Vorblatt

Ziel und Inhalt:

Der vorliegende Gesetzentwurf

- fasst das Grundrecht auf Datenschutz in eine sprachlich verbesserte Form und beschränkt seinen Anwendungsbereich auf natürliche Personen;

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

- enthält Klarstellung von in der Vollzugspraxis aufgetretener Rechtsfragen;

- sieht eine betrieblichen Datenschutzbeauftragten für größere Betriebe vor;

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

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

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

Alternativen:

Keine

Auswirkungen des Regelungsvorhabens

- Finanzielle Auswirkungen:

Durch die teils massive Einschränkung von Prüf- bzw. Meldepflichten im Registrierungsverfahren und durch die Einschränkung des Grundrechtsschutzes auf natürliche Personen sind Arbeitsentlastungen größeren Ausmaßes im Bereich des Datenverarbeitungsregisters sowie bei der Rechtskontrolle durch die vom Bund auszustattende Datenschutzkommission zu erwarten, die zur Entschärfung der angespannten Personalsituation beitragen sollen.

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:

Durch die Einführung eines betrieblichen Datenschutzbeauftragten kommt es zu einem marginalen Mehraufwand für Unternehmen, weil ein zusätzliches Feld in der DVR-Meldung ausgefüllt werden muss.

Durch die Verringerung des Kreises der Auskunftsberechtigten auf natürliche Personen kommt es zu einer Entlastung der Unternehmen von Auskunftspflichten; eine marginale Belastung für Unternehmen kann dadurch entstehen, dass vom Auskunftsberechtigten irrtümlich in Anspruch genommene Dienstleister den Auftraggeber bekanntgeben müssen.

- 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 Abwesenheit 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. Durch die Einführung eines betrieblichen Datenschutzbeauftragten in Betrieben mit mehr als 20 MitarbeiterInnen soll ArbeitnehmerInnen die Durchsetzung ihrer Rechte und Interessen nach dem DSG 2000 erleichtert werden. Schließlich enthält die Novelle eine verständlichere Formulierung einiger Bestimmungen (ohne wesentliche Veränderung des Inhalts), insbesondere auch des Grundrechts auf Datenschutz, dessen Anwendungsbereich überdies auf natürliche Personen beschränkt werden soll, sowie eine Bereinigung der unübersichtlichen Kompetenzrechtslage.

Als Inkrafttretenszeitpunkt ist der 1. Juli 2008 vorgesehen, die Bestimmungen über den betrieblichen Datenschutzbeauftragten sollen im Hinblick auf eine angemessene Vorbereitungszeit jedoch erst am 1. Juli 2009 in Kraft treten.

Finanzielle Auswirkungen:

- Auswirkungen auf andere Gebietskörperschaften:

Durch die vorgeschlagene Kompetenzbereinigung (§ 2), 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 Kosten in derzeit noch nicht zu beziffernder Höhe an.

- Auswirkungen auf den Stellenplan des Bundes:

Die vorgeschlagenen Änderungen durch die DSG-Novelle 2008 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:

Die vorgesehene Meldung der Bestellung eines betrieblichen Datenschutzbeauftragten (§ 19 Abs. 1 Z 8) verursacht keine wesentlichen Auswirkungen auf die Verwaltungslasten für Untenehmen.

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.

Eine Minderung der Verwaltungslasten in nicht zu beziffernder Höhe entsteht durch die Möglichkeit, Meldungen an das Datenverarbeitungsregister künftig online vornehmen zu können (§ 21a).

Durch die Verkleinerung des Kreises der Auskunftsberechtigten auf natürliche Personen ist mit einer entsprechenden Verringerung von Auskunftsersuchen an Unternehmen zu rechnen, wodurch eine Minderung ihrer Verwaltungslasten eintritt. Von den im Rechtsinformationssystem des Bundes veröffentlichten Entscheidungen der Datenschutzkommission seit dem Jahr 2004 betrafen lediglich 7,75 % Auskunftswerber, die keine natürliche Person waren. Es wird daher davon ausgegangen, dass sich die Zahl der Auskunftsbegehren an Unternehmen um denselben Prozentsatz verringern wird. Dadurch ergibt sich eine Minderung der Veraltungslasten für Unternehmen aus der Auskunftspflicht (§ 26) von 695.350 Euro laut Baiserhebung im Sommer 2007 um 7,75 % auf 641.460 Euro.

Zur Melde-, Protokollierungs-, Informations- und Auskunftspflicht bei Videoüberwachung (§§ 50b bis 50e) sind gegenüber der gegenwärtigen Rechtslage insgesamt kaum Änderungen an Verwaltungslasten zu erwarten, die mangels seriöser Daten derzeit auch nicht beziffert werden können.

