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 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:

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

Zu Entlastungen kommt es durch Vereinfachungen der DVR-Meldungen für Informationsverbundsysteme.

- 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 Kosten in derzeit noch nicht zu beziffernder Höhe an.

- 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:

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 (§ 17 Abs. 1a, § 20 Abs. 1).

Durch die 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"), 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 10, 12, 67 und 88 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 10 und 13 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):

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).

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 9 und 17 (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 11 und 12 (§ 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 personenbezogene 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. Schließlich soll klargestellt werden, dass ein Eingriff in das Grundrecht nur dann ausgeschlossen ist, wenn personenbezogene Daten zulässigerweise allgemein verfügbar sind, was etwa bei öffentlichen Registern und Büchern der Fall ist (vgl. auch § 8 Abs. 2, wonach bei der Verwendung von zulässigerweise veröffentlichten Daten schutzwürdige Geheimhaltungsinteressen als nicht verletzt gelten). Dieser – bereits im DSG 2000 enthaltene – Satz wird nunmehr in Abs. 2, in dem auch die zulässigen Einschränkungen des Grundrechts normiert sind, verschoben.

Zu Art. 2 Z 14 bis 16 (§ 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 18 und 27 (§ 4) sowie zu Z 91 (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. Bloßes „Sehen“, 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. 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 19 (§ 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 20 (§ 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 21 (§ 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 22 und Z 26 (§ 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 23 und 24 (§ 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 25 (§ 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 28 (§ 8 Abs. 1):

Diese Änderung ist aufgrund der Neufassung des § 1 Abs. 1 notwendig. Dementsprechend wird auf die im einfachgesetzlichen Teil des DSG 2000 genannten „schutzwürdigen Geheimhaltungsinteressen“ abgestellt.

Zu Art. 2 Z 29 (§ 8 Abs. 2):

Ein Widerspruchsrecht gegen die Verwendung indirekt personenbezogener Daten wäre sinnwidrig und besteht nach § 29 auch derzeit nicht. Diese Rechtslage soll durch die vorgeschlagene Änderung auch in § 8 Abs. 2 nachvollzogen werden.

Zu Art. 2 Z 30 (§ 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 31 (§ 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 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. Eine nähere Ausgestaltung hat in der Verordnung nach § 16 Abs. 3 zu erfolgen.

Zu Art. 2 Z 37 (§ 17 Abs. 4):

Die gegenständliche Ausnahme von der Meldepflicht soll zu einer weiteren Entlastung des bei der Datenschutzkommission eingerichteten Datenverarbeitungsregisters dienen. Die Transparenz ist für den Rechtsunterworfenen dadurch gegeben, dass der Zweck der Datenverwendung, die betroffenen Personengruppen, Datenarten, Übermittlungen und Übermittlungsempfänger in einem Gesetz oder einer Verordnung abschließend geregelt sind. Damit bedarf es auch keiner Duplizierung solcher abschließend geregelten Fälle in der Standard- und Musterverordnung.

Zu Art. 2 Z 38 (§ 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.

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 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 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 drei 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, 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. 3), 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 vor allem der Vermeidung von Vermögensschäden der Betroffenen dienen.

Zu Art. 2 Z 42 und 43 (§ 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).

Zu Art. 2 Z 44 (§ 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 45 (§ 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. Für Betreiber von Informationsverbundsystemen gilt weiterhin § 50 Abs. 1.

Zu Art. 2 Z 46 (§ 27 Abs. 9):

Durch den Entfall der Einschränkung auf *öffentliche* Bücher und Register wird der zum vorgeschlagenen § 26 Abs. 8 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 Art. 2 Z 47 (§ 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 48 und 50 (§ 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 49 (§ 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 und missbräuchliches Abfangen von Daten) vorgenommen.

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

Zu Art. 2 Z 51 (§ 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 52 (§ 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 53 (§ 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 54 bis 56 (§ 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.

Zu Art. 2 Z 57 (§ 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 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 58 (§ 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 59 (§ 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 Erläuterungen zu § 3 Abs. 1 und 2 sowie § 12 Abs. 1. Internationale Zuständigkeitsregelungen nach § 3 werden dadurch nicht verändert.

Zu Art. 2 Z 60 (§ 34 Abs. 4):

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

Zu Art. 2 Z 61 (§ 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 62 (§ 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 63 (§ 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 64 (§ 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 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 65 (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 66 (§ 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 67 (§ 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 68 (§ 39 Abs. 5):

Durch diese Regelung wird lediglich die bisherige Praxis gesetzlich festgeschrieben.

Zu Art. 2 Z 69 (§ 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 70 (§ 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 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 Art. 2 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 Art. 2 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 Art. 2 Z 74 (§ 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 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 Art. 2 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 Art. 2 Z 77 (§ 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 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 Art. 2 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. 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 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 daduch 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 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 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 Überwachung von Babys), fallen diese nicht unter die Bestimmungen des § 50a.

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 der in dieser Bestimmung genannten Sorgfaltspflichten erfolgen.

§ 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 sind – ebenso wie § 8 Abs. 3 und ein Großteil des § 9 - das Ergebnis typisierender Interessenabwägungen nach § 1 Abs. 2 für den privaten Bereich (einschließlich Privatwirtschaftsverwaltung öffentlicher Auftraggeber). 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. 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). 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.

b) die überwachte Person einen überdurchschnittlichem Bekanntheitsgrad in der Öffentlichkeit oder das überwachte Objekt in Aufenthaltsort einer derartigen Person ist, oder
c) oder 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 Geheimhaltungsinteressen 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.

§ 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.

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 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 ist nur mit Genehmigung der Datenschutzkommission erlaubt. Dabei 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 – wie schon bisher – der Vorabkontrolle. 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 vergleichsweisen 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 Kennzeichungspflicht 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 (z. B. 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. Das Auskunftsrecht besteht naturgemäß nicht bei Echtzeitüberwachung, da hier keine Speicherung der Daten gegeben ist.

Zu Art. 2 Z 83 und 84 (§ 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 85 bis 88 (§ 52):

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.

Zu Art. 2 Z 89 (§ 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 90 (§ 55):

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

Zu Art. 2 Z 94 (§ 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 95 (§ 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 gebracht werden. Dass sich dies bei bloßen Streichungen erübrigt, versteht sich von selbst.

Zu Art. 2 Z 96 (§ 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.

Entwurf

Bundesgesetz, mit dem das Bundes-Verfassungsgesetz, das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010)

Der Nationalrat hat beschlossen:

Artikel 1

(Verfassungsbestimmung)

Änderung des Bundes-Verfassungsgesetzes

Das Bundes-Verfassungsgesetz, BGBl. Nr. 1/1930, zuletzt geändert durch das Bundesverfassungsgesetz BGBl. I Nr. 2/2008, wird wie folgt geändert:

1. In Art. 10 Abs. 1 Z 13 wird nach der Wortfolge „Volkszählungswesen sowie – unter Wahrung der Rechte der Länder, im eigenen Land jegliche Statistik zu betreiben – sonstige Statistik, soweit sie nicht nur den Interessen eines einzelnen Landes dient;“ *der Ausdruck* „Schutz personenbezogener Daten;“ *eingefügt.*

2. In Art. 102 Abs. 2 wird nach dem Wort „Denkmalschutz;“ *die Wortfolge* „Schutz personenbezogener Daten;“ *eingefügt.*

3. Dem Art. 151 wird folgender Abs. 41 angefügt:

„(41) Art. 10 Abs. 1 Z 13 und Art. 102 Abs. 2 in der Fassung des Bundesgesetzes BGBl. I Nr. xxx/2008 treten mit 1. Jänner 2010 in Kraft.“

Artikel 2

Änderung des Datenschutzgesetzes 2000

Das Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), BGBl. I Nr. 165/1999, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 13/2005, wird wie folgt geändert:

1. Im Inhaltsverzeichnis entfällt die Zeile

„§ 2 Zuständigkeit“

2. Im Inhaltsverzeichnis wird in der Überschrift zu § 4 nach dem Wort „Definitionen“ *die Wortfolge* „und Regelungsgegenstand“ *ergänzt.*

3. Im Inhaltsverzeichnis lautet § 20:

„§ 20 Prüfungs- und Verbesserungsverfahren“

4. Im Inhaltsverzeichnis lautet § 22:

„§ 22 Richtigstellung des Registers und Rechtsnachfolge“

5. Im Inhaltsverzeichnis wird nach § 22 eingefügt:

„§ 22a Verfahren zur Überprüfung der Erfüllung der Meldepflicht"

6. Im Inhaltsverzeichnis wird nach § 31 eingefügt:

„§ 31a Begleitende Maßnahmen im Beschwerdeverfahren"

7. Im Inhaltsverzeichnis wird nach § 50 eingefügt:

„9a. Abschnitt: Videoüberwachung

§ 50a Allgemeines

§ 50b Besondere Protokollierungs- und Löschungspflicht

§ 50c Meldepflicht und Registrierungsverfahren

§ 50d Information durch Kennzeichnung

§ 50e Auskunftsrecht"

8. Im Inhaltsverzeichnis entfällt die Zeile

„§ 58 Manuelle Dateien"

9. (Verfassungsbestimmung) Die Überschrift „Artikel 1 (Verfassungsbestimmung)" *entfällt.*

10. Vor § 1 wird folgende Abschnittsüberschrift eingefügt:

„1. Abschnitt

Allgemeines"

11. ***(Verfassungsbestimmung)*** *In § 1 wird nach der Paragraphenbezeichnung der Klammerausdruck „(Verfassungsbestimmung)" eingefügt; Abs. 1 lautet:*

„(1) Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten. "

12. In § 1 Abs. 2 wird dem bisherigen Text der folgende Satz vorangestellt:

„Der Anspruch besteht nicht, wenn Daten zulässigerweise allgemein verfügbar sind."

13. § 2 entfällt.

14. In *§ 3 Abs. 1 wird die Wortfolge* „Mitgliedstaaten der Europäischen Union" *durch die Wortfolge* „Vertragsstaaten des Europäischen Wirtschaftsraumes" *ersetzt.*

15. In § 3 Abs. 2 wird die Wortfolge „Mitgliedstaat der Europäischen Union" *durch die Wortfolge* „Vertragsstaat des Europäischen Wirtschaftsraumes" *ersetzt.*

16. § 3 Abs. 4 entfällt.

17. Die Überschrift „Artikel 2" *und die Abschnittsüberschrift* „1. Abschnitt Allgemeines" *vor § 4 entfallen.*

18. Der bisherige § 4 erhält die Überschrift „Definitionen und Regelungsgegenstand" und die Absatzbezeichnung „(1)"*. Weiters entfallen bei sämtlichen Ziffern des nunmehrigen § 4 Abs. 1 die An- und Ausführungszeichen um die definierten Begriffe, auch wenn diese in Klammern stehen.*

19. § 4 Abs. 1 Z 4 lautet:

„4. Auftraggeber: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen. Sie gelten auch dann als Auftraggeber, wenn der mit der Herstellung eines Werkes beauftragte Dienstleister (Z 5) die Entscheidung trifft, zu diesem Zweck Daten zu verwenden (Z 8), es sei denn dies wurde ihm ausdrücklich untersagt oder der Beauftragte hat auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden;"

20. § 4 Abs. 1 Z 5 lautet:

„5. Dienstleister: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden (Z 8);“

21. In § 4 Abs. 1 Z 7 entfällt der Klammerausdruck „(früher „Datenverarbeitung“)“.

22. § 4 Abs. 1 Z 8 lautet:

„8. Verwenden von Daten: jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten;“

23. § 4 Abs. 1 Z 9 lautet:

„9. Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns (Z 12) von Daten;“

24. § 4 Abs. 1 Z 10 entfällt.

25. § 4 Abs. 1 Z 11 lautet:

„11. Überlassen von Daten: die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses (Z 5);“

26. § 4 Abs. 1 Z 12 lautet:

„12. Übermitteln von Daten: die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;“

27. Folgender § 4 Abs. 2 wird nach dem nunmehrigen § 4 Abs. 1 angefügt:

„(2) Dieses Gesetz gilt für Daten, die in einer Datenanwendung oder manuellen Datei verwendet werden. Wo in den folgenden Bestimmungen von Datenanwendungen die Rede ist, gelten sie auch für manuelle Dateien. Für alle übrigen manuellen Daten gelten § 6 Abs. 1 Z 1 bis 3 und Abs. 2, §§ 7 bis 9 und die Bestimmungen des 6. Abschnitts sinngemäß.“

28. In § 8 Abs. 1 wird die Wortfolge „Gemäß § 1 Abs. 1 bestehende schutzwürdige Geheimhaltungsinteressen“ *durch die Wortfolge* „Schutzwürdige Geheimhaltungsinteressen im Sinn des § 7 Abs. 1 und Abs. 2 Z 3“ *ersetzt.*

29. In § 8 Abs. 2 zweiter Satz wird das Wort „solcher“ *durch die Wortfolge* „zulässigerweise veröffentlichter“ *ersetzt.*

30. In § 8 Abs. 4 wird der Punkt am Ende der Z 3 durch das Wort „oder“ *ersetzt und danach die folgende Z 4 eingefügt:*

„4. die Datenweitergabe zum Zweck der Erstattung einer Anzeige an eine zur Verfolgung der angezeigten strafbaren Handlungen (Unterlassungen) zuständige Behörde erfolgt.“

31. In § 12 Abs. 1 erster Satz wird die Wortfolge „Mitgliedstaaten der Europäischen Union“ *durch die Wortfolge* „Vertragsstaaten des Europäischen Wirtschaftsraumes“ *ersetzt.*

32. § 13 Abs. 3 entfällt.

