Textgegenüberstellung

Geltende Fassung	Vorgeschlagene Fassung
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.** (1) Jede natürliche Person hat Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten. Der Anspruch besteht nicht, wenn Daten allgemein verfügbar sind.
(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) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse einer Person oder mit Zustimmung des Betroffenen erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen zulässig. Staatliche Beschränkungen dürfen nur auf Grund von Gesetzen erfolgen, 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 zulässige Beschränkungen dürfen nur in der gelindesten zum Ziel führenden Art vorgenommen werden.
(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, d.h. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen 1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden; 2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.	(3) Jede natürliche Person hat, soweit sie betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, d.h. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen 1. das Recht auf Auskunft darüber, wer welche Daten über sie verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden; 2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.
(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.	Beschränkungen dieser Rechte sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.
(5) Gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, ist, soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen. In allen übrigen Fällen ist die Datenschutzkommission zur Entscheidung	(4) Gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, ist, soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen. In allen übrigen Fällen ist die Datenschutzkommission zur Entscheidung

Geltende Fassung	Vorgeschlagene Fassung
zuständig, es sei denn, daß Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind.	zuständig, es sei denn, dass Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind.“
Zuständigkeit	**Zuständigkeit**
§ 2. (1) Bundessache ist die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr.	„**§ 2.** Bundessache ist die Gesetzgebung und die Vollziehung in Angelegenheiten des Schutzes personenbezogener Daten.
(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 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.	**§ 3.** (1) Die Bestimmungen dieses Bundesgesetzes sind auf die Verwendung von 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)…
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	4. .Auftraggeber: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate

Geltende Fassung	Vorgeschlagene Fassung
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 Werkes Betraute als datenschutzrechtlicher Auftraggeber;	solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden (Z 8), unabhängig davon, ob sie dies selbst tun oder damit einen Dienstleister (Z 5) beauftragen. Sie gelten auch dann als Auftraggeber, wenn sie einen Dienstleister (Z 5) mit der Herstellung eines Werkes beauftragen und erst dieser die Entscheidung trifft, zu diesem Zweck Daten zu verwenden (Z 8), es sei denn dies wurde dem Dienstleister ausdrücklich untersagt. Die Stellung als Auftraggeber kann sich auch aus Gesetzen, Verordnungen oder Verhaltensregeln (§ 6 Abs. 4) ergeben;“
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);

Geltende Fassung	Vorgeschlagene Fassung
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:…
	(2) Die Regelungen des 2., 3., 5. und 8. Abschnitts dieses Bundesgesetzes gelten mit Ausnahme von § 6 Abs. 1 sowie § 7 Abs. 2 und 3 in Verbindung mit den §§ 8 und 9 nur für Daten, die einer Datenanwendung unterzogen oder in einer Datei verwendet werden. Der 4. Abschnitt gilt für Datenanwendungen und Dateien mit der Maßgabe, dass für ohne Automationsunterstützung geführte Dateien Meldepflicht nur besteht, wenn sie ihrem Inhalt nach gemäß § 18 Abs. 2 der Vorabkontrollpflicht unterliegen. Die Meldung solcher Dateien kann abweichend von § 17 Abs. 1a auch in nicht-elektronischer Form erfolgen. Überall dort, wo in diesen Abschnitten bloß von Datenanwendungen die Rede ist, sind die Regelungen auf Dateien sinngemäß anzuwenden, es sei denn es ist ausdrücklich anderes bestimmt. Wo im 6. Abschnitt von Datenanwendungen die Rede ist, gelten die Bestimmungen sinngemäß für alle Daten. Der 9. und 9a. Abschnitt gilt nur für Datenanwendungen.“
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.
(3) Schutzwürdige Geheimhaltungsinteressen sind aus dem Grunde des Abs. 1 Z 4 insbesondere dann nicht verletzt, wenn die Verwendung der Daten…	(3) Schutzwürdige Geheimhaltungsinteressen sind aus dem Grunde des Abs. 1 Z 4 insbesondere dann nicht verletzt, wenn die Verwendung der Daten…
1. …	1…
2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder	2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung a) zur Amtshilfe oder b) zur Unterstützung des Nationalrates, des Bundesrates oder eines Landtages bei der Ausübung parlamentarischer Kontrolltätigkeit nach Art. 52 bis 53 B-VG oder entsprechenden landesverfassungsrechtlichen Bestimmungen

Geltende Fassung	Vorgeschlagene Fassung
	geschieht
	oder
3. bis 4. ….	3. bis 4. …
5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder	5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist oder
6. bis 7. …	6. bis 7. …
(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 strafbaren Handlungen (Unterlassungen) oder zumindest zur Entgegennahme derartiger Anzeigen zuständige Behörde erfolgt.
Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten	**Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten**
§ 9. Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn	**§ 9.** Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn
1. bis 3 ….	1. bis 3. …
4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht oder	4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung a) zur Amtshilfe oder b) zur Unterstützung des Nationalrates, des Bundesrates oder eines Landtages bei der Ausübung parlamentarischer Kontrolltätigkeit nach Art. 52 bis 53 B–VG oder entsprechenden landesverfassungsrechtlichen Bestimmungen geschieht oder
5. bis 8. …	5. bis 8. …
9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder	9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist oder
10. bis 13. ….	10. bis 13. …
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	**§ 12.** (1) Die Übermittlung und Überlassung von Daten an Empfänger in

Geltende Fassung	Vorgeschlagene Fassung
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.	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 auch hinsichtlich der Datenanwendungen, die sie in Vollziehung der Gesetze durchführen, Parteistellung.	*Der Inhalt wird nunmehr von § 40 Abs. 2 abgedeckt.*
(4) bis (7)…	(4) bis (7)…
	Betrieblicher Datenschutzbeauftragter
	§ 15a. (1) Der Inhaber eines Betriebes (§ 34 Abs. 1 des Arbeitsverfassungsgesetzes - ArbVG, BGBl Nr. 22/1974, § 4 Abs. 1 des Post-Betriebsverfassungsgesetzes – PBVG, BGBl I Nr. 326/1996, § 5 Abs. 1 des Landarbeitsgesetzes 1984 - LAG, BGBl. Nr. 287/1984) mit mehr als 20 Mitarbeitern (wobei Mitarbeiter, die nicht zumindest 20 Stunden pro Woche im Betrieb tätig sind, außer Betracht bleiben) hat einen geeigneten Mitarbeiter zum betrieblichen Datenschutzbeauftragten zu bestellen.
	(2) Der Inhaber hat mit dem Betriebsrat, wenn ein Betriebsausschuss errichtet ist, mit diesem, die beabsichtigte Bestellung oder Abberufung des Datenschutzbeauftragten zu beraten. Eine ohne Beratung vorgenommene Bestellung ist rechtsunwirksam. Die Bestellung bedarf auch der zivilrechtlichen Zustimmung des bestellten Mitarbeiters. Stimmt kein geeigneter Mitarbeiter der Bestellung zu, ist eine geeignete betriebsfremde Person oder ein geeignetes Unternehmen zu bestellen.
	(3) Der betriebliche Datenschutzbeauftragte hat die Einhaltung der Vorschriften dieses Bundesgesetzes im Betrieb zu überwachen und den Betriebsinhaber, die Arbeitnehmer und den Betriebsrat in Belangen des Datenschutzes zu beraten. Er ist vom Inhaber über Vorhaben, neue Datenanwendungen einzusetzen, rechtzeitig zu unterrichten. Wird ihm ein Verdacht einer Verletzung datenschutzrechtlicher Vorschriften bekannt, hat er auf die Herstellung eines rechtmäßigen Zustandes hinzuwirken. Ist ihm dies aus Eigenem nicht möglich, hat er den Betriebsinhaber von dem Verdacht in Kenntnis zu setzen.
	(4) Für Beratungen durch den Datenschutzbeauftragten nach Abs. 3 hat der Inhaber Mitarbeitern, die mit der Verwendung von Daten betraut sind, im ersten Dienstjahr