Kompetenzgrundlage:

Der vorliegende Entwurf stützt sich hinsichtlich der Verfassungsbestimmungen auf Art. 10 Abs. 1 Z 1 B-VG (Bundesverfassung), ansonsten auf den nunmehr neu gefassten § 2 DSG 2000 (Angelegenheiten des Schutzes personenbezogener Daten).

Besonderheiten des Normerzeugungsverfahrens:

Z 10, 11, 12, 13, 68, 83 und 89 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 die Bestimmung der Z 3 überdies die Zuständigkeit der Länder in der Vollziehung 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 Z 10 (§ 1):

Durch die vorgeschlagene Änderung soll das Grundrecht auf Datenschutz verständlicher formuliert werden, ohne dass es dabei zu Änderungen in der Substanz kommt. Die einzige wesentliche Änderung betrifft die Beschränkung des Grundrechts und im Weiteren auch des DSG 2000 auf personenbezogene Daten natürlicher Personen. Damit folgt Österreich einem europaweiten Trend, da die meisten in Umsetzung der „Datenschutzrichtlinie“ 95/46/EG ergangenen europäischen Datenschutzgesetze – so wie die Datenschutzrichtlinie selbst auch – nur den Datenschutz natürlicher Personen regeln. Was die Daten juristischer Personen betrifft, so lässt sich schwerlich argumentieren, dass sie einer den natürlichen Personen vergleichbaren Schutzwürdigkeit unterliegen. Vielmehr stieß der weite auch auf juristische Personen bezogene Anwendungsbereich des DSG 2000 immer wieder – auch im europäischen Kontext – vielfach auf Unverständnis. Wie die Praxis gezeigt hat, reduziert sich der Datenschutz juristischer Personen im Wesentlichen auf Daten, die einem Geschäfts- oder Betriebsgeheimnis unterliegen. Das Geschäfts- und Betriebsgeheimnis ist aber in der österreichischen Rechtsordnung ohnehin durch andere Bestimmungen (zB des gewerblichen Rechtsschutzes oder des Urheberrechts) geschützt. Die Einschränkung der Bestimmungen des DSG 2000 auf den Datenschutz natürlicher Personen würde im Übrigen auch zu Entlastungen von Unternehmen selbst (z. B. bei der Registrierungspflicht oder bei der Verpflichtung, den Betroffenen Auskunft zu erteilen) führen.

Die bisher in 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 die allgemeine Verfügbarkeit dieser Daten gegeben war. Die „Datenschutzrichtlinie“ 95/46/EG kennt nämlich die bisher in § 1 DSG 2000 enthaltene Einschränkung nicht und bezieht sich grundsätzlich auf alle personenbezogene Daten, wobei des Weiteren in der Richtlinie Tatbestände festgelegt werden, bei deren Vorliegen personenbezogene Daten verwendet werden dürfen (siehe 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, wenn eine Rückführbarkeit dieser Daten gegeben ist, weshalb auch diese Passage entfallen kann.

Eine weitere geringfügige Änderung des Eingriffsvorbehalts liegt darin, dass fortan Eingriffe nicht nur im lebenswichtigen Interesse des Betroffenen sondern allgemein im lebenswichtigen Interesse jeder Person unmittelbar auf Grund von § 1 Abs. 2 zulässig sind. Solche Eingriffe müssen sich also fortan nicht mehr auf das überwiegende berechtigte Interesse stützen und bedürfen keiner gesetzlichen Anordnung (wiewohl sich eine solche unverändert in § 8 Abs. 3 Z 3 und § 9 Z 8findet).

Durch den Begriff „staatliche Eingriffe“ in Abs. 2 wird klargestellt, dass auch Eingriffe im Rahmen der schlichten Hoheitsverwaltung und auch durch „Beliehene Private“ einer gesetzlichen Determinierung bedürfen.

In Abs. 3 wird klargestellt, dass auch die Rechte auf Auskunftserteilung, Richtigstellung und Löschung nur natürliche Personen in Anspruch nehmen können.

Zu Z 11 (§ 2):

Die bisherige Kompetenzrechtslage erwies sich vor allem seit Inkrafttreten der Richtlinie 95/46/EG als äußerst unbefriedigend, weil diese ein einheitliches Schutzniveau für automationsunterstützt und konventionell (dh in Dateiform) verarbeitete Daten vorsieht. So waren zur Umsetzung der Richtlinie das DSG 2000 und neun durch die Richtlinie bzw. den universell geltenden § 1 im Wesentlichen vordeterminierte Landesdatenschutzgesetze erforderlich, wobei auch der den Ländern verbleibende Vollzugsspielraum minimal war. Somit soll der Schutz personenbezogener Daten zur Gänze in die Bundeskompetenz verschoben werden. Dies schließt freilich – wie schon bisher – die Erlassung von auf den Regelungsgegenstand bezogenen Datenverwendungsbestimmungen in Landesgesetzen nicht aus.