33. § 16 Abs. 1 lautet:

„(1) Die Datenschutzkommission hat ein Register der Auftraggeber mit den von ihnen betriebenen Datenanwendungen zum Zweck der Information der Betroffenen zu führen.“

34. Der letzte Satz von § 16 Abs. 3 entfällt.

35. § 17 Abs. 1 lautet:

„(1) Jeder Auftraggeber hat, soweit in den Abs. 2 und 3 nicht anderes bestimmt ist, vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzkommission mit dem in § 19 festgelegten Inhalt zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten. Diese Meldepflicht gilt auch für Umstände, die nachträglich die Unrichtigkeit und Unvollständigkeit einer Meldung bewirken

(Änderungsmeldung). Für manuelle Dateien besteht eine Meldepflicht nur, soweit die Inhalte zumindest einen der Tatbestände des § 18 Abs. 2 Z 1 bis 4 erfüllen.“

36. Nach § 17 Abs. 1 wird der folgende Abs. 1a eingefügt:

„(1a) Die Meldung ist in elektronischer Form im Wege der vom Bundeskanzler bereit zu stellenden Internetanwendung einzubringen. Die Identifizierung und Authentifizierung kann insbesondere durch die Bürgerkarte (§ 2 Z 10 des E-Government-Gesetzes, BGBl. I Nr. 10/2004) erfolgen. Nähere Bestimmungen über die Identifizierung und Authentifizierung sind in die gemäß § 16 Abs. 3 zu erlassende Verordnung aufzunehmen. Eine Meldung in nicht-elektronischer Form ist für manuelle Dateien sowie bei einem längeren technischen Ausfall der Internetanwendung zulässig.“

37. Nach § 17 Abs. 3 wird der folgende Abs. 4 eingefügt:

„(4) Weiters sind Datenanwendungen von der Meldepflicht ausgenommen, für die der Zweck, die betroffenen Personengruppen, Datenarten, Übermittlungen und Übermittlungsempfänger in einem Gesetz oder in einer Verordnung abschließend geregelt sind.“

38. Nach § 19 Abs. 1 Z 3 wird folgende Z 3a eingefügt:

„3a. die Erklärung, ob die Datenanwendung einen oder mehrere der in § 18 Abs. 2 Z 1 bis 4 genannten Tatbestände erfüllt, und“

39. Die §§ 20 bis 22 samt Überschriften lauten:

„Prüfungs- und Verbesserungsverfahren

§ 20. (1) Meldungen von Datenanwendungen, die nach Angabe des Auftraggebers nicht einen der Tatbestände des § 18 Abs. 2 Z 1 bis 4 erfüllen, sind nur automationsunterstützt auf ihre Vollständigkeit und Plausibilität zu prüfen. Ist demnach die Meldung nicht fehlerhaft, so ist sie sofort zu registrieren.

(2) Wird bei der automationsunterstützten Prüfung ein Fehler der Meldung festgestellt, so ist dem Auftraggeber die Möglichkeit zur Verbesserung einzuräumen. Gleichzeitig ist er darauf hinzuweisen, dass die Meldung als nicht eingebracht gilt, wenn keine Verbesserung erfolgt oder er auf der Einbringung der unverbesserten Meldung besteht. Im letztgenannten Fall ist die Meldung von der Datenschutzkommission auf Mangelhaftigkeit im Sinn des § 19 Abs. 3 zu prüfen.

(3) Meldungen, die der Auftraggeber als vorabkontrollpflichtig bezeichnet hat oder von diesem zulässigerweise nicht im Wege der Internetanwendung (§ 17 Abs. 1a) eingebracht wurden, sind auf Mangelhaftigkeit im Sinn des § 19 Abs. 3 zu prüfen.

(4) Ergibt die Prüfung nach § 19 Abs. 3 eine Mangelhaftigkeit der Meldung, so ist dem Auftraggeber innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung unter Setzung einer Frist aufzutragen. Im Verbesserungsauftrag ist auf die Rechtsfolgen einer Nichtbefolgung nach Abs. 5 hinzuweisen.

(5) Wird dem Verbesserungsauftrag nicht entsprochen, ist die Registrierung der Meldung durch eine schriftliche Mitteilung abzulehnen. In die Mitteilung sind aufzunehmen:

1. die Punkte, in denen der Verbesserungsauftrag nicht erfüllt wurde und

2. der Hinweis, dass innerhalb von zwei Wochen ab Zustellung bei der Datenschutzkommission ein Antrag gestellt werden kann, über die Ablehnung mit Bescheid abzusprechen.

Nach Ablauf der von der Datenschutzkommission gesetzten Frist (Abs. 4) erstattete Verbesserungen sind nicht zu berücksichtigen.

Registrierung

§ 21. (1) Meldungen gemäß § 19 sind in das Datenverarbeitungsregister einzutragen, wenn

1. das Prüfungsverfahren nach § 20 Abs. 1 keinen Fehler ergeben hat oder
2. das Prüfungsverfahren nach § 20 Abs. 2 und 3 keine Mangelhaftigkeit der Meldung ergeben hat oder
3. nach Einlangen einer auf Mangelhaftigkeit zu prüfenden Meldung bei der Datenschutzkommission zwei Monate verstrichen sind, ohne dass ein Verbesserungsauftrag gemäß § 20 Abs. 4 erteilt wurde oder
4. der Auftraggeber die aufgetragenen Verbesserungen (§ 20 Abs. 4) vorgenommen hat.

Die in der Meldung enthaltenen Angaben über Datensicherheitsmaßnahmen sind im Register nicht ersichtlich zu machen.

(2) Bei Datenanwendungen, die gemäß § 18 der Vorabkontrolle unterliegen, können auf Grund der Ergebnisse des Prüfungsverfahrens dem Auftraggeber Auflagen, Bedingungen oder Befristungen für die Vornahme der Datenanwendung durch Bescheid erteilt werden, soweit dies zur Wahrung der durch dieses Bundesgesetz geschützten Interessen der Betroffenen notwendig ist.

(3) Der Auftraggeber ist von der Durchführung und vom Inhalt der Registrierung in geeigneter Weise zu verständigen.

(4) Jedem Auftraggeber ist bei der erstmaligen Registrierung eine Registernummer zuzuteilen.

(5) Hat die automationsunterstützte Prüfung nach § 20 Abs. 1 nicht zu einer Fehlermeldung geführt, so ist in die Registrierung ein Vermerk aufzunehmen, dass der Meldungsinhalt nur automationsunterstützt geprüft wurde.

Richtigstellung des Registers und Rechtsnachfolge

§ 22. (1) Streichungen aus dem Register und sonstige Änderungen des Registers sind auf Grund einer Änderungsmeldung des registrierten Auftraggebers oder von Amts wegen in den Fällen des Abs. 2, des § 22a Abs. 2 und des § 30 Abs. 6a vorzunehmen. Derartige Änderungen sind für die Dauer von drei Jahren ersichtlich zu machen.

(2) Gelangen der Datenschutzkommission aus amtlichen Verlautbarungen Änderungen in der Bezeichnung oder der Anschrift des Auftraggebers zur Kenntnis, so sind die Eintragungen von Amts wegen zu berichtigen. Ergibt sich aus einer amtlichen Verlautbarung der Wegfall der Rechtsgrundlage des Auftraggebers, ist dieser von Amts wegen aus dem Register zu streichen. Außerdem ist eine registrierte Datenanwendung zu streichen, wenn der Datenschutzkommission zur Kenntnis gelangt, dass eine registrierte Datenanwendung dauerhaft nicht mehr betrieben wird.

(3) Berichtigungen oder Streichungen nach Abs. 2 sind ohne weiteres Ermittlungsverfahren durch Mandatsbescheid (§ 38) zu verfügen.

(4) Der Rechtsnachfolger eines registrierten Auftraggebers kann einzelne oder alle registrierten Meldungen des Rechtsvorgängers übernehmen, wenn er innerhalb von zwei Monaten nach Wirksamkeit der Rechtsnachfolge eine entsprechend glaubhaft gemachte Erklärung gegenüber der Datenschutzkommission abgibt. Dem Rechtsnachfolger kann auf Antrag auch die Registernummer des Rechtsvorgängers übertragen werden, wenn der Rechtsvorgänger jegliche Verarbeitung personenbezogener Daten in Auftraggebereigenschaft eingestellt hat.“

40. Nach § 22 wird der folgende § 22a samt Überschrift eingefügt:

„Verfahren zur Überprüfung der Erfüllung der Meldepflicht

§ 22a. (1) Die Datenschutzkommission kann jederzeit die Erfüllung der Meldepflicht durch einen Auftraggeber prüfen. Dies gilt sowohl für die Mangelhaftigkeit einer registrierten Meldung im Sinn des § 19 Abs. 3 als auch für die rechtswidrige Unterlassung von Meldungen.

(2) Bei Vorliegen des Verdachtes der Nichterfüllung der Meldepflicht infolge Mangelhaftigkeit einer registrierten Meldung (Abs. 1) oder Unterlassung der Meldung, die über die Fälle des § 22 Abs. 2 hinausgeht, ist ein Verfahren zur Berichtigung des Datenverarbeitungsregisters durchzuführen. Das Verfahren wird durch begründete Verfahrensanordnung eingeleitet, die dem meldepflichtigen Auftraggeber mit einem Auftrag zur Verbesserung (§ 20 Abs. 4) oder einer Aufforderung zur Nachmeldung (§ 17 Abs. 1) innerhalb gesetzter Frist zuzustellen ist.

(3) Wird einem im Verfahren nach Abs. 2 erteilten Verbesserungsauftrag nicht entsprochen, so ist die Streichung der Meldung mit Bescheid der Datenschutzkommission zu verfügen. Die Streichung kann sich, wenn dies technisch möglich, im Hinblick auf den Zweck der Datenanwendung sinnvoll und zur Herstellung des rechtmäßigen Zustandes ausreichend ist, auch nur auf Teile der Meldung beschränken.

(4) Wird einer im Verfahren nach Abs. 2 erteilten Aufforderung zur Nachmeldung nicht entsprochen und die Unterlassung einer Meldung entgegen § 17 Abs. 1 erwiesen, so ist mit Bescheid der Datenschutzkommission der weitere Betrieb der Datenanwendung, soweit er vom Registerstand abweicht, zu untersagen und gleichzeitig Anzeige nach § 52 Abs. 2 Z 1 an die zuständige Behörde zu erstatten.

(5) Ergibt das Verfahren nach Abs. 2 alleine die Unangemessenheit oder die Nichteinhaltung von nach § 19 Abs. 1 Z 7 erklärten Datensicherheitsmaßnahmen, so ist dies mit Bescheid festzustellen und gleichzeitig eine angemessene Frist zur Herstellung ausreichender Datensicherheit zu setzen. Der Auftraggeber hat innerhalb dieser Frist der Datenschutzkommission die getroffenen Maßnahmen mitzuteilen. Sind diese nicht ausreichend, so ist die Streichung der Datenanwendung zu verfügen.

(6) Die Einleitung und der Stand eines Berichtigungsverfahrens nach Abs. 2 ist bei registrierten Meldungen im Datenverarbeitungsregister bis zur Einstellung oder bis zur Herstellung eines rechtmäßigen Zustandes durch Maßnahmen nach den Abs. 3 bis 6 geeignet anzumerken."

41. Nach § 24 Abs. 2 wird folgender Abs. 2a eingefügt:

„(2a) Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden, hat er darüber unverzüglich die Betroffenen zu informieren."

42. § 26 Abs. 1 lautet:

„(1) Ein Auftraggeber hat jeder Person oder Personengemeinschaft, die dies schriftlich verlangt und ihre Identität in geeigneter Form nachweist, Auskunft über die zu dieser Person oder Personengemeinschaft verarbeiteten Daten zu geben. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt werden. Die Auskunft hat die verarbeiteten Daten, die Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hiefür in allgemein verständlicher Form anzuführen. Auf Verlangen eines Betroffenen sind auch Namen und Adressen von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Wenn zur Person des Auskunftswerbers keine Daten vorhanden sind, genügt die Bekanntgabe dieses Umstandes (Negativauskunft). Mit Zustimmung des Auskunftswerbers kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden."

43. In § 26 Abs. 2 bis 7 wird jeweils das Wort „Betroffener", *gleich in welcher grammatikalischen Form, durch das Wort* „Auskunftswerber" *in der richtigen grammatikalischen Form ersetzt.*

44. § 26 Abs. 8 lautet:

„(8) In dem Umfang, in dem eine Datenanwendung für eine Person oder Personengemeinschaft hinsichtlich der zu ihr verarbeiteten Daten von Gesetzes wegen einsehbar ist, hat diese das Recht auf Auskunft nach Maßgabe der das Einsichtsrecht vorsehenden Bestimmungen. Für das Verfahren der Einsichtnahme (einschließlich deren Verweigerung) gelten die näheren Regelungen des Gesetzes, das das Einsichtsrecht vorsieht. In Abs. 1 genannte Bestandteile einer Auskunft, die vom Einsichtsrecht nicht umfasst sind, können dennoch nach diesem Bundesgesetz geltend gemacht werden."

45. § 26 Abs. 10 lautet:

„(10) Ergibt sich eine Auftraggeberstellung auf Grund von Rechtsvorschriften, obwohl die Datenverarbeitung für Zwecke der Auftragserfüllung für einen Dritten erfolgt (§ 4 Z 4 letzter Satz), kann der Auskunftswerber sein Auskunftsbegehren zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Dieser hat dem Auskunftswerber, soweit ihm dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse des tatsächlichen Auftraggebers mitzuteilen, damit der Auskunftswerber sein Auskunftsrecht gemäß Abs. 1 gegen diesen geltend machen kann. Das gilt auch für einen Dienstleister, wenn ein an ihn gerichtetes Auskunftsbegehren erkennen lässt, dass der Auskunftswerber ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält. Stattdessen kann er auch innerhalb derselben Frist das Auskunftsbegehren an den Auftraggeber weiterleiten und den Auskunftswerber davon verständigen. Für Betreiber von Informationsverbundsystemen gilt jedoch ausschließlich § 50 Abs. 1."