Geltende Fassung	Vorgeschlagene Fassung
	Arbeitszeit im Umfang von zumindest acht Stunden, in folgenden Dienstjahren im Ausmaß von zumindest vier Stunden pro Jahr zur Verfügung zu stellen. Dem betrieblichen Datenschutzbeauftragten selbst sind im ersten Jahr seiner ununterbrochenen Tätigkeit zumindest 40 Stunden und in jedem folgenden Jahr zumindest 20 Stunden an Arbeitszeit zum Erwerb von Fachkenntnissen und zur Weiterbildung auf dem Gebiet des Datenschutzes zur Verfügung zu stellen.
	(5) Der betriebliche Datenschutzbeauftragte ist in Ausübung dieser Funktion nicht an Weisungen des Betriebsinhabers gebunden. Er hat aber datenschutzbezogene Anregungen des Betriebsinhabers dennoch entgegenzunehmen und gegebenenfalls zu begründen, warum er diese nicht unterstützt. Im Hinblick auf den Kündigungs- und Entlassungsschutz ist der betriebliche Datenschutzbeauftragte einer Sicherheitsfachkraft (§ 73 Abs. 1 des ArbeitnehmerInnenschutzgesetzes, BGBl Nr. 450/1994) gleichgestellt.
	(6) Die Bestellung des betrieblichen Datenschutzbeauftragten lässt die Verantwortung des Betriebsinhabers für die Einhaltung der Bestimmungen dieses Bundesgesetzes unberührt.
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).
	(1a) Die Meldung ist in elektronischer Form im Wege der vom Bundeskanzler bereit zu stellenden Internetanwendung einzubringen. Identifizierung und Authentifizierung haben mit der Bürgerkarte (§ 2 Z 10 des E-Government-Gesetzes,

Geltende Fassung	Vorgeschlagene Fassung
	BGBl. I Nr. 10/2004) zu erfolgen.
§ 18. (1) Der Vollbetrieb einer meldepflichtigen Datenanwendung darf - außer in den Fällen des Abs. 2 - unmittelbar nach Abgabe der Meldung aufgenommen werden.	(1b) Der Betrieb einer meldepflichtigen Datenanwendung darf erst nach ihrer Registrierung aufgenommen werden. Ebenso dürfen Änderungen einer gemeldeten Datenanwendung erst nach Registrierung der entsprechenden Änderungsmeldung in Betrieb genommen werden.
§ 17. (2) und (3)…	(2) und (3)….
Aufnahme der Verarbeitung	**Vorabkontrollpflichtige Datenanwendungen**
§ 18. (1) *s. nach § 17 (1)*	
(2) Meldepflichtige Datenanwendungen, die weder einer Musteranwendung nach § 19 Abs. 2 entsprechen, noch innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften noch die Verwendung von Daten im Katastrophenfall für die in § 48a Abs. 1 genannten Zwecke betreffen, dürfen, wenn sie 1. sensible Daten enthalten oder 2. strafrechtlich relevante Daten im Sinne des § 8 Abs. 4 enthalten oder 3. die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder 4. in Form eines Informationsverbundsystems durchgeführt werden sollen, erst nach ihrer Prüfung (Vorabkontrolle) durch die Datenschutzkommission nach den näheren Bestimmungen des § 20 aufgenommen werden.	**§ 18.** Meldepflichtige Datenanwendungen, die weder einer Musteranwendung nach § 19 Abs. 2 entsprechen, noch innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften noch die Verwendung von Daten im Katastrophenfall für die in § 48a Abs. 1 genannten Zwecke betreffen, sind vor ihrer Registrierung einer inhaltlichen Kontrolle auf Mangelhaftigkeit im Sinne des § 19 Abs. 3 (Vorabkontrolle) zu unterziehen, wenn sie 1. sensible Daten enthalten oder 2. strafrechtlich relevante Daten im Sinne des § 8 Abs. 4 enthalten oder 3. die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder 4. in Form eines Informationsverbundsystems durchgeführt werden.
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…. 8. eine Erklärung, ob die Datenanwendung für Zwecke eines Betriebes mit mehr als 20 Mitarbeitern betrieben werden soll und gegebenenfalls, wer in diesem Betrieb zum betrieblichen Datenschutzbeauftragten (§ 15a) bestellt wurde.“
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.	**§ 20.** (1) Meldungen von Datenanwendungen, die nach Angabe des Auftraggebers nicht einen der Tatbestände des § 18 Z 1 bis 4 erfüllen, sind, sind nur automationsunterstützt im Rahmen der Internetanwendung (§ 17 Abs. 1a) auf ihre Vollständigkeit und Plausibilität zu prüfen. Ergibt diese Prüfung keine Fehlermeldung, so ist die Meldung sofort zu registrieren.

Geltende Fassung	Vorgeschlagene Fassung
(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.	(2) Ergibt die Prüfung nach Abs. 1 Fehler, so ist dem Auftraggeber sogleich die Möglichkeit zur Verbesserung einzuräumen. Erfolgt diese nicht und besteht der Auftraggeber dennoch auf der Einbringung der Meldung, so ist diese von der Datenschutzkommission auf Mangelhaftigkeit im Sinne des § 19 Abs. 3 zu prüfen.
	(3) Meldungen, die der Auftraggeber als vorabkontrollpflichtig bezeichnet hat, sind jedenfalls auf Mangelhaftigkeit im Sinne 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 Fristablauf (Abs. 4) erstattete Verbesserungen sind nicht zu berücksichtigen.
§ 20. (2) Liegt wegen wesentlicher Gefährdung schutzwürdiger 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.	*Diese Bestimmungen entfallen. Zum bisherigen Abs. 2 s. § 30 Abs. 6a, Abs. 3 entfällt ersatzlos, der Inhalt von Abs. 5 ist weiterhin durch § 21 Abs. 1 Z 2 abgedeckt, Abs. 6 wird durch § 40 Abs. 2 abgedeckt.*
(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.	

Geltende Fassung	Vorgeschlagene Fassung
Registrierung	**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.	**§ 21.** (1) Meldungen gemäß § 19 sind in das Datenverarbeitungsregister einzutragen, wenn 1. das Prüfungsverfahren nach § 20 Abs. 1 nicht zu einer Fehlermeldung geführt hat ergeben hat oder 2. das Prüfungsverfahren nach § 20 Abs. 2 keine Mangelhaftigkeit der Meldung ergeben hat oder 3. zwei Monate nach Einlangen einer Meldung (§ 20 Abs. 2 oder 3) bei der Datenschutzkommission verstrichen sind, ohne dass ein Verbesserungsauftrag gemäß § 20 Abs. 4 erteilt wurde oder 4. der Auftraggeber die verlangten 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 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.	(2) Bei Datenanwendungen, die gemäß § 18 Abs. 2 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) Dem Auftraggeber ist die Durchführung der Registrierung schriftlich in Form eines Registerauszuges mitzuteilen.	(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.	(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	**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	(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

Geltende Fassung	Vorgeschlagene Fassung
die Streichung aus dem Register anzuordnen.	wegen aus dem Register zu streichen. Außerdem ist eine registrierte Datenanwendung zu streichen, wenn der Datenschutzkommission zur Kenntnis gelangt, dass eine registrierte Datenanwendung 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) Registrierte Meldungen können von der Datenschutzkommission jederzeit auf Mangelhaftigkeit im Sinne des § 19 Abs. 3 geprüft werden. Entsteht bei der Prüfung der Verdacht tatsächlicher Mangelhaftigkeit, ist ein Berichtigungsverfahren nach Abs. 2 durchzuführen.
	(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 wegen der Verwaltungsübertretung nach § 52 Abs. 2 Z 1 an die zuständige Behörde zu erstatten.

Geltende Fassung	Vorgeschlagene Fassung
	(5) Ergibt das Verfahren nach Abs. 2 alleine – oder allenfalls in Kombination mit einem Mangel nach Abs. 6 -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) Ergibt das Verfahren nach Abs. 2 alleine – oder allenfalls in Kombination mit Mängeln nach Abs. 5 -, dass ein Betriebsinhaber entgegen § 15a keinen oder keinen geeigneten betrieblichen Datenschutzbeauftragten bestellt hat, so ist die Bestellung mit Bescheid aufzutragen.
	(7) 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.
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 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.	**§ 26.** (1) Ein Auftraggeber hat jeder natürlichen Person Auskunft über die zu dieser Person verarbeiteten Daten zu geben, wenn sie dies schriftlich verlangt und ihre 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 anzuführen. Auf Verlangen eines Betroffenen sind auch Namen und Adresse 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

Geltende Fassung	Vorgeschlagene Fassung
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 Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.	(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 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	(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

Geltende Fassung	Vorgeschlagene Fassung
Datenschutzkommission bis zum rechtskräftigen Abschluß des Verfahrens nicht vernichten.	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 natürliche Person 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.
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.