Zu Z 12 und 13 (§ 3 Abs. 1 und 2):

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 auch Art. 4 der Richtlinie über das anwendbare einzelstaatliche Recht auch hinsichtlich dieser Staaten umzusetzen ist.

Zu Z 14 und 24 (§ 4) sowie zu Z 82 (Aufhebung von § 58):

In § 4 soll künftig – aufbauend auf der neuen Kompetenzrechtslage - der Regelungsgegenstand von den Begriffsbestimmungen entflochten und in einem eigenen Abs. 2 normiert werden. Nach der Regelung des nunmehrigen Abs. 1, der in neutraler Art (dh unabhängig von Datenanwendungen) die einzelnen Begriffe umschreiben soll, wird in Abs. 2 bestimmt, dass die Grundsätze des § 6 sowie § 7 Abs. 2 und 3 iVm § 8 für Übermittlungen allgemein (dh unabhängig von der Datenverwendung in einer Datenanwendung oder manuellen Datei) gelten. Die übrigen materiellrechtlichen Abschnitte gelten in Ausgestaltung des Grundrechts zum Großteil für Datenanwendungen und Dateien, zum Teil auch nur für Datenanwendungen. Der bisherige § 58 wird damit obsolet.

Zu Z 15 (§ 4 Abs. 1 Z 3):

Die Änderung entspricht der Einschränkung des Datenschutzes auf natürliche Personen (siehe die Erläuterungen zu § 1 DSG 2000).

Zu Z 16 (§ 4 Abs. 1 Z 4):

Mit dieser Bestimmung soll eine Vereinfachung des Auftraggeberbegriffes vorgenommen werden.

Zu Z 17 (§ 4 Abs. 1 Z 5):

Mit der (nunmehr richtlinienkonformen) Neuformulierung soll klargestellt werden, dass Dienstleister auch als so genannte „Ermittlungsdienstleister“ tätig werden können, indem sie im Auftrag des Auftraggebers Daten durch Dritte erhalten und damit diese für den Auftraggeber im Rahmen ihres Dienstleistervertrages (oder einer anderen Rechtsgrundlage) „ermitteln“. Nicht als Dienstleister anzusehen sind aber folgende Fälle:

- ein Empfänger von Daten, der für die Weitergabe an ihn ein Entgelt leistet;

- ein Auftragnehmer, der Daten, die er im Zuge der Erteilung verschiedener Aufträge erhalten hat, verknüpft; oder

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

Zu Z 18 (§ 4 Abs. 1 Z 7):

Der Klammerausdruck (früher „Datenverarbeitung“), der sich noch auf das „alte“ DSG bezog, kann nunmehr nach acht Jahren Anwendung der neuen Terminologie des DSG 2000 entfallen.

Zu Z 19 und Z 23 (§ 4 Abs. 1 Z 8 und Z 12):

In diesen Bestimmungen entfällt die Bezugnahme auf die „Datenanwendung“ (siehe die allgemeinen Ausführungen zu § 4).

Zu Z 20 und 21 (§ 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 Z 22 (§ 4 Abs. 1 Z 11):

Die Neuformulierung des „Überlassens“ stellt klar, dass darunter auch der Datenfluss vom Dienstleister zum Auftraggeber gemeint sein kann (z. B. im Fall eines „Ermittlungsdienstleisters“, siehe dazu die Ausführungen zu § 4 Abs. 1 Z 5).

Zu Z 25 (§ 8 Abs. 1):

Diese Angleichung entspricht der Änderung des § 1 Abs. 1. Dementsprechend wird auf die im einfachgesetzlichen Teil des DSG 2000 genannten „schutzwürdigen Geheimhaltungsinteressen“ abgestellt.

Zu Z 26 (§ 8 Abs. 2):

Die Aufhebung dieser Bestimmung erfolgt lediglich aus Gründen der Klarstellung: Das Widerspruchsrecht nach § 28 Abs. 2, das auch für veröffentlichte Daten gilt, wird dadurch nicht eingeschränkt. Ein Widerspruchsrecht gegen die Verwendung indirekt personenbezogener Daten wäre jedoch sinnwidrig und bestand nach § 29 auch bisher nicht.

Zu Z 27 und 30 (§ 8 Abs. 3 Z 2, § 9 Z 4):

In der Vergangenheit war die Zulässigkeit der Übermittlung personenbezogener Daten bei der Erfüllung von Verpflichtungen im Rahmen der parlamentarischen Kontrolltätigkeit (insb. Beantwortung parlamentarischer Anfragen, Aktenübermittlung an Untersuchungsausschüsse) hinsichtlich der datenschutzrechtlichen Zulässigkeit immer wieder umstritten, insbesondere im Hinblick darauf, wer die Erforderlichkeit personenbezogener Antworten oder Akten zu beurteilen hat. Durch die – auch im Hinblick auf den ähnlichen Wortlaut der Art. 22 und 53 Abs. 3 B-VG - nahe liegende Gleichstellung mit der Amtshilfe wird nunmehr klar gestellt, dass dies im Wesentlichen der ersuchenden parlamentarischen Körperschaft obliegt. Dem ersuchten Auftraggeber verbleibt die Beurteilung der Zuständigkeit und der Frage, ob die Übermittlung denkmöglich ist (vgl. den Bescheid der Datenschutzkommission vom 29. November 2006, GZ K121.229/0006-DSK/2006).

