kann, wenn diese im Zuge eines Verfahrens die Herausgabe als Beweismittel fordern und über entsprechende Durchsetzungsmöglichkeiten (zB §§ 384 ff ZPO, § 19 AVG, §§ 109 ff StPO) verfügen. Die Verantwortung für die Rechtmäßigkeit derartiger Herausgabeforderungen trägt allein das Gericht oder die Behörde. Das Bankgeheimnis bleibt von dieser Bestimmung unberührt.

§ 50a Abs. 7 verbietet zunächst einen automationsunterstützten Abgleich der durch Videoüberwachung gewonnenen Daten mit anderen Bilddaten. So wird insbesondere eine automationsunterstützte Suche nach „unerwünschten Personen“ ausgeschlossen, welche die Gefahr einer Diskriminierung in sich birgt. Auch eine Suche innerhalb des Videomaterials nach sensiblen Kriterien im Sinn des § 4 Abs. 1 Z 2 (zB Hautfarbe) ist unzulässig. Verstöße gegen diese Bestimmung können nach § 52 Abs. 2 Z 6 geahndet werden.

Zu § 50b:

§ 50b Abs. 1 ordnet die lückenlose Protokollierung jedes Verwendungsvorganges bei Videoüberwachung an und lässt daher anders als § 14 Abs. 2 Z 7 bzw. § 14 Abs. 3 keinen Abwägungsspielraum. Die Anordnung umfasst auch Videoüberwachungen, die als Standardanwendungen betrieben werden. Bei reinen Echtzeitüberwachungen ist freilich keine Protokollierung denkbar und daher auch nicht erforderlich (vgl. auch § 14 Abs. 5).

Abs. 2 schreibt grundsätzlich eine Löschung der durch Videoüberwachung gewonnenen Daten nach 48 Stunden vor. Fällt das Ende einer Frist auf einen Samstag, Sonntag, gesetzlichen Feiertag oder den Karfreitag, so ist der nächste Werktag letzter Tag der Frist (§ 33 Abs. 2 AVG). Nur wenn Anhaltspunkte vorliegen, dass die Videoaufzeichnung zur Verwirklichung des Überwachungszwecks aufbewahrt werden muss, aufgezeichnete Daten also im Einzelfall für Schutz- oder Beweissicherungszwecke im Hinblick auf die überwachte Person/das überwachte Objekt oder für eine Weitergabe nach § 50a Abs. 6 (auch auf Grund der Beweisanforderung durch ein Gericht oder eine Behörde) länger benötigt werden, ist ausnahmsweise eine längere Aufbewahrung (so lange wie es in diesem Einzelfall erforderlich ist) zulässig. Eine längere Aufbewahrung kann durch die Datenschutzkommission durch Registrierung einer entsprechenden Meldung akzeptiert werden. Wird die Begründung nicht akzepiert, kann die Registrierung durch die Datenschutzkommission abgelehnt werden. Bei der Beurteilung ist besonders auf die allgemeine Verkehrssitte, wie etwa die Öffnungszeiten von Geschäften, Urlaube dgl. Rücksicht zu nehmen.

Zu § 50c:

§ 50c enthält einige Sonderbestimmungen für die Registrierung von Videoüberwachungen. Da das Gefährdungspotential bei Videoüberwachungen insbesondere im Hinblick auf den oft großen Betroffenenkreis und die Verwendung potentiell sensibler Daten gegenüber „herkömmlichen“ Datenanwendungen doch deutlich hinaufgesetzt ist, unterliegen diese prinzipiell – wie schon bisher – der Vorabkontrolle. Sofern sich jedoch Auftraggeber von vornherein zur Verschlüsselung der Daten verpflichten und den einzigen Schlüssel bei der Datenschutzkommission hinterlegen, unterliegen derartige Videoüberwachungen der „normalen“ Meldepflicht, dh die Verarbeitung kann sofort nach Erstattung der Meldung an die Datenschutzkommission aufgenommen werden. Diesfalls darf eine Auswertung nur im Anlassfall (zB bei einem Überfall oder einer Sachbeschädigung) vorgenommen werden. In diesem Fall ist von der Datenschutzkommission der Schlüssel der zur Entschlüsselung befugten Stelle (zB der Sicherheitsbehörde) zur Verfügung zu stellen. Mit dieser Bestimmung wird einem von Wirtschaftskreisen im Begutachtungsverfahren vorgebrachten Vorschlag entsprochen. Da bei Überwachungen nach § 50a Abs. 4 Z 1 durch die Verwendung des Begriffs „bestimmte Tatsachen“ ein beachtlicher Auslegungsspielraum besteht, wird für auf dieser Grundlage gemeldete Videoüberwachungen die Glaubhaftmachung der Tatsachen im Registrierungsverfahren vorgeschrieben. Die Art der zur Glaubhaftmachung für das Vorliegen eines der genannten Tatbestände wird je nach Überwachungssituation variieren: So könnten etwa eine oder mehrere Strafanzeigen vorgelegt werden. Weiters sind allenfalls notwendige Betriebsvereinbarungen (gemäß § 96a ArbVG) beizubringen.

Abs. 2 normiert die Ausnahmen von der Meldepflicht: Dies sind neben der Möglichkeit der Definition von Standardanwendungen die bloße Echtzeitüberwachung (wegen der vergleichsweise niedrigen Eingriffstiefe) und die Speicherung nur auf einem analogen Speichermedium. Der Einsatz solcher Medien (zB VHS-Videokassette) erfordert zwar zum Teil den Einsatz von Geräten, die automationsunterstützte Elemente enthalten, dennoch ist auf Grund der sehr beschränkten Strukturierbarkeit und damit Suchbarkeit die Gefährdung von Geheimhaltungsinteressen unbeteiligter Dritter deutlich herabgesetzt. Dies rechtfertigt eine Ausnahme von der Meldepflicht, auch nach Art. 18 Abs. 2 erster Unterabsatz der Richtlinie 95/46/EG.

§ 50c Abs. 3 regelt den in der Praxis wohl häufig auftretenden Fall, dass ein Auftraggeber mehrere gleichartige oder räumlich verbundene Personen/Objekte auf derselben Rechtsgrundlage überwachen möchte. Dies soll in einer Meldung möglich sein.

Zu § 50d:

§ 50d ist eine Spezialbestimmung zu § 24. Er konkretisiert die Informationsverpflichtung im Fall von Videoüberwachung zu einer Kennzeichnungspflicht (zB durch deutlich lesbare Aufschriften oder Piktogramme). Die Kennzeichnung soll so erfolgen, dass der Überwachung ausgewichen werden kann, was freilich nicht immer machbar sein wird. Eine Kennzeichnungspflicht entfällt dann, wenn Datenanwendungen gemäß § 17 Abs. 2 Z 4 oder nach Abs. 3 nicht gemeldet werden müssen. Letztgenannte Ausnahme bezieht sich nur auf Behörden, die im Rahmen der Vollziehung hoheitlicher Aufgaben tätig werden. Eine Berufung auf die Ausnahme nach § 17 Abs. 3 kann etwa von Sicherheitsbehörden in Anspruch genommen werden, soweit dies zur Verwirklichung des Zweckes der Videoüberwachung notwendig ist (zB Beobachten eines Drogendealers bei der Übergabe von Drogen).

Zu § 50e:

§ 50e modifiziert schließlich das Auskunftsrecht für Videoüberwachungen. Dabei ist ein Mitwirkungsrecht des Betroffenen vorgesehen, der möglichst genau Zeitraum und Ort der Überwachung benennen soll. Bei der Benennung von Anfangs- und Endpunkt können Abweichungen von einer halben Stunde bis einer Stunde als tolerierbar angesehen werden. Die Erteilung einer schriftlichen Auskunft wie