Geltende Fassung	Vorgeschlagene Fassung
Kontrollbefugnisse der Datenschutzkommission	**Kontrollbefugnisse der Datenschutzkommission**
§ 30. (1)…	**§ 30.** (1)…
	(1a) Ein betrieblicher Datenschutzbeauftragter kann sich wegen des Verdachts der Verletzung datenschutzrechtlicher Vorschriften im Betrieb mit einer Eingabe an die Datenschutzkommission wenden, nachdem er den Betriebsinhaber von dem Verdacht in Kenntnis gesetzt hat, dieser jedoch in angemessener Frist keine geeigneten Maßnahmen zur Beseitigung des vermuteten rechtswidrigen Zustandes getroffen hat.
(2)…	(2)…
	(2a) Sofern sich eine zulässigen 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 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	(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,

Geltende Fassung	Vorgeschlagene Fassung
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.	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.
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 natürlichen Personen, die behaupten, in ihrem Recht auf Auskunft nach § 26, auf Darlegung einer automatisierten Einzelentscheidung nach § 49 Abs. 3 oder auf Bekanntgabe eines Betreibers nach § 50 Abs. 1 dritter Satz verletzt zu sein, soweit sich das Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) nicht auf die Verwendung von Daten für Akte 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 gegen einen Auftraggeber des öffentlichen Bereichs richtet, der nicht als Organ der Gesetzgebung oder der Gerichtsbarkeit tätig ist.	(2) Die Datenschutzkommission erkennt weiters über Beschwerden von natürlichen 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 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,

Geltende Fassung	Vorgeschlagene Fassung
	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 §§ 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

Geltende Fassung	Vorgeschlagene Fassung
	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.
	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.
§ 31. (3) Bei Gefahr im Verzug kann die Datenschutzkommission im Zuge der Behandlung einer Beschwerde nach Abs. 2 die weitere Verwendung von Daten zur Gänze oder teilweise untersagen oder auch - bei Streitigkeiten über die Richtigkeit von Daten - dem Auftraggeber die Anbringung eines Bestreitungsvermerks auftragen.	(2) Ist in einem Verfahren nach § 31 Abs. 2 über die Richtigkeit von Daten strittig, so ist vom Beschwerdegegner bis zum Abschluss des Verfahrens ein Bestreitungsvermerk anzubringen. Erforderlichenfalls hat dies die Datenschutzkommission 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.	(3) 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.
Anrufung der Gerichte	**Anrufung der Gerichte**
§ 32. (1) Ansprüche gegen Auftraggeber des privaten Bereichs wegen Verletzung der Rechte des Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung sind vom Betroffenen auf dem Zivilrechtsweg geltend zu machen.	**§ 32.** (1) Ansprüche wegen Verletzung der Rechte einer natürlichen 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.

Geltende Fassung	Vorgeschlagene Fassung
(2) bis (3) …	(2) bis (3) …
(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 Betroffene seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen des Betroffenen können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Auftraggeber oder der Dienstleister seinen gewöhnlichen Aufenthalt oder Sitz hat.	(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 seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen des Betroffenen können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz oder eine Niederlassung hat.
(5) …	(5) …
(6) Die Datenschutzkommission hat, wenn ein Betroffener es verlangt und es zur Wahrung der nach diesem Bundesgesetz geschützten Interessen einer größeren Zahl von Betroffenen geboten ist, einem Rechtsstreit auf Seiten des Betroffenen als Nebenintervenient (§§ 17 ff ZPO) beizutreten.	(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 Betroffenen als Nebenintervenient (§§ 17 ff ZPO) beizutreten.
	(7) Anlässlich einer zulässigen Klage nach Abs. 1, die sich auf eine nach Ansicht des Gerichts meldepflichtige Datenanwendung bezieht, hat das Gericht bei der Datenschutzkommission die registrierte Meldung dieser Datenanwendung anzufordern. Erachtet das Gericht die Meldepflicht nach § 17 Abs. 1 als nicht erfüllt, so hat es dies begründet der Datenschutzkommission mitzuteilen, die erforderlichenfalls nach den §§ 22 und § 22a vorgeht.
Gemeinsame Bestimmungen	**Gemeinsame Bestimmungen**
§ 34. (1) Der Anspruch auf Behandlung einer Eingabe nach § 30, einer Beschwerde nach § 31 oder einer Klage nach § 32 erlischt, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behauptetermaßen stattgefunden hat, einbringt. Dies ist dem Einschreiter im Falle einer verspäteten Eingabe gemäß § 30 mitzuteilen; verspätete Beschwerden nach § 31 und Klagen nach § 32 sind abzuweisen.	**§ 34.** (1) Der Anspruch auf Behandlung einer Eingabe nach § 30, einer Beschwerde nach § 31 oder einer Klage nach § 32 erlischt, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behauptetermaßen stattgefunden hat, einbringt. Dies ist dem Einschreiter im Falle einer verspäteten Eingabe gemäß § 30 mitzuteilen; verspätete Beschwerden nach § 31 und Klagen nach § 32 sind zurückzuweisen.
(2) …	(2) …
(3) Ist die vermutete Verletzung schutzwürdiger Geheimhaltungsinteressen eines Betroffenen im Inland gemäß § 3 nach der Rechtsordnung eines anderen Mitgliedstaats der Europäischen Union zu beurteilen, so kann die Datenschutzkommission im Falle ihrer Befassung die zuständige ausländische Datenschutzkontrollstelle um Unterstützung ersuchen.	(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.“
(4) Die Datenschutzkommission hat den Unabhängigen Datenschutzkontrollstellen der anderen Mitgliedstaaten der Europäischen Union über Ersuchen Amtshilfe zu leisten.	(4) Die Datenschutzkommission hat den Unabhängigen Datenschutzkontrollstellen der anderen Vertragsstaaten des Europäischen Wirtschaftsraumes über Ersuchen Amtshilfe zu leisten.

Geltende Fassung	Vorgeschlagene Fassung
Zusammensetzung der Datenschutzkommission	**Zusammensetzung der Datenschutzkommission**
§ 36. (1) bis (2) …	**§ 36.** (1) bis (2) …
(3) Ein Mitglied ist aus dem Kreise der rechtskundigen Bundesbeamten vorzuschlagen.	(3) Ein Mitglied ist aus dem Kreise der rechtskundigen Bundesbediensteten vorzuschlagen.
	(3a) Die Mitglieder der Datenschutzkommission üben diese Funktion neben ihnen sonst obliegenden beruflichen Tätigkeiten aus.
(4) bis (5) …	(4) bis (5) …
(6) Hat ein Mitglied der Datenschutzkommission Einladungen zu drei aufeinanderfolgenden Sitzungen ohne genügende Entschuldigung keine Folge geleistet oder tritt bei einem Mitglied ein Ausschließungsgrund des Abs. 5 nachträglich ein, so hat dies nach seiner Anhörung die Datenschutzkommission festzustellen. Diese Feststellung hat den Verlust der Mitgliedschaft zur Folge. Im übrigen kann ein Mitglied der Datenschutzkommission nur aus einem schwerwiegenden Grund durch Beschluß der Datenschutzkommission, dem mindestens drei ihrer Mitglieder zustimmen müssen, seines Amtes für verlustig erklärt werden. Die Mitgliedschaft endet auch, wenn das Mitglied seine Funktion durch schriftliche Erklärung an den Bundeskanzler zurücklegt.	(6) Hat ein Mitglied der Datenschutzkommission Einladungen zu drei aufeinanderfolgenden Sitzungen ohne genügende Entschuldigung keine Folge geleistet oder tritt bei einem Mitglied ein Ausschließungsgrund des Abs. 5 nachträglich ein, so hat dies nach seiner Anhörung die Datenschutzkommission festzustellen. Diese Feststellung hat den Verlust der Mitgliedschaft zur Folge. Im übrigen kann ein Mitglied der Datenschutzkommission nur aus einem schwerwiegenden Grund durch Beschluß der Datenschutzkommission, dem mindestens drei ihrer Mitglieder zustimmen müssen, seines Amtes für verlustig erklärt werden. Die Mitgliedschaft endet auch, wenn das Mitglied seine Funktion durch schriftliche Erklärung an den Bundeskanzler zurücklegt. 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 Richterdienstgesetzes, BGBl Nr. 305/1961, gleich. Die Mitgliedschaft der übrigen Mitglieder endet am 31. Dezember des Jahres, in dem sie das 65. Lebensjahr vollenden.
(7) bis (8) ….	(7) bis (8) ….
(9) Die Mitglieder und Ersatzmitglieder der Datenschutzkommission haben Anspruch auf Ersatz der Reisekosten (Gebührenstufe 3) nach Maßgabe der für Bundesbeamte geltenden Rechtsvorschriften. Sie haben ferner Anspruch auf eine dem Zeit- und Arbeitsaufwand entsprechende Vergütung, die auf Antrag des Bundeskanzlers von der Bundesregierung durch Verordnung festzusetzen ist.	(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 dem Zeit und Arbeitsaufwand entsprechende Vergütung, die auf Antrag des Bundeskanzlers von der Bundesregierung durch Verordnung festzusetzen ist.
Organisation und Geschäftsführung der Datenschutzkommission	**Organisation und Geschäftsführung der Datenschutzkommission**
§ 38. (1) **(Verfassungsbestimmung)** 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 im	**§ 38.** (1) **(Verfassungsbestimmung)** 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 im