Zu Z 28 und 31 (§ 8 Abs. 3 Z 5, § 9 Z 9):

Hier erfolgt lediglich eine Anpassung an Art. 8 Abs. 2 lit. e der Richtlinie 95/46/EG. Nach dem bisherigen Wortlaut war eine Ermittlung von Daten für Zwecke der Anspruchsdurchsetzung nicht erfasst. Freilich muss als Ausdruck des Verhältnismäßigkeitsgrundsatzes die Relevanz für ein behördliches (gerichtliches) Verfahren denkmöglich sein, dh es muss im Zeitpunkt der Datenverwendung der damit verfolgte Anspruch relativ präzise bestimmt sein.

Zu Z 29 (§ 8 Abs. 4):

Die bisherige Regelung über die Verwendung von strafrechtsrelevanten Daten scheint insofern ergänzungsbedürftig, als der hier genannte Fall der Anzeigeerstattung (gleich in welcher Art von Strafverfahren) unter keinen der dort genannten Tatbestände eindeutig subsumierbar scheint.

Zu Z 32 (§ 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 Z 33 (Aufhebung von § 13 Abs. 3):

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

Zu Z 34 (§ 15a), Z 40 (§ 19 Abs. 1 Z 8) und Z 49 (§ 30 Abs. 1a):

Die Einführung eines betrieblichen Datenschutzbeauftragten, der die Einhaltung des DSG 2000 im Betrieb überwachen und die dortigen Arbeitnehmer sowie den Betriebsinhaber in Angelegenheiten des Datenschutzes beraten soll, entspricht einer langjährigen Forderung der Arbeitnehmervertretungen. Organisatorisch dienten im Wesentlichen die Bestimmungen über Sicherheitsfachkräfte in den §§ 73 ff

ASchG als Vorbild, wobei vom Nachweis spezieller Fachkenntnisse vorerst abgesehen wird. Die Beurteilung der Eignung obliegt im Wesentlichen dem Betriebsinhaber, Voraussetzung ist aber jedenfalls volle Geschäftsfähigkeit.

Um die Bestellung auch nachvollziehbar zu machen, ist sie in Meldungen an die Datenschutzkommission anzugeben (s. dazu auch die Übergangsbestimmung in § 61 Abs. 8). Erfolgt sie rechtswidrigerweise nicht, so ist letztlich die Registrierung abzulehnen. Die Datenschutzkommission kann nach dem neuen § 22a Abs. 6 auch die Bestellung eines betrieblichen Datenschutzbeauftragten dem Betriebsinhaber (sofern er gleichzeitig Auftraggeber ist) mit Bescheid auftragen.

Der Datenschutzbeauftragte kann sich nach dem neuen § 30 Abs. 1a in Angelegenheiten des Betriebes an die Datenschutzkommission wenden, sofern er vorher dem Betriebsinhaber den Verdacht einer Verletzung datenschutzrechtlicher Vorschriften nach § 15a Abs. 3 mitgeteilt hat und der Inhaber nach Ansicht des Beauftragten dennoch innerhalb einer angemessenen Frist (die Angemessenheit ist je nach dem Umfang der erforderlichen Maßnahmen zu beurteilen) keinen rechtmäßigen Zustand hergestellt hat.

Zu Z 35 (§ 16 Abs. 1):

Die Regelung hat klarstellenden Charakter und entspricht der derzeitigen Praxis der Registerführung.

Zu Z 36 (§ 16 Abs. 3):

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

Zu Z 37 (§ 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.

Zu Z 38 (§ 17 Abs. 1a und b):

Das Datenverarbeitungsregister soll künftig in Form einer Datenbank geführt und Meldungen nur mehr in automationsunterstützter Form über eine Internetanwendung (also online) erstattet werden, damit die Verwaltungsabläufe vereinfacht und beschleunigt werden können. Da der Kreis der Meldepflichtigen ausschließlich Personen umfasst, die Datenanwendungen – also automationsunterstützte Systeme – einsetzen, scheint die Beschränkung auf den elektronischen Einbringungsweg sachlich gerechtfertigt und zumutbar (zu manuellen Dateien vgl. § 4 Abs. 2). Der Einsatz der Bürgerkarte dabei entspricht der IKT-Strategie des Bundes.