46. In § 27 Abs. 9 entfällt das Wort „öffentliche".

47. Nach § 28 Abs. 2 wird der folgende Abs. 3 angefügt:

„(3) § 27 Abs. 4 bis 6 gelten auch in den Fällen der Abs. 1 und 2."

48. Nach § 30 Abs. 2 wird der folgende Abs. 2a eingefügt:

„(2a) Sofern sich eine zulässige Eingabe nach Abs. 1 oder Abs. 1a oder ein begründeter Verdacht nach Abs. 2 auf eine meldepflichtige Datenanwendung (Datei) bezieht, hat die Datenschutzkommission die Erfüllung der Meldepflicht zu überprüfen und erforderlichenfalls nach den §§ 22 und 22a vorzugehen."

49. § 30 Abs. 5 lautet:

„(5) Informationen, die der Datenschutzkommission oder ihren Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Dazu zählt auch die Verwendung für Zwecke der gerichtlichen Rechtsverfolgung durch den Einschreiter oder die Datenschutzkommission nach § 32. Im Übrigen besteht die Pflicht zur Verschwiegenheit auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, dass dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach den §§ 51 oder 52 dieses Bundesgesetzes, einer strafbaren Handlung nach den §§ 118a, 119 und 119a oder eines Verbrechens nach § 278a des Strafgesetzbuches, BGBl. Nr. 60/1974 (kriminelle Organisation), oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch Ersuchen nach § 76 der Strafprozessordnung, BGBl. Nr. 631/1975, zu entsprechen ist.“

50. § 30 Abs. 6 lautet:

„(6) Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzkommission, sofern nicht Maßnahmen nach den §§ 22 und 22a oder nach Abs. 6a zu treffen sind, Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzkommission je nach der Art des Verstoßes von Amts wegen insbesondere

1. Strafanzeige nach §§ 51 oder 52 erstatten, oder
2. bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 32 Abs. 5 erheben, oder
3. bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, dass der Empfehlung der Datenschutzkommission entsprochen wird, oder der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung darf von der Datenschutzkommission der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht.“

51. Nach § 30 Abs. 6 wird der folgende Abs. 6a eingefügt:

„(6a) Liegt durch den Betrieb einer Datenanwendung eine wesentliche Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen (Gefahr im Verzug) vor, so kann die Datenschutzkommission die Weiterführung der Datenanwendung mit Bescheid gemäß § 57 Abs. 1 AVG untersagen. Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenanwendung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Wird einer Untersagung nicht sogleich Folge geleistet, ist Strafanzeige nach § 52 Abs. 1 Z 3 zu erstatten. Nach Rechtskraft einer Untersagung nach diesem Absatz ist ein Berichtigungsverfahren nach § 22a Abs. 2 formlos einzustellen. Die Datenanwendung ist im Umfang der Untersagung aus dem Register zu streichen.“

52. § 31 samt Überschrift lautet:

„Beschwerde an die Datenschutzkommission

§ 31. (1) Die Datenschutzkommission erkennt über Beschwerden von Personen, die behaupten, in ihrem Recht auf Auskunft nach § 26 oder nach § 50 Abs. 1 dritter Satz oder in ihrem Recht auf Darlegung einer automatisierten Einzelentscheidung nach § 49 Abs. 3 verletzt zu sein, soweit sich das Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) nicht auf die Verwendung von Daten für Akte im Dienste der Gesetzgebung oder der Gerichtsbarkeit bezieht.

(2) Die Datenschutzkommission erkennt weiters über Beschwerden von Personen, die behaupten, in ihrem Recht auf Geheimhaltung (§ 1 Abs. 1) oder in ihrem Recht auf Richtigstellung oder auf Löschung (§§ 27 und 28) verletzt zu sein, sofern der Anspruch nicht nach § 32 Abs. 1 vor einem Gericht geltend zu machen ist oder sich gegen ein Organ im Dienste der Gesetzgebung oder der Gerichtsbarkeit richtet.

(3) Die Beschwerde hat zu enthalten:

1. die Bezeichnung des als verletzt erachteten Rechts,
2. soweit dies zumutbar ist, die Bezeichnung des Rechtsträgers oder Organs, dem die behauptete Rechtsverletzung zugerechnet wird (Beschwerdegegner),
3. den Sachverhalt, aus dem die Rechtsverletzung abgeleitet wird,
4. die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt,

5. das Begehren, die behauptete Rechtsverletzung festzustellen und
6. die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist.

(4) Einer Beschwerde nach Abs. 1 sind außerdem das zu Grunde liegende Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) und eine allfällige Antwort des Beschwerdegegners anzuschließen. Einer Beschwerde nach Abs. 2 sind außerdem der zu Grunde liegende Antrag auf Richtigstellung oder Löschung und eine allfällige Antwort des Beschwerdegegners anzuschließen.

(5) Die der Datenschutzkommission durch § 30 Abs. 2 bis 4 eingeräumten Kontrollbefugnisse kommen ihr auch in Beschwerdeverfahren nach Abs. 1 und 2 gegenüber dem Beschwerdegegner zu. Ebenso besteht auch hinsichtlich dieser Verfahren die Verschwiegenheitspflicht nach § 30 Abs. 5.

(6) Im Fall der Einbringung einer zulässigen Beschwerde nach Abs. 1 oder 2 ist ein auf Grund einer Eingabe nach § 30 Abs. 1 über denselben Gegenstand eingeleitetes Kontrollverfahren durch eine entsprechende Information (§ 30 Abs. 7) zu beenden. Die Datenschutzkommission kann aber dennoch auch während der Anhängigkeit des Beschwerdeverfahrens von Amts wegen nach § 30 Abs. 2 vorgehen, wenn ein begründeter Verdacht einer über den Beschwerdefall hinausgehenden Verletzung datenschutzrechtlicher Verpflichtungen besteht. § 30 Abs. 3 bleibt unberührt.

(7) Soweit sich eine Beschwerde nach Abs. 1 oder 2 als berechtigt erweist, ist ihr Folge zu geben und die Rechtsverletzung festzustellen. Ist eine festgestellte Verletzung im Recht auf Auskunft (Abs. 1) einem Auftraggeber des privaten Bereichs zuzurechnen, so ist diesem auf Antrag zusätzlich die – allenfalls erneute – Reaktion auf das Auskunftsbegehren nach § 26 Abs. 4, 5 oder 10 in jenem Umfang aufzutragen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen. Soweit sich die Beschwerde als nicht berechtigt erweist, ist sie abzuweisen.

(8) Ein Beschwerdegegner, gegen den wegen Verletzung in Rechten nach den §§ 26 bis 28 Beschwerde erhoben wurde, kann bis zum Abschluss des Verfahrens vor der Datenschutzkommission durch Reaktionen gegenüber dem Beschwerdeführer gemäß § 26 Abs. 4 oder § 27 Abs. 4 die behauptete Rechtsverletzung nachträglich beseitigen. Erscheint der Datenschutzkommission durch derartige Reaktionen des Beschwerdegegners die Beschwerde als gegenstandslos, so hat sie den Beschwerdeführer dazu zu hören. Gleichzeitig ist er darauf aufmerksam zu machen, dass die Datenschutzkommission das Verfahren formlos einstellen wird, wenn er nicht innerhalb einer angemessenen Frist begründet, warum er die ursprünglich behauptete Rechtsverletzung zumindest teilweise nach wie vor als nicht beseitigt erachtet. Wird durch eine derartige Äußerung des Beschwerdeführers die Sache ihrem Wesen nach geändert (§ 13 Abs. 8 AVG), so ist von der Zurückziehung der ursprünglichen Beschwerde und der gleichzeitigen Einbringung einer neuen Beschwerde auszugehen. Auch diesfalls ist das ursprüngliche Beschwerdeverfahren formlos einzustellen und der Beschwerdeführer davon zu verständigen. Verspätete Äußerungen sind nicht zu berücksichtigen.“

53. Nach § 31 wird der folgende § 31a samt Überschrift eingefügt:

„Begleitende Maßnahmen im Beschwerdeverfahren

§ 31a. (1) Sofern sich eine zulässige Beschwerde nach § 31 Abs. 2 auf eine meldepflichtige Datenanwendung (Datei) bezieht, hat die Datenschutzkommission die Erfüllung der Meldepflicht zu überprüfen und erforderlichenfalls nach den §§ 22 und 22a vorzugehen.

(2) Bescheinigt der Beschwerdeführer im Rahmen einer Beschwerde nach § 31 Abs. 2 eine wesentliche Beeinträchtigung seiner schutzwürdigen Geheimhaltungsinteressen durch die Verwendung seiner Daten, so kann die Datenschutzkommission nach § 30 Abs. 6a vorgehen.

(3) Ist in einem Verfahren nach § 31 Abs. 2 die Richtigkeit von Daten strittig, so ist vom Beschwerdegegner bis zum Abschluss des Verfahrens ein Bestreitungsvermerk anzubringen. Erforderlichenfalls hat dies die Datenschutzkommission auf Antrag des Beschwerdeführers mit Mandatsbescheid anzuordnen.

(4) Beruft sich ein Auftraggeber des öffentlichen Bereichs bei einer Beschwerde wegen Verletzung des Auskunfts-, Richtigstellungs- oder Löschungsrechts gegenüber der Datenschutzkommission auf die §§ 26 Abs. 5 oder 27 Abs. 5, so hat diese nach Überprüfung der Notwendigkeit der Geheimhaltung die geschützten öffentlichen Interessen in ihrem Verfahren zu wahren. Kommt sie zur Auffassung, dass die Geheimhaltung von verarbeiteten Daten gegenüber dem Betroffenen nicht gerechtfertigt war, ist die Offenlegung der Daten mit Bescheid aufzutragen. Gegen diese Entscheidung der Datenschutzkommission kann die belangte Behörde Beschwerde an den Verwaltungsgerichtshof erheben. Wurde keine derartige Beschwerde eingebracht und wird dem Bescheid der Datenschutzkommission binnen acht Wochen nicht entsprochen, so hat die Datenschutzkommission die Offenlegung der Daten gegenüber dem Betroffenen

selbst vorzunehmen und ihm die verlangte Auskunft zu erteilen oder ihm mitzuteilen, welche Daten bereits berichtigt oder gelöscht wurden. Die ersten beiden Sätze gelten in Verfahren nach § 30 sinngemäß."

54. § 32 Abs. 1 lautet:

„(1) Ansprüche wegen Verletzung der Rechte einer Person auf Geheimhaltung, auf Richtigstellung oder auf Löschung gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, sind auf dem Zivilrechtsweg geltend zu machen, soweit diese Rechtsträger bei der behaupteten Verletzung nicht in Vollziehung der Gesetze tätig geworden sind."

55. § 32 Abs. 4 lautet:

„(4) Für Klagen und Anträge auf Erlassung einer einstweiligen Verfügung nach diesem Bundesgesetz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Kläger (Antragsteller) seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen (Anträge) können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz oder eine Niederlassung hat."

56. § 32 Abs. 6 lautet:

„(6) Die Datenschutzkommission hat, wenn ein Einschreiter (§ 30 Abs. 1) es verlangt und es zur Wahrung der nach diesem Bundesgesetz geschützten Interessen einer größeren Zahl von natürlichen Personen geboten ist, einem Rechtsstreit auf Seiten des Einschreiters als Nebenintervenient (§§ 17 ff ZPO) beizutreten."

57. Nach § 32 Abs. 6 wird folgender Abs. 7 angefügt:

„(7) Anlässlich einer zulässigen Klage nach Abs. 1, die sich auf eine nach Ansicht des Gerichts meldepflichtige Datenanwendung bezieht, hat das Gericht die Datenschutzkommission um Überprüfung nach den §§ 22 und 22a zu ersuchen. Die Datenschutzkommission hat das Gericht vom Ergebnis der Überprüfung zu verständigen. Dieses ist sodann vom Gericht auch den Parteien bekannt zu geben, sofern das Verfahren noch nicht rechtskräftig beendet ist."

58. In § 34 Abs. 1 wird das Wort „abzuweisen" *durch das Wort* „zurückzuweisen" *ersetzt.*

59. § 34 Abs. 3 lautet:

„(3) Ist ein von der Datenschutzkommission zu prüfender Sachverhalt gemäß § 3 nach der Rechtsordnung eines anderen Vertragsstaates des Europäischen Wirtschaftsraumes zu beurteilen, so kann die Datenschutzkommission die zuständige ausländische Datenschutzkontrollstelle um Unterstützung ersuchen."

60. In § 34 Abs. 4 wird die Wortfolge „Mitgliedstaaten der Europäischen Union" *durch* „Vertragsstaaten des Europäischen Wirtschaftsraumes" *ersetzt.*

61. In § 36 Abs. 3 wird das Wort „Bundesbeamten" *durch das Wort* „Bundesbediensteten" *ersetzt.*

62. Nach § 36 Abs. 3 wird der folgende Abs. 3a eingefügt:

„(3a) Die Mitglieder der Datenschutzkommission üben diese Funktion neben ihnen sonst obliegenden beruflichen Tätigkeiten aus."