Geltende Fassung	Vorgeschlagene Fassung
Registrierungsverfahren gemäß § 20 Abs. 2 oder § 22 Abs. 3. Inwieweit einzelne fachlich geeignete Bedienstete der Geschäftsstelle der Datenschutzkommission zum Handeln für die Datenschutzkommission oder das geschäftsführende Mitglied ermächtigt werden, bestimmt die Geschäftsordnung.	Registrierungsverfahren gemäß § 22 Abs. 3 oder § 30 Abs. 6a. Inwieweit einzelne fachlich geeignete Bedienstete der Geschäftsstelle der Datenschutzkommission zum Handeln für die Datenschutzkommission oder das geschäftsführende Mitglied ermächtigt werden, bestimmt die Geschäftsordnung.
Beschlüsse der Datenschutzkommission	**Beschlüsse der Datenschutzkommission**
§ 39. (1) bis (4) …	**§ 39.** (1) bis (4) …
	(5) Beschlüsse der Datenschutzkommission werden vom Vorsitzenden ausgefertigt.
Wirkung von Bescheiden der Datenschutzkommission und des geschäftsführenden Mitglieds	**Wirkung von Bescheiden der Datenschutzkommission und des geschäftsführenden Mitglieds**
§ 40. (1) Gegen Bescheide, die das geschäftsführende Mitglied der Datenschutzkommission gemäß § 20 Abs. 2 oder § 22 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.	**§ 40**. (1) Gegen Bescheide, die das geschäftsführende Mitglied der Datenschutzkommission gemäß § 22 Abs. 3 oder gemäß § 30 Abs. 6a 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. Die Anrufung des Verwaltungsgerichtshofes durch die Parteien des Verfahrens ist außer in den Fällen des Abs. 1 zulässig. Dies gilt auch für die in Vollziehung der Gesetze tätigen Auftraggeber des öffentlichen Bereichs in jenen Fällen, in welchen ihnen gemäß § 13 Abs. 3 oder § 20 Abs. 6 Parteistellung zukommt oder durch Gesetz ausdrücklich ein Beschwerderecht an den Verwaltungsgerichtshof eingeräumt wurde.	(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.
(3) und (4)…	(3) und (4)…
Zusammensetzung des Datenschutzrates	**Zusammensetzung des Datenschutzrates**
§ 42. (1) Dem Datenschutzrat gehören an:	**§ 42.** (1) Dem Datenschutzrat gehören an:
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. Bei Mandatsgleichheit der beiden im Nationalrat am stärksten vertretenen Parteien entsendet jede dieser Parteien drei Vertreter;	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;
2. bis 5. …	2. bis 5. …
(2) bis (4) …	(2) bis (4) …

Geltende Fassung	Vorgeschlagene Fassung
(5) Die Mitglieder gehören dem Datenschutzrat solange an, bis sie dem Bundeskanzler schriftlich ihr Ausscheiden mitteilen oder, mangels einer solchen Mitteilung, von der entsendenden Stelle (Abs. 1) dem Bundeskanzler ein anderer Vertreter namhaft gemacht wird.	(5) Die Mitglieder gehören dem Datenschutzrat solange an, bis sie dem Bundeskanzler schriftlich ihr Ausscheiden mitteilen oder, mangels einer solchen Mitteilung, von der entsendenden Stelle (Abs. 1) dem Bundeskanzler ein anderer Vertreter namhaft gemacht wird. Mitglieder nach Abs. 1 Z 1 scheiden außerdem aus, sobald der Hauptausschuss nach den §§ 29 f des Geschäftsordnungsgesetzes 1975, BGBl Nr. 410, neu gewählt wurde, und sie nicht neuerlich entsendet werden.
(6) …	(6) …
Wissenschaftliche Forschung und Statistik	**Wissenschaftliche Forschung und Statistik**
§ 46. (1) Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Auftraggeber der Untersuchung alle Daten verwenden, die 1. öffentlich zugänglich sind oder 2. der Auftraggeber für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder 3. für den Auftraggeber nur indirekt personenbezogen sind. Andere Daten dürfen nur unter den Voraussetzungen des Abs. 2 Z 1 bis 3 verwendet werden.	**§ 46.** (1) Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Auftraggeber der Untersuchung alle Daten verwenden, die 1. öffentlich zugänglich sind oder 2. er für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder 3. für ihn nur indirekt personenbezogen sind. Andere Daten dürfen nur unter den Voraussetzungen des Abs. 2 Z 1 bis 3 verwendet werden.
(2) Bei Datenanwendungen für Zwecke wissenschaftlicher Forschung und Statistik, die nicht unter Abs. 1 fallen, dürfen Daten, die nicht öffentlich zugänglich sind, nur 1. gemäß besonderen gesetzlichen Vorschriften oder 2. mit Zustimmung des Betroffenen oder 3. mit Genehmigung der Datenschutzkommission gemäß Abs. 3 verwendet werden.	(2) Bei Datenanwendungen für Zwecke wissenschaftlicher Forschung und Statistik, die nicht unter Abs. 1 fallen, dürfen Daten nur 1. gemäß besonderen gesetzlichen Vorschriften oder 2. mit Zustimmung des Betroffenen oder 3. mit Genehmigung der Datenschutzkommission gemäß Abs. 3 verwendet werden.
(3) Eine Genehmigung der Datenschutzkommission für die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik ist zu erteilen, wenn 1. die Einholung der Zustimmung der Betroffenen mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet und 2. ein öffentliches Interesse an der beantragten Verwendung besteht und 3. die fachliche Eignung des Antragstellers glaubhaft gemacht wird. Sollen sensible Daten übermittelt werden, muss ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muss gewährleistet sein, dass die Daten beim Empfänger nur von Personen verwendet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verläßlichkeit sonst glaubhaft ist. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies	(3) Eine Genehmigung der Datenschutzkommission für die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik ist auf Antrag des Auftraggebers der Untersuchung zu erteilen, wenn 1. die Einholung der Zustimmung der Betroffenen mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet und 2. ein öffentliches Interesse an der beantragten Verwendung besteht und 3. die fachliche Eignung des Antragstellers glaubhaft gemacht wird. Sollen sensible Daten ermittelt werden, muss ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muss gewährleistet sein, dass die Daten beim Auftraggeber der Untersuchung nur von Personen verwendet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verläßlichkeit sonst glaubhaft ist. Die