Im Hinblick auf die Vereinfachungen bei der Registerführung und damit im Registrierungsverfahren – bei nicht vorabkontrollpflichtigen Meldungen soll künftig die sofortige Registrierung nach einer bloß automationsunterstützten Prüfung der Regelfall sein - darf im Gegenzug eine meldepflichtige Datenanwendung fortan ausnahmslos nur mehr dann betrieben werden, wenn sie registriert ist. Dies gilt selbstverständlich auch für die Vornahme von meldepflichtigen Änderungen.

Zu Z 39 (§ 18 samt Überschrift):

§ 18 regelt fortan nur mehr die Fälle der Vorabkontrolle, für die das nunmehr allgemeine Prinzip des § 17 Abs. 1a schon bisher gegolten hat. Daher wird auch die Überschrift angepasst. „Vorabkontrolle“ bedeutet im Hinblick auf § 17 Abs. 1b fortan nur mehr eine „vertiefte“ (dh im Sinn von § 19 Abs. 3 vollständige) Form der Prüfung vor der Registrierung. Die Fälle der Vorabkontrollpflicht in Z 1 bis 4 bleiben gegenüber dem früheren Abs. 2 freilich unverändert.

Zu Z 40 (§ 19 Abs. 1 Z 3a):

Dieser Erklärung kommt bei der nach § 20 und § 21a zu treffenden Entscheidung, ob die Meldung nur automationsunterstützt zu prüfen ist, maßgebliche Bedeutung zu.

Zu Z 42 (§§ 20 bis 22):

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. Eine solche 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) verständigt werden kann.

Nur wenn es beim automationsunterstützten Prüfverfahren zu einer Fehlermeldung (dh. der Algorithmus erkennt eine Unvollständigkeit oder Unplausibilität) kommt und der Auftraggeber trotzdem auf der

Einbringung besteht, findet eine vollständige Prüfung nicht vorabkontrollpflichtiger Meldungen nach § 19 Abs. 3 statt (§ 20 Abs. 2). Als vorabkontrollpflichtig bezeichnete Meldungen werden hingegen vor ihrer Registrierung stets nach § 19 Abs. 3 geprüft (§ 20 Abs. 3 iVm § 18).

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. 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 drei Jahren ersichtlich zu machen sind. Daher sind insbesondere gestrichene Auftraggeber bzw. Datenanwendungen erst nach Ablauf dieser Frist zu löschen.

Abs. 2 iVm Abs. 3ermöglicht nunmehr auch in Fällen, in denen der Datenschutzkommission bekannt wird, dass eine einzelne Datenanwendung zur Gänze (ohne erkennbare Wiederaufnahmeabsicht) aufgegeben wurde, eine vereinfachte Streichung durch Mandatsbescheid.

Neu ist die gesetzliche Regelung der Rechtsnachfolge in Abs. 4. Sie baut auf der Idee des geltenden § 13 DVRV 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 Z 43 (§ 22a):

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 registrierter Meldungen durch die Datenschutzkommission (vgl. auch § 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. 3), die in der Regel (außer die Mangelhaftigkeit tritt erst nachträglich durch Änderungen der Rechtslage ein; s. dazu zB die Übergangsbestimmung für Videoüberwachung in Z 85) eigentlich schon im Zuge des Registrierungsverfahrens hätten hervorkommen müssen, 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*, Verwaltungsvefahren, 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 und 6 regeln die Sonderfälle, dass sich als Ergebnis des Berichtigungsverfahrens bloß Mängel bei den Datensicherheitsmaßnahmen bzw. das Fehlen eines nach § 15a Abs. 1 erforderlichen betrieblichen Datenschutzbeauftragten ergibt.

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

Zu Z 44 und 45 (§ 26 Abs. 1 bis 7):

Abgesehen von der Beschränkung des Auskunftsrechts auf natürliche Personen im Lichte von § 1 Abs. 3 Z 1 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 natürlichen 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).

Zu Z 46 (§ 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.

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 Z 47 (§ 26 Abs. 10):

Die ersten beiden Sätze wurden nur sprachlich geringfügig angepasst und bleiben inhaltlich unverändert. In den beiden neuen Sätzen erfolgt der Schluss einer Lücke im System des Auskunftsrechts: Wenn der Auskunftswerber ein Auskunftsbegehren irrtümlich an einen Dienstleister richtet, so hat ihm dieser nunmehr den Auftraggeber zu benennen. Stattdessen kann er das Auskunftsbegehren auch gleich an den Auftraggeber weiterleiten, für den mit dem Einlangen die achtwöchige Frist nach Abs. 4 zu laufen beginnt.

Zu Z 48 (§ 27 Abs. 9):

Durch den Entfall der Einschränkung auf *öffentliche* Bücher und Register wird der in Z 45 ausgeführte Gedanke auf die Richtigstellung und Löschung übertragen: Wenn ein besonderes Verfahren vorgesehen ist, um die (zum Teil anders bezeichnete) Richtigstellung/Löschung aus einem behördlich geführten Buch oder Register zu erlangen, so geht dieses der Rechtsdurchsetzung nach dem DSG 2000 vor (zB Berichtigung nach § 15 MeldeG).