63. § 36 Abs. 6 werden die folgenden Sätze angefügt:

„Die Mitgliedschaft des richterlichen Mitglieds sowie des Mitglieds aus dem Kreis der rechtskundigen Bundesbediensteten endet auch, wenn diese aus ihren Dienstverhältnissen zum Bund ausscheiden, in den Ruhestand übertreten oder in den Ruhestand versetzt werden. Bei Richtern steht dem Ausscheiden eine Dienstzuteilung nach § 78 des Richter- und Staatsanwaltschaftsdienstgesetzes, BGBl. Nr. 305/1961, gleich. Die Mitgliedschaft der übrigen Mitglieder endet am 31. Dezember des Jahres, in dem sie das 65. Lebensjahr vollenden."

64. § 36 Abs. 9 lautet:

„(9) Die Mitglieder und Ersatzmitglieder der Datenschutzkommission haben für die Anreise zu den Sitzungen der Datenschutzkommission sowie für in Ausübung ihrer Funktion erforderliche sonstige Dienstreisen Anspruch auf Ersatz der Reisekosten (Gebührenstufe 3) durch den Bundeskanzler nach Maßgabe der für Bundesbedienstete geltenden Rechtsvorschriften. Sie haben ferner Anspruch auf eine der

Zeit und dem Arbeitsaufwand entsprechende Vergütung, die auf Antrag des Bundeskanzlers von der Bundesregierung durch Verordnung festzusetzen ist."

*65. **(Verfassungsbestimmung)** In § 38 Abs. 1 entfällt der Klammerausdruck „(Verfassungsbestimmung)".*

66. § 38 Abs. 1 lautet:

„(1) Die Datenschutzkommission hat sich eine Geschäftsordnung zu geben, in der eines ihrer Mitglieder mit der Führung der laufenden Geschäfte zu betrauen ist (geschäftsführendes Mitglied). Diese Betrauung umfasst auch die Erlassung von verfahrensrechtlichen Bescheiden und von Mandatsbescheiden. Inwieweit einzelne fachlich geeignete Bedienstete der Geschäftsstelle der Datenschutzkommission zum Handeln für die Datenschutzkommission oder das geschäftsführende Mitglied ermächtigt werden, bestimmt ebenfalls die Geschäftsordnung. Diese ist im Internet kundzumachen."

67. § 38 Abs. 2 wird der folgende Satz angefügt:

„Er hat das Recht, sich jederzeit über alle Gegenstände der Geschäftsführung der Datenschutzkommission beim Vorsitzenden und dem geschäftsführenden Mitglied zu unterrichten."

68. § 39 wird der folgende Abs. 5 angefügt:

„(5) Beschlüsse der Datenschutzkommission werden vom Vorsitzenden ausgefertigt."

69. § 40 Abs. 1 und 2 lauten:

„(1) Gegen Bescheide, die das geschäftsführende Mitglied der Datenschutzkommission gemäß § 22 Abs. 3, § 30 Abs. 6a oder § 31a Abs. 3 in Verbindung mit § 38 Abs. 1 erlassen hat, ist die Vorstellung an die Datenschutzkommission gemäß § 57 Abs. 2 AVG zulässig. Eine Vorstellung gegen einen gemäß § 22 Abs. 3 ergangenen Bescheid hat aufschiebende Wirkung.

(2) Gegen Bescheide der Datenschutzkommission ist kein Rechtsmittel zulässig. Sie unterliegen nicht der Aufhebung oder Abänderung im Verwaltungsweg. Auftraggeber des öffentlichen Bereichs haben in Verfahren vor der Datenschutzkommission stets Parteistellung. Die Anrufung des Verwaltungsgerichtshofes durch die Parteien des Verfahrens ist zulässig. Dies gilt jedoch nicht für Auftraggeber des öffentlichen Bereichs als Beschwerdegegner im Verfahren nach § 31, es sei denn es ist durch besondere gesetzliche Regelung die Möglichkeit einer Amtsbeschwerde (Art. 131 Abs. 2 B-VG) vorgesehen."

70. Nach § 41 Abs. 2 Z 4 wird folgende Z 4a eingefügt:

„4a. hat der Datenschutzrat das Recht, von der Datenschutzkommission, Auskünfte und Berichte sowie Einsicht in Unterlagen zu verlangen;"

71. § 42 Abs. 1 Z 1 lautet:

„1. Vertreter der politischen Parteien: Von der im Hauptausschuss des Nationalrates am stärksten vertretenen Partei sind vier Vertreter, von der am zweitstärksten vertretenen Partei sind drei Vertreter und von jeder anderen im Hauptausschuss des Nationalrates vertretenen Partei ist ein Vertreter in den Datenschutzrat zu entsenden, wobei es allein auf die Stärke im Zeitpunkt der Entsendung ankommt. Bei Mandatsgleichheit zweier Parteien im Hauptausschuss ist die Stimmenstärke bei der letzten Wahl zum Nationalrat ausschlaggebend;"

72. § 42 Abs. 5 wird der folgende Satz angefügt:

„Mitglieder nach Abs. 1 Z 1 scheiden außerdem aus, sobald der Hauptausschuss nach den §§ 29 und 30 des Geschäftsordnungsgesetzes 1975, BGBl. Nr. 410, neu gewählt wurde, und sie nicht neuerlich entsendet werden."

73. In § 46 Abs. 1 Z 2 werden die Worte „der Auftraggeber" *durch das Wort* „er" *ersetzt. In § 46 Abs. 1 Z 3 werden die Worte* „den Auftraggeber" *durch das Wort* „ihn" *ersetzt.*

74. In § 46 Abs. 2 entfällt die Wortfolge „, die nicht öffentlich zugänglich sind,".

75. In § 46 Abs. 3 wird vor den Worten „zu erteilen" *die Wortfolge* „auf Antrag des Auftraggebers der Untersuchung" *eingefügt. Das Wort* „übermittelt" *wird durch das Wort* „ermittelt" und das Wort „Empfänger" durch die Wortfolge „Auftraggeber der Untersuchung" *ersetzt.*

76. Nach § 46 Abs. 3 wird der folgende Abs. 3a angefügt:

„(3a) Einem Antrag nach Abs. 3 ist jedenfalls eine vom Eigentümer der Datenbestände, aus denen die Daten ermittelt werden sollen, oder einem sonst darüber Verfügungsbefugten unterfertigte Erklärung anzuschließen, dass er dem Auftraggeber die Datenbestände für die Untersuchung zur Verfügung stellt. Anstelle dieser Erklärung kann auch ein diese Erklärung ersetzender Exekutionstitel (§ 367 Abs. 1 der Exekutionsordnung – EO, RGBl. Nr. 79/1896) vorgelegt werden."

77. In § 47 Abs. 4 wird nach der Wortfolge „Die Datenschutzkommission hat" *die Wortfolge* „auf Antrag eines Auftraggebers, der Adressdaten verarbeitet," *eingefügt.*

78. § 49 Abs. 3 wird der folgende Satz angefügt:

„§ 26 Abs. 2 bis 10 gilt sinngemäß."

79. Nach § 50 Abs. 1 dritter Satz wird der folgende Satz eingefügt:

„Abgesehen von der abweichenden Frist gilt § 26 Abs. 3 bis 10 sinngemäß."

80. § 50 Abs. 2 lautet:

„(2) Durch entsprechenden Rechtsakt können auch weitere Auftraggeberpflichten, insbesondere auch die Vornahme der Meldung des Informationsverbundsystems, auf den Betreiber übertragen werden. Allein für die Übertragung der Meldepflicht ist die Vorlage von Vollmachten nach § 10 des Allgemeinen Verwaltungsverfahrensgesetzes 1991, BGBl. Nr. 51, nicht erforderlich. Soweit der Pflichtenübergang nicht durch Gesetz angeordnet ist, ist er gegenüber Dritten nur wirksam, wenn er – auf Grund einer entsprechenden Meldung an die Datenschutzkommission – aus der Registrierung im Datenverarbeitungsregister ersichtlich ist."

81. Nach § 50 Abs. 2 wird der folgende Abs. 2a eingefügt:

„(2a) Wird ein Informationsverbundsystem auf Grund einer Meldung von zumindest zwei Auftraggebern registriert, so können Auftraggeber, die in der Folge die Teilnahme an dem Informationsverbundsystem anstreben, die Meldung im Umfang des § 19 Z 3 bis 8 auf einen Verweis auf den Inhalt der Meldung eines bereits registrierten Auftraggebers beschränken, wenn sie eine Teilnahme im genau gleichen Umfang anstreben. Soweit sich ein solcher weiterer Auftraggeber anlässlich der Meldung ausdrücklich den Auflagen unterwirft, die die Datenschutzkommission anlässlich der Meldung, auf die er verweist, ausgesprochen hat, werden diese für ihn mit der Registrierung in gleicher Weise und mit gleicher Wirkung (§ 52 Abs. 1 Z 3) verbindlich und ist die Erlassung eines gesonderten Auflagenbescheides durch die Datenschutzkommission nicht erforderlich."

82. Nach § 50 wird der folgende 9a. Abschnitt eingefügt:

„9a. Abschnitt
Videoüberwachung

Allgemeines

§ 50a. (1) Videoüberwachung bezeichnet die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt („überwachtes Objekt") oder eine bestimmte Person („überwachte Person") betreffen, durch technische Bildaufnahme- oder Bildübertragungsgeräte. Für derartige Überwachungen gelten die folgenden Absätze, sofern nicht durch andere Gesetze Besonderes bestimmt ist. § 45 bleibt unberührt.

(2) Für Videoüberwachung gelten die §§ 6 und 7, insbesondere der Verhältnismäßigkeitsgrundsatz (§ 7 Abs. 3). Rechtmäßige Zwecke einer Videoüberwachung, insbesondere der Auswertung und Übermittlung der dabei ermittelten Daten, sind jedoch vorbehaltlich des Abs. 5 nur der Schutz des überwachten Objekts oder der überwachten Person oder die Erfüllung gesetzlicher oder vergleichbarer rechtlicher Sorgfaltspflichten, jeweils einschließlich der Beweissicherung, im Hinblick auf Ereignisse nach Abs. 1.

(3) Ein Betroffener ist durch eine Videoüberwachung dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen (§ 7 Abs. 2 Z 3) verletzt, wenn

1. diese im lebenswichtigen Interesse einer Person erfolgt, oder
2. Daten über ein Verhalten verarbeitet werden, das ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden, oder
3. er der Verwendung seiner Daten im Rahmen der Überwachung ausdrücklich zugestimmt hat.

(4) Ein Betroffener ist darüber hinaus durch eine Videoüberwachung ausschließlich dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen (§ 7 Abs. 2 Z 3) verletzt, wenn sie nicht im Rahmen der Vollziehung hoheitlicher Aufgaben erfolgt und

1. bestimmteTatsachen die Annahme rechtfertigen, das überwachte Objekt oder die überwachte Person könnte das Ziel oder der Ort eines gefährlichen Angriffs werden, oder
2. unmittelbar anwendbare Rechtsvorschriften des Völker- oder des Gemeinschaftsrechts, Gesetze, Verordnungen, Bescheide oder gerichtliche Entscheidungen dem Auftraggeber spezielle Sorgfaltspflichten zum Schutz des überwachten Objekts oder der überwachten Person auferlegen, oder
3. sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte Objekt/die überwachte Person betreffenden Ereignisse erschöpft, diese also weder gespeichert (aufgezeichnet) noch in sonst einer anderen Form weiterverarbeitet werden (Echtzeitüberwachung), und sie zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt.

(5) Mit einer Videoüberwachung nach Abs. 4 dürfen nicht Ereignisse an Orten festgestellt werden, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen. Weiters ist die Videoüberwachung zum Zweck der Mitarbeiterkontrolle an Arbeitsstätten untersagt.

(6) Schutzwürdige Geheimhaltungsinteressen Betroffener sind auch dann nicht verletzt, wenn durch Videoüberwachung aufgezeichnete Daten über eine Verwendung entsprechend den Abs. 2 bis 4 hinaus in folgenden Fällen übermittelt werden:

1. an die zuständige Behörde oder das zuständige Gericht, weil beim Auftraggeber der begründete Verdacht entstanden ist, die Daten könnten eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren, oder
2. an Sicherheitsbehörden zur Ausübung der diesen durch § 53 Abs. 5 des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991, eingeräumten Befugnisse,

auch wenn sich die Handlung oder der Angriff nicht gegen das überwachte Objekt richtet. Die Befugnisse von Behörden und Gerichten zur Durchsetzung der Herausgabe von Beweismaterial und zur Beweismittelsicherung sowie damit korrespondierende Verpflichtungen des Auftraggebers bleiben unberührt.

(7) Mit einer Videoüberwachung gewonnene Daten von Betroffenen dürfen nicht automationsunterstützt mit anderen Bilddaten abgeglichen und nicht nach sensiblen Daten als Auswahlkriterium durchsucht werden.

Besondere Protokollierungs- und Löschungspflicht

§ 50b. (1) Jeder Verwendungsvorgang einer Videoüberwachung ist zu protokollieren. Dies gilt nicht für Fälle der Echtzeitüberwachung.

(2) Aufgezeichnete Daten sind, sofern sie nicht aus konkretem Anlass für die Verwirklichung der zu Grunde liegenden Schutz- oder Beweissicherungszwecke oder für Zwecke nach § 50a Abs. 6 benötigt werden, spätestens nach 48 Stunden zu löschen. Die Datenschutzkommission kann eine längere Aufbewahrungsdauer festsetzen, wenn dies aus besonderen Gründen zur Zweckerreichung regelmäßig erforderlich ist. Ein Antrag auf Festsetzung einer längeren Aufbewahrungsdauer ist bei meldepflichtigen Videoüberwachungen tunlichst mit der Meldung zu verbinden.