Geltende Fassung	Vorgeschlagene Fassung
zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten, notwendig ist.	Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten, notwendig ist.
	(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 EO) vorgelegt werden.
(4) bis (5) …	(4) bis (5) …
Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen	**Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen**
§ 47. (1) bis (3) …	**§ 47.** (1) bis (3) …
(4) Die Datenschutzkommission hat die Genehmigung zur Übermittlung zu erteilen, wenn der Antragsteller das Vorliegen der in Abs. 3 genannten Voraussetzungen glaubhaft macht und überwiegende schutzwürdige Geheimhaltungsinteressen der Betroffenen der Übermittlung nicht entgegenstehen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten als Auswahlkriterium, notwendig ist.	(4) Die Datenschutzkommission hat auf Antrag eines Auftraggebers, der Adressdaten verarbeitet, die Genehmigung zur Übermittlung zu erteilen, wenn der Antragsteller das Vorliegen der in Abs. 3 genannten Voraussetzungen glaubhaft macht und überwiegende schutzwürdige Geheimhaltungsinteressen der Betroffenen der Übermittlung nicht entgegenstehen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten als Auswahlkriterium, notwendig ist.
(5) bis (6) …	(5) bis (6) …
Automatisierte Einzelentscheidungen	**Automatisierte Einzelentscheidungen**
§ 49. (1) bis (2) …	**§ 49.** (1) bis (2) …
(3) Dem Betroffenen ist bei automatisierten Einzelentscheidungen auf Antrag der logische Ablauf der automatisierten Entscheidungsfindung in allgemein verständlicher Form darzulegen.	(3) Dem Betroffenen ist bei automatisierten Einzelentscheidungen auf Antrag der logische Ablauf der automatisierten Entscheidungsfindung in allgemein verständlicher Form darzulegen. § 26 Abs. 2 bis 10 gilt sinngemäß.
Informationsverbundsysteme	**Informationsverbundsysteme**
§ 50. (1) Die Auftraggeber eines Informationsverbundsystems haben, soweit dies nicht bereits durch Gesetz geregelt ist, einen geeigneten Betreiber für das System zu bestellen. Name (Bezeichnung) und Anschrift des Betreibers sind in der Meldung zwecks Eintragung in das Datenverarbeitungsregister bekannt zu geben. Unbeschadet des Rechtes des Betroffenen auf Auskunft nach § 26 hat der Betreiber jedem Betroffenen auf Antrag binnen zwölf Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen	**§ 50.** (1) Die Auftraggeber eines Informationsverbundsystems haben, soweit dies nicht bereits durch Gesetz geregelt ist, einen geeigneten Betreiber für das System zu bestellen. Name (Bezeichnung) und Anschrift des Betreibers sind in der Meldung zwecks Eintragung in das Datenverarbeitungsregister bekannt zu geben. Unbeschadet des Rechtes des Betroffenen auf Auskunft nach § 26 hat der Betreiber jedem Betroffenen auf Antrag binnen zwölf Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen

Geltende Fassung	Vorgeschlagene Fassung
Auftraggeber festzustellen; in Fällen, in welchen der Auftraggeber gemäß § 26 Abs. 5 vorzugehen hätte, hat der Betreiber mitzuteilen, dass kein der Pflicht zur Auskunftserteilung unterliegender Auftraggeber benannt werden kann. Die Unterstützungspflicht des Betreibers gilt auch bei Anfragen von Behörden. Den Betreiber trifft überdies die Verantwortung für die notwendigen Maßnahmen der Datensicherheit (§ 14) im Informationsverbundsystem. Von der Haftung für diese Verantwortung kann sich der Betreiber unter den gleichen Voraussetzungen, wie sie in § 33 Abs. 3 vorgesehen sind, befreien. Wird ein Informationsverbundsystem geführt, ohne dass eine entsprechende Meldung an die Datenschutzkommission unter Angabe eines Betreibers erfolgt ist, treffen jeden einzelnen Auftraggeber die Pflichten des Betreibers.	Auftraggeber festzustellen; in Fällen, in welchen der Auftraggeber gemäß § 26 Abs. 5 vorzugehen hätte, hat der Betreiber mitzuteilen, dass kein der Pflicht zur Auskunftserteilung unterliegender Auftraggeber benannt werden kann. Abgesehen von der abweichenden Frist gilt § 26 Abs. 3 bis 10 sinngemäß. Die Unterstützungspflicht des Betreibers gilt auch bei Anfragen von Behörden. Den Betreiber trifft überdies die Verantwortung für die notwendigen Maßnahmen der Datensicherheit (§ 14) im Informationsverbundsystem. Von der Haftung für diese Verantwortung kann sich der Betreiber unter den gleichen Voraussetzungen, wie sie in § 33 Abs. 3 vorgesehen sind, befreien. Wird ein Informationsverbundsystem geführt, ohne dass eine entsprechende Meldung an die Datenschutzkommission unter Angabe eines Betreibers erfolgt ist, treffen jeden einzelnen Auftraggeber die Pflichten des Betreibers.
(2) Durch entsprechenden Rechtsakt können auch weitere Auftraggeberpflichten auf den Betreiber übertragen werden. Soweit dies nicht durch Gesetz geschehen ist, ist dieser Pflichtenübergang gegenüber den Betroffenen und den für die Vollziehung dieses Bundesgesetzes zuständigen Behörden nur wirksam, wenn er - auf Grund einer entsprechenden Meldung an die Datenschutzkommission - aus der Registrierung im Datenverarbeitungsregister ersichtlich ist.	(2) Durch entsprechenden Rechtsakt können auch weitere Auftraggeberpflichten, insbesondere auch die Vornahme der Meldung des Informationsverbundsystems, auf den Betreiber übertragen werden. Soweit dies nicht durch Gesetz geschehen ist, ist dieser Pflichtenübergang gegenüber Dritten nur wirksam, wenn er – auf Grund einer entsprechenden Meldung an die Datenschutzkommission – aus der Registrierung im Datenverarbeitungsregister ersichtlich ist.
	(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. 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.
(3)…	(3)…
	9a. Abschnitt **Videoüberwachung**
	Allgemeines
	§ 50a. (1) Videoüberwachung bezeichnet die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt („überwachtes Objekt“) betreffen, durch technische Bildaufnahmegeräte. Für derartige Überwachungen gelten die folgenden Absätze, sofern nicht durch andere Gesetze Besonderes bestimmt ist.

Geltende Fassung

Vorgeschlagene Fassung

(2) Videoüberwachung sowie die Auswertung und Übermittlung der dabei ermittelten Daten darf vorbehaltlich des Abs. 5 nur zum Schutz der überwachten Objekte oder zur Beweissicherung im Hinblick auf Ereignisse nach Abs. 1 erfolgen.

(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, oder
4. sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte Objekt betreffenden Ereignisse erschöpft, diese also weder gespeichert (aufgezeichnet) noch in sonst einer anderen Form weiterverarbeitet werden, und sie zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt, oder
5. bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt könnte das Ziel oder der Ort eines gefährlichen Angriffes im Sinn von § 16 Abs. 1 Z 1 des Sicherheitspolizeigesetzes (SPG), BGBl. Nr. 566/1991 in der jeweils geltenden Fassung, werden. Als bestimmte Tatsache ist es insbesondere anzusehen, wenn
   a) das überwachte Objekt bereits einmal Ziel oder Ort eines gefährlichen Angriffs war und eine Wiederholung wahrscheinlich ist. Zu berücksichtigen sind jedenfalls nur gefährliche Angriffe, die sich innerhalb der vergangenen zehn Jahre ereignet haben. Ist für die dem gefährlichen Angriff zu Grunde liegende gerichtlich strafbare Handlung (§ 16 Abs. 2 SPG) nach § 57 des Strafgesetzbuches (StGB), BGBl Nr. 60/1974 in der jeweils geltenden Fassung, eine kürzere Verjährungsfrist vorgesehen, so sind nur gefährliche Angriffe innerhalb dieser Frist relevant. § 58 StGB hat dabei außer Betracht zu bleiben, oder
   b) das überwachte Objekt eine Person mit überdurchschnittlichem Bekanntheitsgrad in der Öffentlichkeit oder ein Aufenthaltsort einer derartigen Person ist, oder
   c) das überwachte Objekt ein verfassungsmäßiges Organ oder dessen Aufenthaltsort ist, oder
   d) das überwachte Objekt ein beweglicher Gegenstand mit Geldwert von mehr als EUR 100.000,-- oder ein Aufenthaltsort derartiger Gegenstände ist, oder

Geltende Fassung

Vorgeschlagene Fassung

e) das überwachte Objekt ein Gegenstand von überdurchschnittlichem künstlerischem Wert ist,

oder

6. unmittelbar anwendbare Rechtsvorschriften des Völker- oder des Gemeinschaftsrechts, Gesetze, Verordnungen, Bescheide oder gerichtliche Entscheidungen dem Auftraggeber spezielle Sorgfaltspflichten zum Schutz der überwachten Objekte auferlegen, oder
7. die Videoüberwachung zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche des Auftraggebers vor einem Gericht im Sinn von Art. 234 EGV erforderlich ist.

(4) Abs. 3 Z 4 bis 7 sind für Auftraggeber des öffentlichen Bereichs bei Wahrnehmung ihrer hoheitlichen Aufgaben nicht anwendbar. Außerdem dürfen mit einer Videoüberwachung nach Abs. 3 Z 4 bis 7 nicht Ereignisse an Orten festgestellt werden, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen.