Zu Z 49 (§ 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 Z 51 und 53 (§ 30 Abs. 2a und Abs. 6):

Auch diese Bestimmung soll den Entfall der inhaltlichen Prüfung von nicht vorabkontrollpflichtigen Registermeldungen im Sinne einer verwaltungseffizienten und am Rechtsschutzbedarf orientierten Lösung ausgleichen (s. schon oben zu Z 41 und 42): 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 (und endet) das Verfahren nach § 30 im Fall eines Verdachts der Nichterfüllung der Meldepflicht bei 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 Z 52 (§ 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.

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

Zu Z 54 (§ 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 die 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 Z 55 (§ 31):

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 insb. 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.

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 2. Satz) vorgesehen. Diesbezüglich bestand bisher (jedenfalls dem Wortlaut nach) eine Rechtsschutzlücke.

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 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 zu Z 42 Gesagte sinngemäß.

Zu Z 56 (§ 31a):

Zur Wahrung der Übersichtlichkeit des § 31 werden mit dem Beschwerdeverfahren zusammenhängende Instrumente nunmehr in § 31a geregelt. Zunächst wird in dessen Abs. 1 eine Z 30 und 31 entsprechende 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 § 22 Abs. 4 und 5 (Z 26 und 27) der Datenschutzkommission genau die gleichen Möglichkeiten geben. Hinsichtlich des Bestreitungsvermerks wird nunmehr in § 31a Abs. 2 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. 3 unverändert wieder. Es wird lediglich angeordnet, dass die ersten beiden Sätze im Verfahren nach § 30 sinngemäß anzuwenden sind.

Zu Z 57 bis 59 (§ 32 Abs. 1, 4 und 6):

Hier gilt das schon zu Z 37 Ausgeführte analog: Es werden materiellrechtliche Begriffe durch prozessrechtliche ersetzt bzw. die Terminologie an § 1 Abs. 5 angeglichen.

Zu Z 60 (§ 32 Abs. 7):

Diese neue Verpflichtung des Gerichts zur Kontaktaufnahme mit der Datenschutzkommission, um die Erfüllung der Meldepflicht im Hinblick auf eine klagsgegenständliche Datenanwendung zu überprüfen, soll ebenfalls den Entfall der Prüfung nicht vorabkontrollpflichtiger Datenanwendungen ausgleichen (s. schon oben zu Z 42, Z 50 und 52 sowie Z 54).

Zu Z 61 (§ 34 Abs. 1):

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

Zu Z 62 (§ 34 Abs. 3):

Die Bestimmung wird sprachlich vereinfacht und dadurch gleichzeitig etwas weiter gefasst, was der Intention des Art. 28 Abs. 6 der Richtline 95/46/EG entspricht. Zur Erweiterung auf den Europäischen Wirtschaftsraum vgl. die Erwägungen zu Z 5, 6 und 24.

Zu Z 63 (§ 34 Abs. 4):

Vgl. die Erwägungen zu Z 5, 6 und 24.

Zu Z 64 (§ 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 Z 65 (§ 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 Z 66 (§ 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 waren. Bei den übrigen Mitgliedern wird – da ihre Mitgliedschaft nicht auf einem Dienstverhältnis beruht – eine Altersgrenze eingeführt.

Zu Z 67 (§ 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. inbesondere Art. 29 der RL 95/46/EG) und daher den Mitgliedern auch Reisetätigkeit abverlangt wird. Nunmehr wird dafür explizit ein öffentlich-rechtlicher Ersatzanspruch vorgesehen.

Zu Z 68 (§ 38 Abs. 1):

Es handelt sich lediglich um eine Anpassung der Verweise.

Zu Z 69 (§ 39 Abs. 5):

Durch diese Regelung wird lediglich die bisherige Praxis gesetzlich festgeschrieben.

Zu 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 bleibt aber hinsichtlich dieser Auftraggeber weiterhin einer speziellen gesetzlichen Anordnung (zB § 91 Abs. 1 Z 2 SPG) vorbehalten.

Zu Z 71 (§ 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 Z 72 (§ 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 Z 73 (§ 46 Abs. 1):

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

Zu Z 74 (§ 46 Abs. 2):

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

Zu Z 75 (§ 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 Z 76 (§ 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 Z 77 (§ 47 Abs. 4):

Auch hier wird (vgl. Z 60) die Antragslegitimation klargestellt. Allerdings ist nach § 47 (anders als nach § 46) der über die Adressdaten verfügende Auftraggeber antragslegitimiert.

Zu Z 78 (§ 49 Abs. 3) und Z 79 (§ 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 Z 80 und 81 (§ 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. 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. Damit gelten für solche weiteren Meldungen im Ergebnis ähnliche Vereinfachungen wie für Musteranwendungen. Wenn sich der weitere Teilnehmer anlässlich der vereinfachten Meldung 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.