Meldepflicht und Registrierungsverfahren

§ 50c. (1) Videoüberwachungen unterliegen der Vorabkontrolle (§ 18 Abs. 2). Bestimmte Tatsachen im Sinn von § 50a Abs. 4 Z 1 müssen bei Erstattung der Meldung glaubhaft gemacht werden. Soweit gemäß § 96a des Arbeitsverfassungsgesetzes 1974, BGBl. Nr. 22, Betriebsvereinbarungen abzuschließen sind, sind diese im Registrierungsverfahren vorzulegen.

(2) Eine Videoüberwachung ist über § 17 Abs. 2 bis 4 hinaus von der Meldepflicht ausgenommen

1. in Fällen der Echtzeitüberwachung oder
2. wenn eine Speicherung (Aufzeichnung) nur auf einem analogen Speichermedium erfolgt.

(3) Mehrere überwachte Objekte oder überwachte Personen, für deren Videoüberwachung derselbe Auftraggeber eine gesetzliche Zuständigkeit oder rechtliche Befugnis (§ 7 Abs. 1) hat, können auf Grund ihrer gleichartigen Beschaffenheit oder ihrer räumlichen Verbundenheit in einer Meldung zusammengefasst werden, wenn sich diese auf die gleiche Rechtsgrundlage stützt.

Information durch Kennzeichnung

§ 50d. (1) Der Auftraggeber einer Videoüberwachung hat diese geeignet zu kennzeichnen. Aus der Kennzeichnung hat jedenfalls der Auftraggeber eindeutig hervorzugehen, es sei denn dieser ist den Betroffenen nach den Umständen des Falles bereits bekannt. Die Kennzeichnung hat örtlich derart zu erfolgen, dass jeder potentiell Betroffene, der sich einem überwachten Objekt oder einer überwachten Person nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen.

(2) Keine Kennzeichnungsverpflichtung besteht bei Videoüberwachungen, die nach § 17 Abs. 2 Z 4 nicht meldepflichtig sind. Dies gilt auch für Videoüberwachungen im Rahmen der Vollziehung hoheitlicher Aufgaben, die nach § 17 Abs. 3 von der Meldepflicht ausgenommen sind.

Auskunftsrecht

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

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

(3) In Fällen der Echtzeitüberwachung ist ein Auskunftsrecht ausgeschlossen."

83. In § 51 Abs. 1 entfällt die Absatzbezeichnung „(1)". *Die Wortfolge* „in der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen" *wird durch die Wortfolge* „mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen," *ersetzt.*

84. § 51 Abs. 2 entfällt.

85. § 52 Abs. 1 wird die Zahl „18 890"durch „25 000" ersetzt.

86. In § 52 Abs. 2 wird die Zahl „9 445" *durch* „10 000" *ersetzt.*

87. § 52 Abs. 2 Z 1 lautet:

„1. verarbeitet oder übermittelt, ohne seine Meldepflicht gemäß den §§ 17 oder 50c erfüllt zu haben oder"

88. § 52 Abs. 2 Z 3 lautet:

„Seine Offenlegungs- oder Informationspflichten gemäß den §§ 23, 24, 25 oder 50d verletzt oder"

89. § 52 Abs. 4 lautet:

„(4) Die Strafe des Verfalls von Datenträgern und Programmen sowie Bildübertragungs- und Bildaufzeichnungsgeräten kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 oder 2 in Zusammenhang stehen."

90. In § 55 wird der Ausdruck „§ 2 Abs. 3 BGBlG, BGBl. Nr. 660/1996" *durch den Ausdruck* „§ 4 des Bundesgesetzblattgesetzes, BGBl. I Nr. 100/2003" *ersetzt.*

91. § 58 entfällt.

*92. **(Verfassungsbestimmung)** Dem § 60 Abs. 3 wird der folgende Abs. 4 angefügt:*

„(4) **(Verfassungsbestimmung)** Die Einfügung des Klammerausdrucks „(Verfassungsbestimmung)" in § 1 sowie § 1 Abs. 1 und 2 in der Fassung des Bundesgesetzes BGBl. I Nr. xxx/2009 treten mit 1. Jänner 2010 in Kraft. Gleichzeitig treten die Überschrift „Artikel 1 (Verfassungsbestimmung)" und der Klammerausdruck „(Verfassungsbestimmung)" in § 38 Abs. 1 außer Kraft."

93. Dem neuen § 60 Abs. 4 wird der folgende Abs. 5 angefügt:

„(5) Das Inhaltsverzeichnis, die Abschnittsüberschrift vor § 1, § 3 Abs. 1 und 2, die Überschrift und die Absatzgliederung von § 4, § 4 Abs. 1 Z 4, 5, 7 bis 9, 11 und 12, § 4 Abs. 2, § 8 Abs. 1 und 2, § 8 Abs. 4, § 12 Abs. 1, § 16 Abs. 1 und 3, § 17 Abs. 1, 1a und 4, § 19 Abs. 1 Z 3a, die §§ 20 bis 22a samt Überschriften, § 24 Abs. 2a, § 26 Abs. 1 bis 8 und 10, § 27 Abs. 9, § 28 Abs. 3, § 30 Abs. 2a, 5 bis 6a, die §§ 31 und 31a samt Überschriften, § 32 Abs. 1, 4, 6 und 7, § 34 Abs. 1, 3 und 4, § 36 Abs. 3, 3a, 6 und 9, § 38 Abs. 1und 2, § 39 Abs. 5, § 40 Abs. 1 und 2, § 41 Abs. 2 Z 4a, § 42 Abs. 1 Z 1, § 42 Abs. 5, § 46 Abs. 1 Z 2 und 3, Abs. 2 bis 3a, § 47 Abs. 4, § 49 Abs. 3, § 50 Abs. 1 bis 2a, , der 9a. Abschnitt, § 55, § 51, § 52 Abs. 2 und 4, § 61 Abs. 6 bis 9 sowie § 64 in der Fassung des Bundesgesetzes BGBl. I Nr. xxx/2009 treten mit 1. Jänner 2010 in Kraft. Gleichzeitig treten § 2, § 3 Abs. 4, die Überschrift „Artikel 2“, die Abschnittsüberschrift vor § 4, § 4 Abs. 1 Z 10, § 13 Abs. 3, § 51 Abs. 2 und § 58 außer Kraft.“

94. § 61 Abs. 6 lautet:

„(6) Videoüberwachungen, die vor dem Inkrafttreten der §§ 50a bis 50e registriert wurden, bleiben in ihrer registrierten Form rechtmäßig, wenn sie den am 31. Dezember 2009 geltenden datenschutzrechtlichen Bestimmungen genügen und die Datenschutzkommission keine Befristung verfügt hat. Hat die Datenschutzkommission hingegen eine Befristung einer solchen Videoüberwachung verfügt, bleibt diese bis zum Ablauf der Befristung, längstens aber bis zum 31. Dezember 2012 rechtmäßig.“

95. Nach § 61 Abs. 7 wird folgender Abs. 8 angefügt:

„(8) Die Verordnung nach § 16 Abs. 3 ist vom Bundeskanzler nach Maßgabe der technischen Möglichkeiten des Datenverarbeitungsregisters bis spätestens 1. Jänner 2011 neu zu erlassen. Bis zum Inkrafttreten dieser Verordnung sind die §§ 16 bis 22, § 30 Abs. 3 und 6 sowie § 40 Abs. 1 (letzterer mit Ausnahme des Verweises auf § 31a Abs. 3) in der Fassung vor dem Bundesgesetz BGBl. I Nr. xxx/2009 anzuwenden; § 22a, § 30 Abs. 2a und 6a, § 31a Abs. 1 und 2 sowie § 32 Abs. 7 sind bis dahin nicht anzuwenden. § 31 Abs. 3 in der Fassung vor dem Bundesgesetz BGBl. I Nr. xxx/2009 ist bis dahin zusätzlich weiter anzuwenden. Die Erklärung, ob eine Datenanwendung einen oder mehrere der in § 18 Abs. 2 Z 1 bis 4 genannten Tatbestände erfüllt (§ 19 Abs. 1 Z 3a), ist der Datenschutzkommission bei im Zeitpunkt des Inkrafttretens der neuen Verordnung nach § 16 Abs. 3 registrierten Datenanwendungen anlässlich der ersten über eine Streichung hinausgehenden Änderungsmeldung zu melden, die nach diesem Zeitpunkt erstattet wird. Eine Meldung allein im Hinblick auf § 19 Abs. 1 Z 3a ist nicht erforderlich.“

96. § 64 lautet:

„**§ 64.** Mit der Vollziehung dieses Bundesgesetzes ist, soweit sie nicht der Bundesregierung obliegt, der Bundeskanzler betraut.“

Artikel 3

Änderung des Sicherheitspolizeigesetzes

Das Sicherheitspolizeigesetz – SPG, BGBl. Nr. 566/1991, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 4/2008, wird wie folgt geändert:

1. Dem § 54 wird folgender Abs. 8 angefügt:

„(8) Die Sicherheitsbehörden sind ermächtigt, zur Echtzeitüberwachung Bildübertragungsgeräte einzusetzen, sofern sie zum Einsatz von Bildaufzeichnungsgeräten befugt sind oder dies zur Erfüllung einer sicherheitspolizeilichen Aufgabe oder zur Unterstützung des Streifendienstes erforderlich ist.“

2. Dem § 94 wird folgender Abs. 25 angefügt:

„(25) § 54 Abs. 8 in der Fassung des Bundesgesetzes BGBl. I Nr. xxx/2009 tritt mit 1. Jänner 2009 in Kraft.“

Textgegenüberstellung

Geltende Fassung	Vorgeschlagene Fassung
Artikel 1	
Novelle zum B-VG	
Artikel 10 (1) Bundessache ist die Gesetzgebung und die Vollziehung in folgenden Angelegenheiten:	**Artikel 10** (1) Bundessache ist die Gesetzgebung und die Vollziehung in folgenden Angelegenheiten:
1.….	1.….
13. wissenschaftlicher und fachtechnischer Archiv- und Bibliotheksdienst; Angelegenheiten der künstlerischen und wissenschaftlichen Sammlungen und Einrichtungen des Bundes; Angelegenheiten der Bundestheater mit Ausnahme der Bauangelegenheiten; Denkmalschutz; Angelegenheiten des Kultus; Volkszählungswesen sowie - unter Wahrung der Rechte der Länder, im eigenen Land jegliche Statistik zu betreiben - sonstige Statistik, soweit sie nicht nur den Interessen eines einzelnen Landes dient; Stiftungs- und Fondswesen, soweit es sich um Stiftungen und Fonds handelt, die nach ihren Zwecken über den Interessenbereich eines Landes hinausgehen und nicht schon bisher von den Ländern autonom verwaltet wurden;	13. wissenschaftlicher und fachtechnischer Archiv- und Bibliotheksdienst; Angelegenheiten der künstlerischen und wissenschaftlichen Sammlungen und Einrichtungen des Bundes; Angelegenheiten der Bundestheater mit Ausnahme der Bauangelegenheiten; Denkmalschutz; Angelegenheiten des Kultus; Volkszählungswesen sowie - unter Wahrung der Rechte der Länder, im eigenen Land jegliche Statistik zu betreiben - sonstige Statistik, soweit sie nicht nur den Interessen eines einzelnen Landes dient; Schutz personenbezogener Daten; Stiftungs- und Fondswesen, soweit es sich um Stiftungen und Fonds handelt, die nach ihren Zwecken über den Interessenbereich eines Landes hinausgehen und nicht schon bisher von den Ländern autonom verwaltet wurden;
14….	14….
Artikel 102 (1)…	**Artikel 102** (1)…
(2) Folgende Angelegenheiten können im Rahmen des verfassungsmäßig festgestellten Wirkungsbereiches unmittelbar von Bundesbehörden besorgt werden:	(2) Folgende Angelegenheiten können im Rahmen des verfassungsmäßig festgestellten Wirkungsbereiches unmittelbar von Bundesbehörden besorgt werden:
…; Denkmalschutz; Organisation und Führung der Bundespolizei;…	…; Denkmalschutz; Schutz personenbezogener Daten; Organisation und Führung der Bundespolizei; …
	Artikel 151 (1)…
	(41) Art. 10 Abs. 1 Z 13 und Art. 102 Abs. 2 in der Fassung des Bundesgesetzes BGBl. I Nr. xxx/2008 treten mit 1. Jänner 2010 in Kraft.“

Geltende Fassung	Vorgeschlagene Fassung
Artikel 2	
Novelle zum DSG 2000	
Grundrecht auf Datenschutz	**Grundrecht auf Datenschutz**
§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.	**§ 1. (Verfassungsbestimmung)** (1) Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten.
(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.	(2) Der Anspruch besteht nicht, wenn Daten zulässigerweise allgemein verfügbar sind. Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.
(3) bis (5)…	(3) bis (5)…
Zuständigkeit	
§ 2. (1) Bundessache ist die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr.	
(2) Die Vollziehung solcher Bundesgesetze steht dem Bund zu. Soweit solche Daten von einem Land, im Auftrag eines Landes, von oder im Auftrag von juristischen Personen, die durch Gesetz eingerichtet sind und deren Einrichtung hinsichtlich der Vollziehung in die Zuständigkeit der Länder fällt, verwendet werden, sind diese Bundesgesetze von den Ländern zu vollziehen, soweit nicht durch Bundesgesetz die Datenschutzkommission, der Datenschutzrat oder Gerichte mit der Vollziehung betraut werden.	
Räumlicher Anwendungsbereich	**Räumlicher Anwendungsbereich**
§ 3. (1) Die Bestimmungen dieses Bundesgesetzes sind auf die Verwendung von	**§ 3.** (1) Die Bestimmungen dieses Bundesgesetzes sind auf die Verwendung von