(5) Schutzwürdige Geheimhaltungsinteressen Betroffener sind auch dann nicht verletzt, wenn durch Videoüberwachung aufgezeichnete Daten über eine Verwendung entsprechend den Abs. 2 und 3 hinaus an die zuständige Behörde oder das zuständige Gericht übermittelt werden, weil beim Auftraggeber der begründete Verdacht entstanden ist, die Daten könnten

1. eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren, oder
2. der Abwehr oder Beendigung eines gefährlichen Angriffs dienen,

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.

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

(7) Im Übrigen gelten auch für Videoüberwachung die §§ 6 und 7, insbesondere der Verhältnismäßigkeitsgrundsatz (§ 7 Abs. 3).

Besondere Protokollierungs- und Löschungspflicht

§ 50b. (1) Jeder Verwendungsvorgang einer Videoüberwachung ist zu protokollieren.

(2) Aufgezeichnete Daten sind, sofern sie nicht aus konkretem Anlass für die Verwirklichung der zu Grunde liegenden Schutz- oder Beweissicherungszwecke oder

Geltende Fassung

Vorgeschlagene Fassung

für Zwecke nach § 50a Abs. 5 benötigt werden, spätestens nach 48 Stunden zu löschen. Die Datenschutzkommission hat auf Antrag des Auftraggebers eine längere Aufbewahrung zu genehmigen, wenn dies aus besonderen Gründen zur Zweckerreichung regelmäßig erforderlich ist. Ein solcher Antrag ist bei meldepflichtigen Videoüberwachungen tunlichst mit der Meldung zu verbinden.

Meldepflicht und Registrierungsverfahren

§ 50c. (1) Eine Videoüberwachung ist über § 17 Abs. 2 hinaus von der Meldepflicht ausgenommen, wenn

1. § 50a Abs. 3 Z 4 erfüllt ist oder
2. eine Speicherung (Aufzeichnung) nur auf einem analogen Speichermedium erfolgt.

(2) Meldepflichtige Überwachungen unterliegen stets der Vorabkontrolle (§ 18 Abs. 2). Bestimmte Tatsachen im Sinn von § 50a Abs. 1 Z 5 und die Anspruchsverfolgung nach § 50a Abs. 1 Z 7 müssen bei Erstattung der Meldung glaubhaft gemacht werden.

(3) Mehrere überwachte Objekte, 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. Die Kennzeichnung hat jedenfalls den Auftraggeber zu benennen und hat örtlich derart zu erfolgen, dass jeder potentiell Betroffene, der sich einem überwachten Objekt nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen.

(2) Die Kennzeichnung kann entfallen,

1. wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte oder der Beschaffenheit des überwachten Objekts, insbesondere dessen Mobilität, einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordern würde, oder
2. im Fall einer Überwachung nach § 50a Abs. 3 Z 7, wenn dadurch die Gewinnung von Beweismitteln zur Anspruchsverfolgung vereitelt würde.

(3) Der beabsichtigte Entfall einer Kennzeichnung nach Abs. 2 ist bei meldepflichtigen Überwachungen in der Meldung an die Datenschutzkommission anzugeben. Wenn diese die Voraussetzungen nicht als gegeben erachtet, hat sie eine

Geltende Fassung	Vorgeschlagene Fassung
	Kennzeichnung mit Bescheid anzuordnen.
	Auskunftsrecht
	§ 50e. (1) Abweichend von § 26 Abs. 1 ist dem Auskunftswerber, nachdem dieser den Zeitraum, in dem er möglicherweise von der Überwachung betroffen war, möglichst präzise 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.
Feststellungen der Europäischen Kommission	**Feststellungen der Europäischen Kommission**
§ 55. Der Inhalt der in einem Verfahren gemäß Art. 31 Abs. 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995, S. 31, getroffenen Feststellungen der Europäischen Kommission über	**§ 55.** Der Inhalt der in einem Verfahren gemäß Art. 31 Abs. 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995, S. 31, getroffenen Feststellungen der Europäischen Kommission über
1. …	1. …
2. die Eignung bestimmter Standardvertragsklauseln oder Verpflichtungserklärungen zur Gewährleistung eines ausreichenden Schutzes der Datenverwendung in einem Drittland ist vom Bundeskanzler im Bundesgesetzblatt gemäß § 2 Abs. 3 BGBlG, BGBl. Nr. 660/1996, kundzumachen.	2. die Eignung bestimmter Standardvertragsklauseln oder Verpflichtungserklärungen zur Gewährleistung eines ausreichenden Schutzes der Datenverwendung in einem Drittland ist vom Bundeskanzler im Bundesgesetzblatt gemäß § 4 des Bundesgesetzblattgesetzes, BGBl. I Nr. 100/2003, kundzumachen.
§ 60. (1) **(Verfassungsbestimmung)** Die Verfassungsbestimmungen des Art. 1, der §§ 35 Abs. 2, 37, 38 Abs. 1 und 61 Abs. 4 und 7 treten mit 1. Jänner 2000 in Kraft. Mit dem Inkrafttreten dieses Bundesgesetzes tritt das Datenschutzgesetz, BGBl. Nr. 565/1978 in der geltenden Fassung, außer Kraft.	„**§ 60.** (1) **(Verfassungsbestimmung)** Die Verfassungsbestimmungen des Art. 1, der §§ 35 Abs. 2, 37, 38 Abs. 1 und 61 Abs. 4 und 7 treten mit 1. Jänner 2000 in Kraft. § 1, § 2, § 3 Abs. 1 und 2 sowie § 38 Abs. 1 in der Fassung der Novelle BGBl I Nr. xxx/2008 treten am 1. Juli 2008 in Kraft.“
(2) bis (3) …	(2) bis (3) …
	„(4) Das Inhaltsverzeichnis, die Überschrift und Absatzgliederung von § 4, § 4

Geltende Fassung	Vorgeschlagene Fassung
	Abs. 1 Z 3 bis 5, § 4 Abs. 1 Z 7 bis 9, § 4 Z 11 und 12, § 4 Abs. 2, § 8 Abs. 1 und 2, § 8 Abs. 3 Z 2 und 5, § 8 Abs. 4, § 9 Z 4 und 9, § 12 Abs. 1, § 16 Abs. 3, § 17 Abs. 1 und 1a, § 18 samt Überschrift, § 19 Abs. 1 Z 3a, die §§ 20 bis 22 samt Überschriften, § 22a Abs. 1 bis 5 samt Überschrift, § 26 Abs. 1 bis 8, § 26 Abs. 10, § 27 Abs. 9, § 28 Abs. 3, § 30 Abs. 2a und Abs. 5 bis 6a, die §§ 31 und 31a samt Überschriften, § 32 Abs. 1, 4, 6 und 7, § 34 Abs. 3 und 4, § 36 Abs. 3, 3a, 6 und 9, § 39 Abs. 5, § 40 Abs. 1 und 2, § 42 Abs. 1 Z 1, § 42 Abs. 5, § 46 Abs. 1 bis 3a, § 47 Abs. 4, § 49 Abs. 3, § 50 Abs. 1 bis 2a, der 9a. Abschnitt sowie § 55 in der Fassung der Novelle BGBl I Nr. xxx/2008 treten am 1. März 2008 in Kraft. Gleichzeitig treten § 4 Abs. 1 Z 10, § 13 Abs. 3 und § 58 außer Kraft.
	(5) § 15a, § 19 Abs. 1 Z 8, § 22a Abs. 6 und § 30 Abs. 1a in der Fassung der Novelle BGBl I Nr. xxx/2008 treten am 1. Juli 2009 in Kraft.
Übergangsbestimmungen	**Übergangsbestimmungen**
§ 61. (1) bis (5) …	**§ 61.** (1) bis (5) …
(6) Die zum Zeitpunkt des Inkrafttretens dieses Gesetzes im Amt befindliche Datenschutzkommission übernimmt für den Zeitraum von sechs Monaten ab Inkrafttreten dieses Gesetzes die Funktion der Datenschutzkommission gemäß § 35.	
	(6) Videoüberwachungen, die vor dem Inkrafttreten der §§ 50a bis 50e registriert wurden, sind bis zum 1. Juli 2010 auch dann rechtmäßig, wenn sie den am 30. Juni 2008 geltenden datenschutzrechtlichen Bestimmungen genügen.
(7)…	(7)…
	(8) Die Angaben zum betrieblichen Datenschutzbeauftragten (§ 19 Abs. 1 Z 8) sind der Datenschutzkommission bei vor dem 1. Juli 2009 registrierten Datenanwendungen anlässlich der ersten über eine Streichung hinausgehenden Änderungsmeldung zu melden, die ab diesem Datum erstattet wird. Eine Meldung allein im Hinblick auf § 19 Abs. 1 Z 8 ist nicht erforderlich.
	(9) Die Verordnung nach § 16 Abs. 3 ist vom Bundeskanzler nach Maßgabe der technischen Möglichkeiten des Datenverarbeitungsregisters bis spätestens zum 1. Jänner 2011 neu zu erlassen. Bis zum Inkrafttreten dieser Verordnung sind die §§ 16 bis 22 sowie § 30 Abs. 6 in der Fassung vor der Novelle BGBl I Nr. xxx/2008 anzuwenden; § 22a, § 30 Abs. 2a und 6a, § 31a Abs. 1 sowie § 32 Abs. 7 sind bis dahin nicht 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), sind 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