in § 26 Abs. 1 vorgesehen ist hier hinsichtlich der verarbeiteten Daten aus nahe liegenden Gründen keine transparente Lösung. Daher besteht diesbezüglich grundsätzlich ein Anspruch auf Erhalt der Videoaufzeichnung, die übrigen Auskunftsbestandteile sind schriftlich zu erteilen. Freilich muss der Geheimhaltungsanspruch Dritter gewahrt bleiben. Erlauben diese die Übersendung der Aufzeichnung an den Betroffenen nicht, so muss auf die schriftliche Auskunftserteilung in Gestalt einer präzisen Beschreibung des verarbeiteten Verhaltens zurückgegriffen werden. Alternativ kann der Auftraggeber auch eine Kopie unter technischer Unkenntlichmachung der anderen Personen zur Verfügung stellen. § 26 Abs. 6 bleibt unberührt. Das Auskunftsrecht besteht naturgemäß nicht bei Echtzeitüberwachung, da hier keine Speicherung der Daten gegeben ist. Weitere Ausnahmen vom Auskunftsrecht ergeben sich aus der in § 50c Abs.1 vorgesehenen Möglichkeit des Betreibens einer verschlüsselten Videoüberwachung, wobei der einzige Schlüssel bei der DSK zu hinterlegen ist: Da die verschlüsselten Daten vom Auftraggeber selbst nicht auf Personen rückgeführt werden können, können in diesen Fällen (entsprechend dem bereits bestehenden § 29) die durch die §§ 26 bis 28 gewährleisteten Rechte nicht geltend gemacht werden. Sobald ein Personenbezug durch Entschlüsselung hergestellt wird, ist hingegen ein Auskunftsrecht der Betroffenen gegeben.

Zu Art. 2 Z 84 und 85 (§ 51):

Durch den Wegfall des Abs. 2 wird der gegenständliche Straftatbestand von einem Ermächtigungsdelikt zu einem Offizialdelikt. Weiters wird die Formulierung des Bereicherungsvorsatzes terminologisch dem StGB angeglichen (vgl. zB dessen §§ 129 und 146). Alternativ wird der Tatbestand nunmehr auch dann erfüllt wenn eine Absicht (§ 5 Abs. 2 StGB) besteht, jemanden in seinem Recht auf Geheimhaltung zu schädigen.

Zu Art. 2 Z 86 bis 89 (§ 52 Abs. 1, 2 und 2a):

Mit diesen Bestimmungen werden die für Verwaltungsübertretungen nach § 52 vorgesehenen Höchststrafen angehoben. Weiters werden die Verwaltungsstrafbestände durch Verweise auf die im 9a. Abschnitt enthaltenen entsprechenden Bestimmungen betreffend Meldepflicht und Kennzeichnungspflicht ergänzt. Überdies werden entsprechende Sanktionen für den Verstoß gegen verbindliche Zusagen des Auftraggebers (§§ 13 Abs. 2 Z 2 und 19 Abs. 2) oder von der Datenschutzkommission ausgesprochene Auflagen, Bedingungen oder Befristungen (§ 21 Abs. 2) sowie der nach § 50a Abs. 7 und § 50b Abs. 1 erforderlichen Maßnahmen sowie gegen die in § 50b Abs. 2 vorgesehene Löschungsverpflichtung vorgesehen. Klargestellt wird, dass auch die falsche Bezeichnung einer Meldung (etwa Unterlassung der Kennzeichnung einer Datenanwendung als vorabkontrollpflichtig) strafbar ist. Weiters ist in Hinkunft auch jener Auftraggeber strafbar, der Daten des Betroffenen nicht fristgerecht beauskunftet, richtigstellt oder löscht, auch wenn er noch nicht durch Urteil oder Bescheid zur Auskunftserteilung, Richtigstellung oder Löschung verpflichtet wurde. Mit dieser Norm soll auf die Einhaltung der gesetzlichen Frist abgezielt werden. Eine unvollständige Beauskunftung ist hingegen nach wie vor unter § 52 Abs. 1 Z 3 zu ahnden. Was die Einhaltung der Frist betrifft, so ist auf die Judikatur der Datenschutzkommission (K121.525/0004-DSK/2009) zu verweisen, wonach dem Auskunftswerber erst mit dem Identitätsnachweis Anspruch auf Erteilung einer inhaltlichen Auskunft erwächst und damit die Acht-Wochen-Frist zu laufen beginnt (wobei im gegenständlichen Fall die Aufforderung zum Identitätsnachweis innerhalb von acht Wochen ab Einlangen des Auskunftsbegehrens erfolgte).