Zu Z 82 (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 als Mittel der Gefahrenabwehr durch Private 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.

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 fallen damit nicht darunter, sehr wohl aber auch gezieltes Fotografieren. Überwachtes Objekt ist jene Person, Gegenstand oder Ort, auf die sich die systematische Erfassung von Ereignissen intentional richtet.

§ 50a Abs. 2 regelt die einzigen Zwecke (§ 6 Abs. 1 Z 2), für die Videoüberwachung zulässigerweise eingesetzt werden darf.

§ 50a Abs. 3 bestimmt - als lex specialis zu den §§ 8 und 9 – Fälle, in denen schutzwürdige Geheimhaltungsinteressen eines von Videoüberwachung Betroffenen nicht verletzt werden. Z 1 bis 3 regeln zunächst jene Fälle, 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 einer Zustimmung gleichzuhalten sind (Z 3). Dazu zählt etwa „Straßenkunst“ oder Auftritte im Rahmen von Veranstaltungen.

Die Z 4 bis 6 sind – ebenso wie § 8 Abs. 3 und ein Großteil des § 9 - das Ergebnis typisierender Interessenabwägungen nach § 1 Abs. 2. 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 5, die nur demonstrativ konkretisiert werden, Anknüpfen am gesamten Rechtsquellensystem für die Ermittlung von Sorgfaltspflichten in Z 6). Selbstverständlich ist auch der Verhältnismäßigkeitsgrundsatz der §§ 1 Abs. 2 und 7 Abs. 3, insbesondere im Hinblick auf die Tauglichkeit von Videoüberwachung zur Zweckerreichung und das gelindeste Mittel, stets zu beachten. Im Einzelnen ist zu den Erlaubnistatbeständen der Z 4 bis 6 auszuführen:

- Die Überwachung eines Objekts durch bloße Echtzeitwiedergabe (dh. es erfolgt keinerlei Speicherung; Z 1) 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, jedenfalls dann, wenn sie nur Rechtsgüter des Auftraggebers schützen sollen. 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. Daher kann hier generell von einem Interesse des Auftraggebers ausgegangen werden, das Geheimhaltungsinteressen überwiegt.

Echtzeitüberwachungen, die dem Schutz von Rechtsgütern Dritter dienen, können allenfalls – eine gesetzliche Zuständigkeit oder eine rechtliche Befugnis nach § 7 Abs. 1 vorausgesetzt – auf Z 2 oder 3 gestützt werden.

- Z 5 erlaubt die Videoüberwachung zum Schutz des überwachten Objekts vor gefährlichen Angriffen im Sinn des SPG und ermöglicht es dem Auftraggeber damit, auf konkret belegte Gefährdungssituationen zu reagieren. Im Hinblick darauf, dass es sich um eine Bedrohung mit gerichtlich 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 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).

Die beispielhafte Aufzählung in den lit. a bis e soll auch als Maßstab für vergleichbare Fälle dienen, die nicht ausdrücklich angeführt sind.

- Ebenfalls auf potentiell gefährliche Situationen, die aber nicht durch gefährliche Angriffe erzeugt sein müssen, stellt Z 6 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.

- Durch Z 7 wird schließlich der zweite Fall des Art. 8 Abs. 5 lit. e der Richtlinie 95/46/EG umgesetzt. Videoüberwachung darf demnach zur Anspruchsverfolgung vor einem Gericht (im Sinn des EGV) erfolgen. Dass eine derartige Anspruchsverfolgung erforderlich sein wird, muss freilich manifest sein, dh

der Auftraggeber ist entweder selbst belangt worden oder hat einen begründeten konkreten Verdacht einer Verletzung seiner Rechte.

§ 50a Abs. 4 grenzt den Anwendungsbereich der Erlaubnistatbestände nach Abs. 3 Z 4 bis 6 auf „Private“ im weiteren Sinn (dh einschließlich der Privatwirtschaftsverwaltung) ein. Dahinter steht der Gedanke, dass Videoüberwachung für Zwecke der Hoheitsverwaltung abgesehen vom Fall des lebenswichtigen Interesses stets nur auf besonderer gesetzlicher Grundlage stattfinden soll. Solche Grundlagen sind zum Teil auch schon vorhanden (vgl. zB § 54 Abs. 4 und 5 SPG).

Durch den zweiten Satz wird die Durchführung von Überwachungen auf Grundlage des Abs. 3 Z 4 bis 6 an Orten verboten, die dem höchstpersönlichen Lebensbereich zuzurechnen sind. Solche Orte sind etwa Privatwohnungen, Umkleide- oder WC-Kabinen.