Geltende Fassung	Vorgeschlagene Fassung
personenbezogenen Daten im Inland anzuwenden. Darüber hinaus ist dieses Bundesgesetz auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der Europäischen Union für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung (§ 4 Z 15) eines Auftraggebers (§ 4 Z 4) geschieht.	personenbezogenen Daten im Inland anzuwenden. Darüber hinaus ist dieses Bundesgesetz auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Vertragsstaaten des Europäischen Wirtschaftsraumes für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung (§ 4 Z 15) eines Auftraggebers (§ 4 Z 4) geschieht.
(2) Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist.	(2) Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Vertragsstaat des Europäischen Wirtschaftsraumes personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist.
(3)…	(3)…
(4)Von den Abs. 1 bis 3 abweichende gesetzliche Regelungen sind nur in Angelegenheiten zulässig, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.	
Definitionen	Definitionen und Regelungsgegenstand
§ 4. Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten die Begriffe:	**§ 4.** (1) Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten die Begriffe:
1. „Daten“ („personenbezogene Daten“):…	1. Daten (personenbezogene Daten):…
2. „sensible Daten“ („besonders schutzwürdige Daten“):…	2. sensible Daten (besonders schutzwürdige Daten):…
3. „Betroffener“: jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden;	3. Betroffener: jede vom Auftraggeber (Z 4) verschiedene natürliche Person, deren Daten verwendet werden (Z 8).
4. ,,Auftraggeber": natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten (Z 9), und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Als Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie einem anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten. Wurde jedoch dem Auftragnehmer anläßlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt oder hat der Auftragnehmer die Entscheidung über die Art und Weise der Verwendung, insbesondere die Vornahme einer Verarbeitung der überlassenen Daten, auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 6 Abs. 4 eigenverantwortlich zu treffen, so gilt der mit der Herstellung des	4. Auftraggeber: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen. Sie gelten auch dann als Auftraggeber, wenn der mit der Herstellung eines Werkes beauftragte Dienstleister (Z 5) die Entscheidung trifft, zu diesem Zweck Daten zu verwenden (Z 8), es sei denn dies wurde ihm ausdrücklich untersagt oder der Beauftragte hat auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden;

Geltende Fassung	Vorgeschlagene Fassung
Werkes Betraute als datenschutzrechtlicher Auftraggeber;	
5. „Dienstleister": natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden (Z 8);	5. Dienstleister: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werks verwenden.
6. „Datei“:…	6. Datei:…
7. „Datenanwendung“ (früher: „Datenverarbeitung“): die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);	7. Datenanwendung: die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);
8. „Verwenden von Daten“: jede Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten;	8. Verwenden von Daten: jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten;
9. „Verarbeiten von Daten“: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister mit Ausnahme des Übermittelns (Z 12) von Daten;	9. Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns (Z 12) von Daten.“
10. „Ermitteln von Daten“: das Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden;	
11. „Überlassen von Daten“: die Weitergabe von Daten vom Auftraggeber an einen Dienstleister;	11. Überlassen von Daten: die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses (Z 5);
12. „Übermitteln von Daten“: die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;	12. Übermitteln von Daten: die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;
13. „Informationsverbundsystem“:…	13. Informationsverbundsystem:…
14. „Zustimmung“:…	14. Zustimmung:…
15. „Niederlassung:…	15. Niederlassung:…

Geltende Fassung	Vorgeschlagene Fassung
Manuelle Dateien	(2) Dieses Gesetz gilt für Daten, die in einer Datenanwendung oder manuellen Datei verwendet werden. Wo in den folgenden Bestimmungen von Datenanwendungen die Rede ist, gelten sie auch für manuelle Dateien. Für alle übrigen manuellen Daten gelten § 6 Abs. 1 Z 1 bis 3 und Abs. 2, §§ 7 bis 9 und die Bestimmungen des 6. Abschnitts sinngemäß.
§ 58. Soweit manuell, dh. ohne Automationsunterstützung geführte Dateien für Zwecke solcher Angelegenheiten bestehen, in denen die Zuständigkeit zur Gesetzgebung Bundessache ist, gelten sie als Datenanwendungen im Sinne des § 4 Z 7. § 17 gilt mit der Maßgabe, dass die Meldepflicht nur für solche Dateien besteht, deren Inhalt gemäß § 18 Abs. 2 der Vorabkontrolle unterliegt.	
Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten	**Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten**
§ 8. (1) Gemäß § 1 Abs. 1 bestehende schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn…	**§ 8.** (1) Schutzwürdige Geheimhaltungsinteressen im Sinn des § 7 Abs. 1 und Abs. 2 Z 3 sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn…
(2) Bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten gelten schutzwürdige Geheimhaltungsinteressen als nicht verletzt. Das Recht, gegen die Verwendung solcher Daten gemäß § 28 Widerspruch zu erheben, bleibt unberührt.	(2) Bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten gelten schutzwürdige Geheimhaltungsinteressen als nicht verletzt. Das Recht, gegen die Verwendung zulässigerweise veröffentlichter Daten gemäß § 28 Widerspruch zu erheben, bleibt unberührt.
(3)…	(3)…
(4) Die Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen verstößt - unbeschadet der Bestimmungen des Abs. 2 - nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn	(4) Die Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen verstößt - unbeschadet der Bestimmungen des Abs. 2 - nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn
1. bis 3.: … .	1. bis 3. … ; 4. die Datenweitergabe zum Zweck der Erstattung einer Anzeige an eine zur Verfolgung der angezeigten strafbaren Handlungen (Unterlassungen) zuständige Behörde erfolgt.
Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland	**Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland**
§ 12. (1) Die Übermittlung und Überlassung von Daten an Empfänger in Mitgliedstaaten der Europäischen Union ist keinen Beschränkungen im Sinne des § 13 unterworfen. Dies gilt nicht für den Datenverkehr zwischen Auftraggebern des öffentlichen Bereichs in Angelegenheiten, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.	**§ 12.** (1) Die Übermittlung und Überlassung von Daten an Empfänger in Vertragsstaaten des Europäischen Wirtschaftsraumes (EWR) ist keinen Beschränkungen im Sinne des § 13 unterworfen. Dies gilt nicht für den Datenverkehr zwischen Auftraggebern des öffentlichen Bereichs in Angelegenheiten, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.
(2) bis (5)…	(2) bis (5)…
Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland	**Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland**
§ 13. (1) und (2)…	**§ 13.** (1) und (2)…
(3) Im Genehmigungsverfahren haben Auftraggeber des öffentlichen Bereichs	*Der Inhalt wird nunmehr von § 40 Abs. 2 abgedeckt.*

Geltende Fassung	Vorgeschlagene Fassung
auch hinsichtlich der Datenanwendungen, die sie in Vollziehung der Gesetze durchführen, Parteistellung.	
(4) bis (7)…	(4) bis (7)…
Datenverarbeitungsregister	**Datenverarbeitungsregister**
§ 16. (1) Bei der Datenschutzkommission ist ein Register der Datenanwendungen zum Zweck der Prüfung ihrer Rechtmäßigkeit und zum Zweck der Information der Betroffenen eingerichtet.	**§ 16.** (1) Die Datenschutzkommission hat ein Register der Auftraggeber mit den von ihnen betriebenen Datenanwendungen zum Zweck der Information der Betroffenen zu führen.
(2)…	(2)…
(3) Der Bundeskanzler hat die näheren Bestimmungen über die Führung des Registers durch Verordnung zu erlassen. Dabei ist auf die Richtigkeit und Vollständigkeit des Registers, die Übersichtlichkeit und Aussagekraft der Eintragungen und die Einfachheit der Einsichtnahme Bedacht zu nehmen. Es ist die Möglichkeit vorzusehen, eine Meldung (§§ 17 und 19) auf automationsunterstütztem Wege vorzunehmen.	(3) Der Bundeskanzler hat die näheren Bestimmungen über die Führung des Registers durch Verordnung zu erlassen. Dabei ist auf die Richtigkeit und Vollständigkeit des Registers, die Übersichtlichkeit und Aussagekraft der Eintragungen und die Einfachheit der Einsichtnahme Bedacht zu nehmen.
Meldepflicht des Auftraggebers	**Meldepflicht des Auftraggebers**
§ 17. (1) Jeder Auftraggeber hat, soweit in den Abs. 2 und 3 nicht anderes bestimmt ist, vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzkommission mit dem in § 19 festgelegten Inhalt zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten. Diese Meldepflicht gilt auch für Umstände, die nachträglich die Unrichtigkeit und Unvollständigkeit einer Meldung bewirken.	**§ 17.** (1) Jeder Auftraggeber hat, soweit in den Abs. 2 und 3 nicht anderes bestimmt ist, vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzkommission mit dem in § 19 festgelegten Inhalt zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten. Diese Meldepflicht gilt auch für Umstände, die nachträglich die Unrichtigkeit und Unvollständigkeit einer Meldung bewirken (Änderungsmeldung). Für manuelle Dateien besteht eine Meldepflicht nur, soweit die Inhalte zumindest einen der Tatbestände des § 18 Abs. 2 Z 1 bis 4 erfüllen.
	(1a) Die Meldung ist in elektronischer Form im Wege der vom Bundeskanzler bereit zu stellenden Internetanwendung einzubringen. Die Identifizierung und Authentifizierung kann insbesondere durch die Bürgerkarte (§ 2 Z 10 des E-Government-Gesetzes, BGBl. I Nr. 10/2004) erfolgen. Nähere Bestimmungen über die Identifizierung und Authentifizierung sind in die gemäß § 16 Abs. 3 zu erlassende Verordnung aufzunehmen. Eine Meldung in nicht-elektronischer Form ist für manuelle Dateien sowie bei einem längeren technischen Ausfall der Internetanwendung zulässig.
§ 17. (2) und (3)…	(2) und (3)….
	(4) Weiters sind Datenanwendungen von der Meldepflicht ausgenommen, für die der Zweck, die betroffenen Personengruppen, Datenarten, Übermittlungen und Übermittlungsempfänger in einem Gesetz oder in einer Verordnung abschließend geregelt sind.

Geltende Fassung	Vorgeschlagene Fassung
Notwendiger Inhalt der Meldung	**Notwendiger Inhalt der Meldung**
§ 19. (1) Eine Meldung im Sinne des § 17 hat zu enthalten: 1. bis 3. …	**§ 19.** (1) Eine Meldung im Sinne des § 17 hat zu enthalten: 1. bis 3. … 3a. die Erklärung, ob die Datenanwendung einen oder mehrere der in § 18 Abs. 2 Z 1 bis 4 genannten Tatbestände erfüllt, und
4. bis 7….	4. bis 7….
Prüfungs- und Verbesserungsverfahren	**Prüfungs- und Verbesserungsverfahren**
§ 20. (1) Die Datenschutzkommission hat alle Meldungen binnen zwei Monaten zu prüfen. Kommt sie hiebei zur Auffassung, daß eine Meldung im Sinne des § 19 Abs. 3 mangelhaft ist, so ist dem Auftraggeber längstens innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung des Mangels unter Setzung einer Frist aufzutragen. (2), (3), (5), (6) s. sogleich (4) Wird einem Verbesserungsauftrag nicht fristgerecht entsprochen, so hat die Datenschutzkommission die Registrierung mit Bescheid abzulehnen; andernfalls gilt die Meldung als ursprünglich richtig eingebracht.	**§ 20.** (1) Meldungen von Datenanwendungen, die nach Angabe des Auftraggebers nicht einen der Tatbestände des § 18 Abs. 2 Z 1 bis 4 erfüllen, sind nur automationsunterstützt auf ihre Vollständigkeit und Plausibilität zu prüfen. Ist demnach die Meldung nicht fehlerhaft, so ist sie sofort zu registrieren. (2) Wird bei der automationsunterstützten Prüfung ein Fehler der Meldung festgestellt, so ist dem Auftraggeber die Möglichkeit zur Verbesserung einzuräumen. Gleichzeitig ist er darauf hinzuweisen, dass die Meldung als nicht eingebracht gilt, wenn keine Verbesserung erfolgt oder er auf der Einbringung der unverbesserten Meldung besteht. Im letztgenannten Fall ist die Meldung von der Datenschutzkommission auf Mangelhaftigkeit im Sinn des § 19 Abs. 3 zu prüfen. (3) Meldungen, die der Auftraggeber als vorabkontrollpflichtig bezeichnet hat oder von diesem zulässigerweise nicht im Wege der Internetanwendung (§ 17 Abs. 1a) eingebracht wurden, sind auf Mangelhaftigkeit im Sinn des § 19 Abs. 3 zu prüfen. (4) Ergibt die Prüfung nach § 19 Abs. 3 eine Mangelhaftigkeit der Meldung, so ist dem Auftraggeber innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung unter Setzung einer Frist aufzutragen. Im Verbesserungsauftrag ist auf die Rechtsfolgen einer Nichtbefolgung nach Abs. 5 hinzuweisen. (5) Wird dem Verbesserungsauftrag nicht entsprochen, ist die Registrierung der Meldung durch eine schriftliche Mitteilung abzulehnen. In die Mitteilung sind aufzunehmen: 1. die Punkte, in denen der Verbesserungsauftrag nicht erfüllt wurde und 2. der Hinweis, dass innerhalb von zwei Wochen ab Zustellung bei der Datenschutzkommission ein Antrag gestellt werden kann, über die Ablehnung mit Bescheid abzusprechen. Nach Ablauf der von der Datenschutzkommission gesetzten Frist (Abs. 4) erstattete Verbesserungen sind nicht zu berücksichtigen.
§ 20. (2) Liegt wegen wesentlicher Gefährdung schutzwürdiger	*Diese Bestimmungen entfallen. Zum bisherigen Abs. 2 s. § 30 Abs. 6a, Abs. 3*

Geltende Fassung

Geheimhaltungsinteressen der Betroffenen durch die gemeldete Datenanwendung Gefahr im Verzug vor, so hat die Datenschutzkommission die Weiterführung der Datenanwendung mit Bescheid gemäß § 57 Abs. 1 AVG vorläufig zu untersagen.