Zu Art. 2 Z 90 (§ 52 Abs. 4):

Hier wird klargestellt, dass auch Bildaufzeichnungsgeräte für verfallen erklärt werden dürfen. „Bildübertragungsgeräte“ waren jedenfalls gesondert zu erwähnen, da sie nicht unter „Datenträger“ subsumiert werden können.

Zu Art. 2 Z 91 (§ 55):

Es handelt sich lediglich um eine Anpassung des Verweises auf das aktuelle BGBlG.

Zu Art. 2 Z 95 (§ 61 Abs. 6):

Die im 9a. Abschnitt getroffenen Regelungen über Videoüberwachung entsprechen in vieler Hinsicht der bisherigen Entscheidungspraxis der Datenschutzkommission. Für Fälle, in denen sich die durch den Entwurf geschaffene Rechtslage als strenger erweist und daher bereits registrierte Videoüberwachungen nicht mehr registriert werden könnten, soll im Hinblick auf das Vertrauen der Auftraggeber in die Rechtslage und damit allenfalls verbundene Investitionen ein weiterer Betrieb der Videoüberwachung in der registrierten Form zulässig sein. Hat die Datenschutzkommission hingegen eine Befristung einer bereits registrierten Videoüberwachung verfügt, soll der Betrieb in der registrierten Form nur bis zum Ablauf dieser Befristung, wenn diese erst nach dem 31. Dezember 2012 endet, längstens bis zu diesem Zeitpunkt zulässig sein. Voraussetzung ist jeweils, dass die registrierte Videoüberwachung zum Zeitpunkt der Registrierung rechtmäßig war.

Zu Art. 2 Z 96 (§ 61 Abs. 8):

Anlässlich der Neuregelung des Registrierungsverfahrens sollen hinsichtlich der im jeweiligen Inkrafttretenszeitpunkt registrierten Datenanwendungen keine besonderen Meldepflichten entstehen. Daher sind jene Bestandteile der Meldung, die nach der neuen Rechtslage zusätzlich erforderlich sind, erst anlässlich der nächsten Änderungsmeldung der Datenschutzkommission zur Kenntnis zu bringen. Dass sich dies bei bloßen Streichungen erübrigt, versteht sich von selbst.

Zu Art. 2 Z 97 (§ 64):

Die Vollzugsklausel wird an die neue Kompetenzrechtslage angepasst.

Zu Art. 3 Z 1 (§ 54 Abs. 8 SPG):

Echtzeitüberwachung (unter Einsatz von Bildübertragungsgeräten) stellt einen Eingriff in das Recht auf Geheimhaltung nach § 1 Abs. 1 DSG 2000 dar und unterliegt daher den in Abschnitt 9a des DSG 2000 geschaffenen Bestimmungen zur Videoüberwachung. Spezifische Ermächtigungen für diese Form der Datenermittlung sind auch im Sicherheitspolizeigesetz vorzusehen.

Wie zu § 50a DSG 2000 ausgeführt wird, stellt der Eingriff in das Grundrecht auf Datenschutz durch Echtzeitüberwachung ein gelinderes Mittel dar als eine Speicherung der Daten, weshalb er jedenfalls in den Fällen zulässig ist, in denen das SPG eine ausdrückliche Ermächtigung zur Bildaufzeichnung enthält. Darüber hinaus dürfen Übertragungsgeräte im Rahmen sicherheitspolizeilicher Aufgabenerfüllung, insbesondere auch zur Unterstützung des Streifen- und Überwachungsdienstes gemäß § 5 Abs. 3 SPG eingesetzt werden.