§ 50a Abs. 5 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 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, sei es, dass diese schon begangen wurden (Z 1) oder ihre Verwirklichung droht bzw. im Gange ist, dh in der Terminologie des SPG die Videodaten der Abwehr oder Beendigung eines gefährlichen Angriffs dienen könnten. Regelmäßig wird ein derartiger begründeter Verdacht durch einen entsprechenden Hinweis Dritter entstehen.

Klargestellt wird in Abs. 5 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.

§ 50a Abs. 6 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 Haufarbe) ist unzulässig.

§ 50a Abs. 7 ordnet – nur der Deutlichkeit halber – nochmals die zusätzlich Geltung der allgemeinen Bestimmungen der §§ 6 und 7, insb. des Verhältnismäßigkeitsgrundsatzes, an. Dieser kommt insbesondere 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 genannten Fällen möglich ist. Die ausdrückliche Erwähnung der Echtzeitüberwachung in § 50a Abs. 3 Z 4 erfolgt deshalb, weil nur der dort genannte Tatbestand unter die in § 50b Abs. 1 Z 1 normierte Ausnahme von der Meldepflicht fällt. Echtzeitüberwachung wird insbesondere dann ausreichen, wenn eine Videoüberwachung ausschließlich bezweckt, das überwachte Objekt (das auch eine Person sein kann) vor einer Gefahr rechtzeitig schützen zu können bzw. bei Eintreten eines schädigenden Ereignisses (z. B. eines Unfalls) unverzüglich reagieren zu können.

Nach dem Verhältnismäßigkeitsgrundsatz zu beurteilen wird auch die Zulässigkeit einer Gebäudeüberwachung sein, die mehrere Mieter und deren Besucher betrifft. Insbesondere können sich 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.

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. 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 das überwachte Objekt oder für eine Weitergabe nach § 50a Abs. 5 (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 regelmäßige längere Aufbewahrung ist nur mit Genehmigung der Datenschutzkommission erlaubt.

Zu § 50c:

§ 50c enthält einige Sonderbestimmungen für die Registrierung von Videoüberwachungen. Abs. 1 stellt allerdings zunächst (implizit) klar, dass § 17 – insbesondere die Möglichkeit der Definition von Standardanwendungen – auch für Videoüberwachungen gilt. Lediglich zwei Fälle werden von der Registrierungspflicht ausgenommen und zwar die bloße Echtzeitüberwachung nach § 50a Abs. 4 Z 4 (s. bereits dort zur 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.

Umgekehrt ist dieses Gefährdungspotential bei den übrigen Fällen der Videoüberwachung insbesondere im Hinblick auf den oft großen Betroffenenkreis und die Verwendung potentiell sensibler Daten gegenüber „herkömmlichen“ Datenanwendungen doch deutlich hinaufgesetzt. Dies erfordert ihre Prüfung im Vorabkontrollverfahren. Da bei Überwachungen nach § 50a Abs. 3 Z 5 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. Ein ähnliches Gefährdungspotential ist gegeben, wenn sich der Auftraggeber auf Z 7 beruft. Hier könnten etwa eine erhaltene Klage oder eine eigene Klagevorbereitung zur Glaubhaftmachung herangezogen werden.

Um die Gefahren der Videoüberwachung möglichst gering zu halten, wird in § 50c Abs. 3 die Anordnung einer Löschfrist durch die DSK zwingend vorgeschrieben und dafür eine Höchstgrenze von 48 Stunden vorgesehen, die nur in vom Auftraggeber darzulegenden Ausnahmefällen überschritten werden darf.

§ 50c Abs. 4 regelt den in der Praxis wohl häufig auftretenden Fall, dass ein Auftraggeber mehrere gleichartige oder räumlich verbundene 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. Sie darf nur dann entfallen wenn eine Abwägung zwischen der Wahrscheinlichkeit der Beeinträchtigung von Betroffeneninteressen oder der Beschaffenheit des überwachten Objekts auf der einen Seite und den Kosten der Überwachung auf der anderen Seite eine unverhältnismäßige Kostenbelastung ergeben würde. Hier sind bewegliche überwachte Objekte besonders hervorzuheben. Weiters darf die Kennzeichnung im Fall einer Überwachung nach § 50a Abs. 3 Z 7 entfallen, wenn dadurch der Zweck der Gewinnung von Beweismitteln beeinträchtigt würde. Die Rechtmäßigkeit des Entfalls der Kennzeichnung ist von der Datenschutzkommission im Registrierungsverfahren zu prüfen.

Zu § 50e:

§ 50e modifiziert schließlich das Auskunftsrecht für Videoüberwachungen. 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.

Zu Z 83 (§ 55):

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

Zu Z 87 (§ 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 Betrieb für weitere zwei Jahre möglich sein.

Zu Z 86 und 87 (§ 61 Abs. 8 bis 10):

Anlässlich des Inkrafttretens der Bestimmungen über den betrieblichen Datenschutzbeauftragten sowie die 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 gebracht werden. Dass sich dies bei bloßen Streichungen erübrigt, versteht sich von selbst.