(3) Bei Datenanwendungen, die gemäß § 18 Abs. 2 der Vorabkontrolle unterliegen, ist gleichzeitig mit einem allfälligen Auftrag zur Verbesserung darüber abzusprechen, ob die Verarbeitung bereits aufgenommen werden darf oder ob dies mangels Nachweises ausreichender Rechtsgrundlagen für die gemeldete Datenanwendung nicht zulässig ist.

(5) Wird innerhalb von zwei Monaten nach Erstattung der Meldung kein Auftrag zur Verbesserung erteilt, gilt die Meldepflicht als erfüllt. Bei Datenanwendungen, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegen, darf die Verarbeitung aufgenommen werden.

(6) Im Registrierungsverfahren haben Auftraggeber des öffentlichen Bereichs auch hinsichtlich der Datenanwendungen, die sie in Vollziehung der Gesetze durchführen, Parteistellung.

Registrierung

§ 21. (1) Meldungen gemäß § 19 sind in das Datenverarbeitungsregister einzutragen, wenn

1. das Prüfungsverfahren die Zulässigkeit der Registrierung ergeben hat oder
2. zwei Monate nach Einlangung der Meldung bei der Datenschutzkommission verstrichen sind, ohne daß ein Verbesserungsauftrag gemäß § 20 Abs. 1 erteilt wurde oder
3. der Auftraggeber die verlangten Verbesserungen fristgerecht vorgenommen hat.

Die in der Meldung enthaltenen Angaben über Datensicherheitsmaßnahmen sind im Register nicht ersichtlich zu machen.

(2) Bei Datenanwendungen, die gemäß § 18 Abs. 2 der Vorabkontrolle unterliegen, können auf Grund der Ergebnisse des Prüfungsverfahrens dem Auftraggeber Auflagen für die Vornahme der Datenanwendung durch Bescheid erteilt werden, soweit dies zur Wahrung der durch dieses Bundesgesetz geschützten Interessen der Betroffenen notwendig ist.

(3) Dem Auftraggeber ist die Durchführung der Registrierung schriftlich in Form eines Registerauszuges mitzuteilen.

(4) Jedem Auftraggeber ist bei der erstmaligen Registrierung eine Registernummer zuzuteilen.

Vorgeschlagene Fassung

entfällt ersatzlos, der Inhalt von Abs. 5 ist weiterhin durch § 21 Abs. 1 Z 2 abgedeckt, Abs. 6 wird durch § 40 Abs. 2 abgedeckt.

Registrierung

§ 21. (1) Meldungen gemäß § 19 sind in das Datenverarbeitungsregister einzutragen, wenn

1. das Prüfungsverfahren nach § 20 Abs. 1 keinen Fehler ergeben hat oder
2. das Prüfungsverfahren nach § 20 Abs. 2 und 3 keine Mangelhaftigkeit der Meldung ergeben hat oder
3. nach Einlangen einer auf Mangelhaftigkeit zu prüfenden Meldung bei der Datenschutzkommission zwei Monate verstrichen sind, ohne dass ein Verbesserungsauftrag gemäß § 20 Abs. 4 erteilt wurde oder
4. der Auftraggeber die aufgetragenen Verbesserungen (§ 20 Abs. 4) vorgenommen hat.

Die in der Meldung enthaltenen Angaben über Datensicherheitsmaßnahmen sind im Register nicht ersichtlich zu machen.

(2) Bei Datenanwendungen, die gemäß § 18 der Vorabkontrolle unterliegen, können auf Grund der Ergebnisse des Prüfungsverfahrens dem Auftraggeber Auflagen, Bedingungen oder Befristungen für die Vornahme der Datenanwendung durch Bescheid erteilt werden, soweit dies zur Wahrung der durch dieses Bundesgesetz geschützten Interessen der Betroffenen notwendig ist.

(3) Der Auftraggeber ist von der Durchführung und vom Inhalt der Registrierung in geeigneter Weise zu verständigen.

(4) Jedem Auftraggeber ist bei der erstmaligen Registrierung eine Registernummer

Geltende Fassung	Vorgeschlagene Fassung
	zuzuteilen.
	(5) Hat die automationsunterstützte Prüfung nach § 20 Abs. 1 nicht zu einer Fehlermeldung geführt, so ist in die Registrierung ein Vermerk aufzunehmen, dass der Meldungsinhalt nur automationsunterstützt geprüft wurde.
Richtigstellung des Registers	**Richtigstellung des Registers und Rechtsnachfolge**
§ 22. (1) Streichungen und Änderungen im Datenverarbeitungsregister sind auf Antrag des Eingetragenen oder in den Fällen der Abs. 2 und 4 von Amts wegen durchzuführen.	**§ 22.** (1) Streichungen aus dem Register und sonstige Änderungen des Registers sind auf Grund einer Änderungsmeldung des registrierten Auftraggebers oder von Amts wegen in den Fällen des Abs. 2, des § 22a Abs. 2 und des § 30 Abs. 6a vorzunehmen. Derartige Änderungen sind für die Dauer von drei Jahren ersichtlich zu machen.
(2) Gelangen der Datenschutzkommission aus amtlichen Verlautbarungen Änderungen in der Bezeichnung oder der Anschrift des Auftraggebers zur Kenntnis, so sind die Eintragungen von Amts wegen zu berichtigen. Ergibt sich aus einer amtlichen Verlautbarung der Wegfall der Rechtsgrundlage des Auftraggebers, ist von Amts wegen die Streichung aus dem Register anzuordnen.	(2) Gelangen der Datenschutzkommission aus amtlichen Verlautbarungen Änderungen in der Bezeichnung oder der Anschrift des Auftraggebers zur Kenntnis, so sind die Eintragungen von Amts wegen zu berichtigen. Ergibt sich aus einer amtlichen Verlautbarung der Wegfall der Rechtsgrundlage des Auftraggebers, ist dieser von Amts wegen aus dem Register zu streichen. Außerdem ist eine registrierte Datenanwendung zu streichen, wenn der Datenschutzkommission zur Kenntnis gelangt, dass eine registrierte Datenanwendung dauerhaft nicht mehr betrieben wird.
(3) Änderungen oder Streichungen nach Abs. 2 sind ohne weiteres Ermittlungsverfahren durch Bescheid zu verfügen.	(3) Berichtigungen oder Streichungen nach Abs. 2 sind ohne weiteres Ermittlungsverfahren durch Mandatsbescheid (§ 38) zu verfügen.
	(4) Der Rechtsnachfolger eines registrierten Auftraggebers kann einzelne oder alle registrierten Meldungen des Rechtsvorgängers übernehmen, wenn er innerhalb von zwei Monaten nach Wirksamkeit der Rechtsnachfolge eine entsprechend glaubhaft gemachte Erklärung gegenüber der Datenschutzkommission abgibt. Dem Rechtsnachfolger kann auf Antrag auch die Registernummer des Rechtsvorgängers übertragen werden, wenn der Rechtsvorgänger jegliche Verarbeitung personenbezogener Daten in Auftraggebereigenschaft eingestellt hat.
	Verfahren zur Überprüfung der Erfüllung der Meldepflicht
§ 22. (4) Werden der Datenschutzkommission andere als die in Abs. 2 bezeichneten Umstände bekannt, die den Verdacht der Mangelhaftigkeit einer Registrierung im Sinne des § 19 Abs. 3 oder der rechtswidrigen Unterlassung einer Meldung begründen, so hat die Datenschutzkommission ein Verfahren zur Feststellung des für die Erfüllung der Meldepflicht erheblichen Sachverhalts einzuleiten und das Datenverarbeitungsregister entsprechend dem Ergebnis des Verfahrens zu berichtigen.	**§ 22a.** (1) Die Datenschutzkommission kann jederzeit die Erfüllung der Meldepflicht durch einen Auftraggeber prüfen. Dies gilt sowohl für die Mangelhaftigkeit einer registrierten Meldung im Sinn des § 19 Abs. 3 als auch für die rechtswidrige Unterlassung von Meldungen.
	(2) Bei Vorliegen des Verdachtes der Nichterfüllung der Meldepflicht infolge Mangelhaftigkeit einer registrierten Meldung (Abs. 1) oder Unterlassung der Meldung, die über die Fälle des § 22 Abs. 2 hinausgeht, ist ein Verfahren zur Berichtigung des Datenverarbeitungsregisters durchzuführen. Das Verfahren wird durch begründete Verfahrensanordnung eingeleitet, die dem meldepflichtigen Auftraggeber mit einem Auftrag zur Verbesserung (§ 20 Abs. 4) oder einer Aufforderung zur Nachmeldung

Geltende Fassung	Vorgeschlagene Fassung
	(§ 17 Abs. 1) innerhalb gesetzter Frist zuzustellen ist.
	(3) Wird einem im Verfahren nach Abs. 2 erteilten Verbesserungsauftrag nicht entsprochen, so ist die Streichung der Meldung mit Bescheid der Datenschutzkommission zu verfügen. Die Streichung kann sich, wenn dies technisch möglich, im Hinblick auf den Zweck der Datenanwendung sinnvoll und zur Herstellung des rechtmäßigen Zustandes ausreichend ist, auch nur auf Teile der Meldung beschränken.
	(4) Wird einer im Verfahren nach Abs. 2 erteilten Aufforderung zur Nachmeldung nicht entsprochen und die Unterlassung einer Meldung entgegen § 17 Abs. 1 erwiesen, so ist mit Bescheid der Datenschutzkommission der weitere Betrieb der Datenanwendung, soweit er vom Registerstand abweicht, zu untersagen und gleichzeitig Anzeige nach § 52 Abs. 2 Z 1 an die zuständige Behörde zu erstatten.
	(5) Ergibt das Verfahren nach Abs. 2 alleine die Unangemessenheit oder die Nichteinhaltung von nach § 19 Abs. 1 Z 7 erklärten Datensicherheitsmaßnahmen, so ist dies mit Bescheid festzustellen und gleichzeitig eine angemessene Frist zur Herstellung ausreichender Datensicherheit zu setzen. Der Auftraggeber hat innerhalb dieser Frist der Datenschutzkommission die getroffenen Maßnahmen mitzuteilen. Sind diese nicht ausreichend, so ist die Streichung der Datenanwendung zu verfügen.
	(6) Die Einleitung und der Stand eines Berichtigungsverfahrens nach Abs. 2 ist bei registrierten Meldungen im Datenverarbeitungsregister bis zur Einstellung oder bis zur Herstellung eines rechtmäßigen Zustandes durch Maßnahmen nach den Abs. 3 bis 6 geeignet anzumerken.
Informationspflicht des Auftraggebers	**Informationspflicht des Auftraggebers**
§ 24.(1) und (2)…	**§ 24.**(1) und (2)…
	(2a) Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden, hat er darüber unverzüglich die Betroffenen zu informieren.
(3) und (4)	(3) und (4)
Auskunftsrecht	**Auskunftsrecht**
§ 26. (1) Der Auftraggeber hat dem Betroffenen Auskunft über die zu seiner Person verarbeiteten Daten zu geben, wenn der Betroffene dies schriftlich verlangt und seine Identität in geeigneter Form nachweist. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt werden. Die Auskunft hat die verarbeiteten Daten, die verfügbaren Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hiefür in allgemein verständlicher Form	**§ 26.** (1) Ein Auftraggeber hat jeder Person oder Personengemeinschaft, die dies schriftlich verlangt und ihre Identität in geeigneter Form nachweist, Auskunft über die zu ihrer Person verarbeiteten Daten zu geben. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt werden. Die Auskunft hat die verarbeiteten Daten, die Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hiefür in allgemein verständlicher Form anzuführen. Auf Verlangen

Geltende Fassung	Vorgeschlagene Fassung
anzuführen. Auf Verlangen des Betroffenen sind auch Namen und Adresse von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Mit Zustimmung des Betroffenen kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.	eines Betroffenen sind auch Namen und Adressen von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Wenn zur Person des Auskunftswerbers keine Daten vorhanden sind, genügt die Bekanntgabe dieses Umstandes (Negativauskunft). Mit Zustimmung des Auskunftswerbers kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.
(2) Die Auskunft ist nicht zu erteilen, soweit dies zum Schutz des Betroffenen aus besonderen Gründen notwendig ist oder soweit überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen, der Auskunftserteilung entgegenstehen. Überwiegende öffentliche Interessen können sich hiebei aus der Notwendigkeit	(2) Die Auskunft ist nicht zu erteilen, soweit dies zum Schutz des Auskunftswerbers aus besonderen Gründen notwendig ist oder soweit überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen, der Auskunftserteilung entgegenstehen. Überwiegende öffentliche Interessen können sich hiebei aus der Notwendigkeit
1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder	1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder	2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder
3. der Sicherung der Interessen der umfassenden Landesverteidigung oder	3. der Sicherung der Interessen der umfassenden Landesverteidigung oder
4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder	4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder
5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten ergeben. Die Zulässigkeit der Auskunftsverweigerung aus den Gründen der Z 1 bis 5 unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission gemäß § 31 Abs. 4.	5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten ergeben. Die Zulässigkeit der Auskunftsverweigerung aus den Gründen der Z 1 bis 5 unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission gemäß § 31 Abs. 4.
(3) Der Betroffene hat am Auskunftsverfahren über Befragung in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden.	(3) Der Auskunftswerber hat am Auskunftsverfahren über Befragung in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden.
(4) Innerhalb von acht Wochen nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. Von der Erteilung der Auskunft kann auch deshalb abgesehen werden, weil der Betroffene am Verfahren nicht gemäß Abs. 3 mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.	(4) Innerhalb von acht Wochen nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. Von der Erteilung der Auskunft kann auch deshalb abgesehen werden, weil der Auskunftswerber am Verfahren nicht gemäß Abs. 3 mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.
(5) 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, die eine Auskunftsverweigerung erfordert, folgendermaßen vorzugehen: Es ist in allen Fällen, in welchen keine Auskunft erteilt wird - also auch weil tatsächlich keine Daten verwendet werden -, anstelle einer inhaltlichen Begründung der Hinweis zu geben, dass keine der Auskunftspflicht unterliegenden Daten über den Betroffenen verwendet werden. Die Zulässigkeit dieser	(5) 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, die eine Auskunftsverweigerung erfordert, folgendermaßen vorzugehen: Es ist in allen Fällen, in welchen keine Auskunft erteilt wird - also auch weil tatsächlich keine Daten verwendet werden -, anstelle einer inhaltlichen Begründung der Hinweis zu geben, dass keine der Auskunftspflicht unterliegenden Daten über den Auskunftswerber verwendet werden. Die Zulässigkeit