Geltende Fassung	Vorgeschlagene Fassung
	wird. Eine Meldung allein im Hinblick auf § 19 Abs. 1 Z 3a ist nicht erforderlich.“
	(10) **(Verfassungsbestimmung)** Bis zur Neuerlassung der Verordnung nach § 16 Abs. 3 ist auch § 38 Abs. 1 in der Fassung vor der Novelle BGBl I Nr. xxx/2008 anzuwenden.“

Entwurf

Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2008)

Der Nationalrat hat beschlossen:

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

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

2. Im Inhaltsverzeichnis wird nach § 15 eingefügt:

§ 15a	Betrieblicher Datenschutzbeauftragter

3. Im Inhaltsverzeichnis lautet § 18:

§ 18	Vorabkontrollpflichtige Datenanwendungen

4. Im Inhaltsverzeichnis lautet § 20:

§ 20	Prüfungs- und Verbesserungsverfahren

5. Im Inhaltsverzeichnis lautet § 22:

§ 22	Richtigstellung des Registers und Rechtsnachfolge

6. Im Inhaltsverzeichnis wird nach § 22 eingefügt:

§ 22a	Verfahren zur Überprüfung der Erfüllung der Meldepflicht

7. Im Inhaltsverzeichnis wird nach § 31 eingefügt:

§ 31a	Begleitende Maßnahmen im Beschwerdeverfahren

8. Im Inhaltsverzeichnis wird nach § 50 eingefügt:

„9a. Abschnitt: Videoüberwachung

§ 50a	Allgemeines
§ 50b	Besondere Protokollierungspflicht
§ 50c	Meldepflicht und Registrierungsverfahren
§ 50d	Information durch Kennzeichnung
§ 50e	Auskunftsrecht“

*10. **(Verfassungsbestimmung)** § 1 samt Überschrift lautet:*

„Grundrecht auf Datenschutz

§ 1. (1) Jede natürliche Person hat Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten. Der Anspruch besteht nicht, wenn Daten allgemein verfügbar sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse einer Person oder mit Zustimmung des Betroffenen erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen zulässig. Staatliche Beschränkungen dürfen nur auf Grund von Gesetzen erfolgen, 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 zulässige Beschränkungen dürfen nur in der gelindesten zum Ziel führenden Art vorgenommen werden.

(3) Jede natürliche Person hat, soweit sie betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, d.h. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über sie verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

Beschränkungen dieser Rechte sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

(4) Gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, ist, soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen. In allen übrigen Fällen ist die Datenschutzkommission zur Entscheidung zuständig, es sei denn, dass Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind.“

*11. **(Verfassungsbestimmung)** § 2 lautet:*

„**§ 2.** Bundessache ist die Gesetzgebung und die Vollziehung in Angelegenheiten des Schutzes personenbezogener Daten.“

*12. **(Verfassungsbestimmung)** In § 3 Abs. 1 wird die Wortfolge* „Mitgliedstaaten der Europäischen Union“ *durch die Wortfolge* „Vertragsstaaten des Europäischen Wirtschaftsraumes“ *ersetzt.*

*13. **(Verfassungsbestimmung)** In § 3 Abs. 2 wird die Wortfolge* „Mitgliedstaat der Europäischen Union“ *durch die Wortfolge* „Vertragsstaat des Europäischen Wirtschaftsraumes“ *ersetzt.*

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

15. § 4 Abs. 1 Z 3 lautet:

„3. Betroffener: jede vom Auftraggeber (Z 4) verschiedene natürliche Person, deren Daten verwendet werden (Z 8);“

16. § 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 dies selbst tun oder damit einen Dienstleister (Z 5) beauftragen. Sie gelten auch dann als Auftraggeber, wenn sie einen Dienstleister (Z 5) mit der Herstellung eines Werkes beauftragen und erst dieser die Entscheidung trifft, zu diesem Zweck Daten zu verwenden (Z 8), es sei denn dies wurde dem Dienstleister ausdrücklich untersagt. Die Stellung als Auftraggeber kann sich auch aus Gesetzen, Verordnungen oder Verhaltensregeln (§ 6 Abs. 4) ergeben;“

17. § 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 Werks verwenden;

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

19. § 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;“

20. § 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.“

21. § 4 Abs. 1 Z 10 wird aufgehoben.

22. § 4 Abs. 1 Z 11 lautet:

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

23. § 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;“

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

„(2) Die Regelungen des 2., 3., 5. und 8. Abschnitts dieses Bundesgesetzes gelten mit Ausnahme von § 6 Abs. 1 sowie § 7 Abs. 2 und 3 in Verbindung mit den §§ 8 und 9 nur für Daten, die einer Datenanwendung unterzogen oder in einer Datei verwendet werden. Der 4. Abschnitt gilt für Datenanwendungen und Dateien mit der Maßgabe, dass für ohne Automationsunterstützung geführte Dateien Meldepflicht nur besteht, wenn sie ihrem Inhalt nach gemäß § 18 Abs. 2 der Vorabkontrollpflicht unterliegen. Die Meldung solcher Dateien kann abweichend von § 17 Abs. 1a auch in nicht-elektronischer Form erfolgen. Überall dort, wo in diesen Abschnitten bloß von Datenanwendungen die Rede ist, sind die Regelungen auf Dateien sinngemäß anzuwenden, es sei denn es ist ausdrücklich anderes bestimmt. Wo im 6. Abschnitt von Datenanwendungen die Rede ist, gelten die Bestimmungen sinngemäß für alle Daten. Der 9. und 9a. Abschnitt gilt nur für Datenanwendungen.“

25. 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.*

26. § 8 Abs. 2 zweiter Satz wird aufgehoben.

27. § 8 Abs. 3 Z 2 lautet:

„2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung

a) zur Amtshilfe oder

b) zur Unterstützung des Nationalrates, des Bundesrates oder eines Landtages bei der Ausübung parlamentarischer Kontrolltätigkeit nach Art. 52 bis 53 B–VG oder entsprechenden landesverfassungsrechtlichen Bestimmungen geschieht

oder“

28. In § 8 Abs. 3 Z 5 entfällt die Wortfolge „ und die Daten rechtmäßig ermittelt wurden“.

29. 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 strafbaren Handlungen (Unterlassungen) oder zumindest zur Entgegennahme derartiger Anzeigen zuständige Behörde erfolgt.“

30. § 9 Z 4 lautet:

„2. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung

a) zur Amtshilfe oder

b) zur Unterstützung des Nationalrates, des Bundesrates oder eines Landtages bei der Ausübung parlamentarischer Kontrolltätigkeit nach Art. 52 bis 53 B–VG oder entsprechenden landesverfassungsrechtlichen Bestimmungen geschieht

oder“

31. In § 9 Z 9 entfällt die Wortfolge „ und die Daten rechtmäßig ermittelt wurden“.

32. In § 12 Abs. 1 erster Satz wird die Wortfolge „Mitgliedstaaten der Europäischen Union“ *durch die Wortfolge* „Vertragsstaaten des Europäischen Wirtschaftsraums (EWR)“ *ersetzt.*

33. § 13 Abs. 3 wird aufgehoben.