Geltende Fassung	Vorgeschlagene Fassung
Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.	dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.
(6) Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Betroffene im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat. In allen anderen Fällen kann ein pauschalierter Kostenersatz von 18,89 Euro verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.	(6) Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Auskunftswerber im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat. In allen anderen Fällen kann ein pauschalierter Kostenersatz von 18,89 Euro verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.
(7) Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Betroffenen innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 31 an die Datenschutzkommission bis zum rechtskräftigen Abschluß des Verfahrens nicht vernichten.	(7) Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Auskunftswerber innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 31 an die Datenschutzkommission bis zum rechtskräftigen Abschluß des Verfahrens nicht vernichten.
(8) Soweit Datenanwendungen von Gesetzes wegen öffentlich einsehbar sind, hat der Betroffene ein Recht auf Auskunft in dem Umfang, in dem ein Einsichtsrecht besteht. Für das Verfahren der Einsichtnahme gelten die näheren Regelungen der das öffentliche Buch oder Register einrichtenden Gesetze.	(8) In dem Umfang, in dem eine Datenanwendung für eine Person oder Personengemeinschaft hinsichtlich der zu ihr verarbeiteten Daten von Gesetzes wegen einsehbar ist, hat diese das Recht auf Auskunft nach Maßgabe der das Einsichtsrecht vorsehenden Bestimmungen. Für das Verfahren der Einsichtnahme (einschließlich deren Verweigerung) gelten die näheren Regelungen des Gesetzes, das das Einsichtsrecht vorsieht. In Abs. 1 genannte Bestandteile einer Auskunft, die vom Einsichtsrecht nicht umfasst sind, können dennoch nach diesem Bundesgesetz geltend gemacht werden.
(9) …	(9) …
(10) Im Falle der auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 6 Abs. 4 eigenverantwortlichen Entscheidung über die Durchführung einer Datenanwendung durch einen Auftragnehmer gemäß § 4 Z 4, dritter Satz, kann der Betroffene sein Auskunftsbegehren zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Dieser hat dem Betroffenen, soweit dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse des eigenverantwortlichen Auftragnehmers mitzuteilen, damit der Betroffene sein Auskunftsrecht gemäß Abs. 1 gegen diesen geltend machen kann.	(10) Ergibt sich eine Auftraggeberstellung aus einem Gesetz, einer Verordnung oder auf Grund von Verhaltensregeln, obwohl die Datenverarbeitung für Zwecke der Auftragserfüllung für einen Dritten erfolgt (§ 4 Z 4 letzter Satz), kann der Auskunftswerber sein Auskunftsbegehren zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Dieser hat dem Auskunftswerber, soweit ihm dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse des tatsächlichen Auftraggebers mitzuteilen, damit der Auskunftswerber sein Auskunftsrecht gemäß Abs. 1 gegen diesen geltend machen kann. Das gilt auch für einen Dienstleister, wenn ein an ihn gerichtetes Auskunftsbegehren erkennen lässt, dass der Auskunftswerber ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält. Stattdessen kann er auch innerhalb derselben Frist das Auskunftsbegehren an den Auftraggeber weiterleiten und den Auskunftswerber davon verständigen.

Geltende Fassung	**Vorgeschlagene Fassung**
Recht auf Richtigstellung oder Löschung	**Recht auf Richtigstellung oder Löschung**
§ 27. (1) bis (8) …	**§ 27.** (1) bis (8) …
(9) Die Regelungen der Abs. 1 bis 8 gelten für das gemäß Strafregistergesetz 1968 geführte Strafregister sowie für öffentliche Bücher und Register, die von Auftraggebern des öffentlichen Bereichs geführt werden, nur insoweit als für 1. die Verpflichtung zur Richtigstellung und Löschung von Amts wegen oder 2. das Verfahren der Durchsetzung und die Zuständigkeit zur Entscheidung über Berichtigungs- und Löschungsanträge von Betroffenen durch Bundesgesetz nicht anderes bestimmt ist.	(9) Die Regelungen der Abs. 1 bis 8 gelten für das gemäß Strafregistergesetz 1968 geführte Strafregister sowie für Bücher und Register, die von Auftraggebern des öffentlichen Bereichs geführt werden, nur insoweit als für 1. die Verpflichtung zur Richtigstellung und Löschung von Amts wegen oder 2. das Verfahren der Durchsetzung und die Zuständigkeit zur Entscheidung über Berichtigungs- und Löschungsanträge von Betroffenen durch Bundesgesetz nicht anderes bestimmt ist.
Widerspruchsrecht	**Widerspruchsrecht**
§ 28. (1) bis (2) …	**§ 28.** (1) bis (2) …
	(3) § 27 Abs. 4 bis 6 gelten auch in den Fällen der Abs. 1 und 2.
Kontrollbefugnisse der Datenschutzkommission	**Kontrollbefugnisse der Datenschutzkommission**
§ 30. (1) und (2)…	**§ 30.** (1) und (2)…
	(2a) Sofern sich eine zulässige Eingabe nach Abs. 1 oder Abs. 1a oder ein begründeter Verdacht nach Abs. 2 auf eine meldepflichtige Datenanwendung (Datei) bezieht, hat die Datenschutzkommission die Erfüllung der Meldepflicht zu überprüfen und erforderlichenfalls nach den §§ 22 und 22a vorzugehen.
(3) bis (4) …	(3) bis (4) …
(5) Informationen, die der Datenschutzkommission oder ihren Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Die Pflicht zur Verschwiegenheit besteht auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, daß dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach den §§ 51 oder 52 dieses Bundesgesetzes oder eines Verbrechens nach § 278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch dem Ersuchen der Strafgerichte nach § 26 StPO zu entsprechen ist.	(5) Informationen, die der Datenschutzkommission oder ihren Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Dazu zählt auch die Verwendung für Zwecke der gerichtlichen Rechtsverfolgung durch den Einschreiter oder die Datenschutzkommission nach § 32. Im Übrigen besteht die Pflicht zur Verschwiegenheit auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, dass dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach den §§ 51 oder 52 dieses Bundesgesetzes oder eines Verbrechens nach § 278a des Strafgesetzbuches, BGBl Nr. 60/1974 (kriminelle Organisation), oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch Ersuchen nach § 76 der Strafprozessordnung, BGBl Nr. 631/1975, zu entsprechen ist.
(6) Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzkommission Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht	„(6) Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzkommission, sofern nicht Maßnahmen nach den §§ 22 und 22a oder nach Abs. 6a zu treffen sind, Empfehlungen aussprechen, für deren Befolgung

Geltende Fassung	Vorgeschlagene Fassung
entsprochen, so kann die Datenschutzkommission je nach der Art des Verstoßes von Amts wegen insbesondere 1. ein Verfahren zur Überprüfung der Registrierung gemäß § 22 Abs. 4 einleiten, oder 2. Strafanzeige nach §§ 51 oder 52 erstatten, oder 3. bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 32 Abs. 5 erheben, oder 4. bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, daß der Empfehlung der Datenschutzkommission entsprochen wird, oder der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung darf von der Datenschutzkommission der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht.	erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzkommission je nach der Art des Verstoßes von Amts wegen insbesondere 1. Strafanzeige nach §§ 51 oder 52 erstatten, oder 2. bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 32 Abs. 5 erheben, oder 3. bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, dass der Empfehlung der Datenschutzkommission entsprochen wird, oder der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung darf von der Datenschutzkommission der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht.
Vgl. den geltenden § 20 Abs. 2.	(6a) Liegt durch den Betrieb einer Datenanwendung eine wesentliche Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen (Gefahr im Verzug) vor, so hat die Datenschutzkommission die Weiterführung der Datenanwendung mit Bescheid gemäß § 57 Abs. 1 AVG zu untersagen. Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenanwendung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Wird einer Untersagung nicht sogleich Folge geleistet, ist Strafanzeige wegen der Verwaltungsübertretung nach § 52 Abs. 1 Z 3 zu erstatten. Nach Rechtskraft einer Untersagung nach diesem Absatz ist ein Berichtigungsverfahren nach § 22a Abs. 2 formlos einzustellen. Die Datenanwendung ist im Umfang der Untersagung aus dem Register zu streichen.
Beschwerde an die Datenschutzkommission	**Beschwerde an die Datenschutzkommission**
§ 31. (1) Die Datenschutzkommission erkennt auf Antrag des Betroffenen über behauptete Verletzungen des Rechtes auf Auskunft gemäß § 26 durch den Auftraggeber einer Datenanwendung, soweit sich das Auskunftsbegehren nicht auf die Verwendung von Daten für Akte der Gesetzgebung oder der Gerichtsbarkeit bezieht.	**§ 31.** (1) Die Datenschutzkommission erkennt über Beschwerden von Personen, die behaupten, in ihrem Recht auf Auskunft nach § 26 oder nach § 50 Abs. 1 dritter Satz oder in ihrem Recht auf Darlegung einer automatisierten Einzelentscheidung nach § 49 Abs. 3 verletzt zu sein, soweit sich das Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) nicht auf die Verwendung von Daten für Akte im Dienste der Gesetzgebung oder der Gerichtsbarkeit bezieht.
(2) Zur Entscheidung über behauptete Verletzungen der Rechte eines Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung nach diesem Bundesgesetz ist die Datenschutzkommission dann zuständig, wenn der Betroffene seine Beschwerde	(2) Die Datenschutzkommission erkennt weiters über Beschwerden von Personen, die behaupten, in ihrem Recht auf Geheimhaltung (§ 1 Abs. 1) oder in ihrem Recht auf Richtigstellung oder auf Löschung (§§ 27 und 28) verletzt zu sein, sofern der Anspruch

Geltende Fassung	Vorgeschlagene Fassung
gegen einen Auftraggeber des öffentlichen Bereichs richtet, der nicht als Organ der Gesetzgebung oder der Gerichtsbarkeit tätig ist.	nicht nach § 32 Abs. 1 vor einem Gericht geltend zu machen ist oder sich gegen ein Organ im Dienste der Gesetzgebung oder der Gerichtsbarkeit richtet. (3) Die Beschwerde hat zu enthalten: 1. die Bezeichnung des als verletzt erachteten Rechts, 2. soweit dies zumutbar ist, die Bezeichnung des Rechtsträgers oder Organs, dem die behauptete Rechtsverletzung zugerechnet wird (Beschwerdegegner), 3. den Sachverhalt, aus dem die Rechtsverletzung abgeleitet wird, 4. die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt, 5. das Begehren, die behauptete Rechtsverletzung festzustellen und 6. die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist. (4) Einer Beschwerde nach Abs. 1 sind außerdem das zu Grunde liegende Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) und eine allfällige Antwort des Beschwerdegegners anzuschließen. Einer Beschwerde nach Abs. 2 sind außerdem der zu Grunde liegende Antrag auf Richtigstellung oder Löschung und eine allfällige Antwort des Beschwerdegegners anzuschließen. (5) Die der Datenschutzkommission durch § 30 Abs. 2 bis 4 eingeräumten Kontrollbefugnisse kommen ihr auch in Beschwerdeverfahren nach Abs. 1 und 2 gegenüber dem Beschwerdegegner zu. Ebenso besteht auch hinsichtlich dieser Verfahren die Verschwiegenheitspflicht nach § 30 Abs. 5. (6) Im Fall der Einbringung einer zulässigen Beschwerde nach Abs. 1 oder 2 ist ein auf Grund einer Eingabe nach § 30 Abs. 1 über denselben Gegenstand eingeleitetes Kontrollverfahren durch eine entsprechende Information (§ 30 Abs. 7) zu beenden. Die Datenschutzkommission kann aber dennoch auch während der Anhängigkeit des Beschwerdeverfahrens von Amts wegen nach § 30 Abs. 2 vorgehen, wenn ein begründeter Verdacht einer über den Beschwerdefall hinausgehenden Verletzung datenschutzrechtlicher Verpflichtungen besteht. § 30 Abs. 3 bleibt unberührt. (7) Soweit sich eine Beschwerde nach Abs. 1 oder 2 als berechtigt erweist, ist ihr Folge zu geben und die Rechtsverletzung festzustellen. Ist eine festgestellte Verletzung im Recht auf Auskunft (Abs. 1) einem in Formen des Privatrechts eingerichteten Rechtsträger zuzurechnen, der nicht in Ausübung von Hoheitsgewalt tätig geworden ist, so ist diesem auf Antrag zusätzlich die - allenfalls erneute - Reaktion auf das Auskunftsbegehren nach § 26 Abs. 4, 5 oder 10 in jenem Umfang aufzutragen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen. Soweit sich die Beschwerde als nicht berechtigt erweist, ist sie abzuweisen. (8) Ein Beschwerdegegner, gegen den wegen Verletzung in Rechten nach den