34. Nach § 15 wird der folgende § 15a samt Überschrift eingefügt:

„Betrieblicher Datenschutzbeauftragter

§ 15a. (1) Der Inhaber eines Betriebes (§ 34 Abs. 1 des Arbeitsverfassungsgesetzes - ArbVG, BGBl Nr. 22/1974, § 4 Abs. 1 des Post-Betriebsverfassungsgesetzes – PBVG, BGBl I Nr. 326/1996, § 5 Abs. 1 des Landarbeitsgesetzes 1984 - LAG, BGBl. Nr. 287/1984) mit mehr als 20 Mitarbeitern (wobei Mitarbeiter, die nicht zumindest 20 Stunden pro Woche im Betrieb tätig sind, außer Betracht bleiben) hat einen geeigneten Mitarbeiter zum betrieblichen Datenschutzbeauftragten zu bestellen.

(2) Der Inhaber hat mit dem Betriebsrat, wenn ein Betriebsausschuss errichtet ist, mit diesem, die beabsichtigte Bestellung oder Abberufung des Datenschutzbeauftragten zu beraten. Eine ohne Beratung vorgenommene Bestellung ist rechtsunwirksam. Die Bestellung bedarf auch der zivilrechtlichen Zustimmung des bestellten Mitarbeiters. Stimmt kein geeigneter Mitarbeiter der Bestellung zu, ist eine geeignete betriebsfremde Person oder ein geeignetes Unternehmen zu bestellen.

(3) Der betriebliche Datenschutzbeauftragte hat die Einhaltung der Vorschriften dieses Bundesgesetzes im Betrieb zu überwachen und den Betriebsinhaber, die Arbeitnehmer und den Betriebsrat in Belangen des Datenschutzes zu beraten. Er ist vom Inhaber über Vorhaben, neue Datenanwendungen einzusetzen, rechtzeitig zu unterrichten. Wird ihm ein Verdacht einer Verletzung datenschutzrechtlicher Vorschriften bekannt, hat er auf die Herstellung eines rechtmäßigen Zustandes hinzuwirken. Ist ihm dies aus Eigenem nicht möglich, hat er den Betriebsinhaber von dem Verdacht in Kenntnis zu setzen.

(4) Für Beratungen durch den Datenschutzbeauftragten nach Abs. 3 hat der Inhaber Mitarbeitern, die mit der Verwendung von Daten betraut sind, im ersten Dienstjahr Arbeitszeit im Umfang von zumindest acht Stunden, in folgenden Dienstjahren im Ausmaß von zumindest vier Stunden pro Jahr zur Verfügung zu stellen. Dem betrieblichen Datenschutzbeauftragten selbst sind im ersten Jahr seiner ununterbrochenen Tätigkeit zumindest 40 Stunden und in jedem folgenden Jahr zumindest 20 Stunden an Arbeitszeit zum Erwerb von Fachkenntnissen und zur Weiterbildung auf dem Gebiet des Datenschutzes zur Verfügung zu stellen.

(5) Der betriebliche Datenschutzbeauftragte ist in Ausübung dieser Funktion nicht an Weisungen gebunden. Er hat aber datenschutzbezogene Anregungen des Betriebsinhabers dennoch entgegenzunehmen und gegebenenfalls zu begründen, warum er diese nicht unterstützt. Im Hinblick auf den Kündigungs- und Entlassungsschutz ist der betriebliche Datenschutzbeauftragte einer Sicherheitsfachkraft (§ 73 Abs. 1 des ArbeitnehmerInnenschutzgesetzes, BGBl Nr. 450/1994) gleichgestellt.

(6) Die Bestellung des betrieblichen Datenschutzbeauftragten lässt die Verantwortung des Betriebsinhabers für die Einhaltung der Bestimmungen dieses Bundesgesetzes unberührt.“

35. § 16 Abs. 1 lautet:

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

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

37. In § 17 Abs. 1 wird nach dem Wort „bewirken“ *der Klammerausdruck* „(Änderungsmeldung)“ *eingefügt.*

38. Nach § 17 Abs. 1 werden die folgenden Abs. 1a und 1b eingefügt:

„(1a) Die Meldung ist in elektronischer Form im Wege der vom Bundeskanzler bereit zu stellenden Internetanwendung einzubringen. Identifizierung und Authentifizierung haben mit der Bürgerkarte (§ 2 Z 10 des E-Government-Gesetzes, BGBl. I Nr. 10/2004) zu erfolgen.

(1b) Der Betrieb einer meldepflichtigen Datenanwendung darf erst nach ihrer Registrierung aufgenommen werden. Ebenso dürfen Änderungen einer gemeldeten Datenanwendung erst nach Registrierung der entsprechenden Änderungsmeldung in Betrieb genommen werden."

39. § 18 samt Überschrift lautet:

Vorabkontrollpflichtige Datenanwendungen

§ 18. Meldepflichtige Datenanwendungen, die weder einer Musteranwendung nach § 19 Abs. 2 entsprechen, noch innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften noch die Verwendung von Daten im Katastrophenfall für die in § 48a Abs. 1 genannten Zwecke betreffen, sind vor ihrer Registrierung einer inhaltlichen Kontrolle auf Mangelhaftigkeit im Sinne des § 19 Abs. 3 (Vorabkontrolle) zu unterziehen, wenn sie

1. sensible Daten enthalten oder
2. strafrechtlich relevante Daten im Sinne des § 8 Abs. 4 enthalten oder
3. die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder
4. in Form eines Informationsverbundsystems durchgeführt werden."

40. 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"

41. Nach § 19 Abs. 1 Z 7 wird folgende Z 8 eingefügt:

„8. eine Erklärung, ob die Datenanwendung für Zwecke eines Betriebes mit mehr als 20 Mitarbeitern betrieben werden soll und gegebenenfalls, wer in diesem Betrieb zum betrieblichen Datenschutzbeauftragten (§ 15a) bestellt wurde."

42. 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 Z 1 bis 4 erfüllen, sind, sind nur automationsunterstützt im Rahmen der Internetanwendung (§ 17 Abs. 1a) auf ihre Vollständigkeit und Plausibilität zu prüfen. Ergibt diese Prüfung keine Fehlermeldung, so ist die Meldung sofort zu registrieren.

(2) Ergibt die Prüfung nach Abs. 1 Fehler, so ist dem Auftraggeber sogleich die Möglichkeit zur Verbesserung einzuräumen. Erfolgt diese nicht und besteht der Auftraggeber dennoch auf der Einbringung der Meldung, so ist diese von der Datenschutzkommission auf Mangelhaftigkeit im Sinne des § 19 Abs. 3 zu prüfen.

(3) Meldungen, die der Auftraggeber als vorabkontrollpflichtig bezeichnet hat, sind jedenfalls auf Mangelhaftigkeit im Sinne 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 Fristablauf (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 nicht zu einer Fehlermeldung geführt hat ergeben hat oder
2. das Prüfungsverfahren nach § 20 Abs. 2 keine Mangelhaftigkeit der Meldung ergeben hat oder
3. zwei Monate nach Einlangen einer Meldung (§ 20 Abs. 2 oder 3) bei der Datenschutzkommission verstrichen sind, ohne dass ein Verbesserungsauftrag gemäß § 20 Abs. 4 erteilt wurde oder

4. der Auftraggeber die verlangten 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 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.“

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

„Verfahren zur Überprüfung der Erfüllung der Meldepflicht

§ 22a. (1) Registrierte Meldungen können von der Datenschutzkommission jederzeit auf Mangelhaftigkeit im Sinne des § 19 Abs. 3 geprüft werden. Entsteht bei der Prüfung der Verdacht tatsächlicher Mangelhaftigkeit, ist ein Berichtigungsverfahren nach Abs. 2 durchzuführen.

(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 wegen der Verwaltungsübertretung nach § 52 Abs. 2 Z 1 an die zuständige Behörde zu erstatten.

(5) Ergibt das Verfahren nach Abs. 2 alleine – oder allenfalls in Kombination mit einem Mangel nach Abs. 6 -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) Ergibt das Verfahren nach Abs. 2 alleine – oder allenfalls in Kombination mit Mängeln nach Abs. 5 -, dass ein Betriebsinhaber entgegen § 15a keinen oder keinen geeigneten betrieblichen Datenschutzbeauftragten bestellt hat, so ist die Bestellung mit Bescheid aufzutragen.

(7) 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.“

44. § 26 Abs. 1 lautet:

„**§ 26.** (1) Ein Auftraggeber hat jeder natürlichen Person Auskunft über die zu dieser Person verarbeiteten Daten zu geben, wenn sie dies schriftlich verlangt und ihre 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 anzuführen. Auf Verlangen eines Betroffenen sind auch Namen und Adresse 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.“

45. 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.*

46. § 26 Abs. 8 lautet:

„(8) In dem Umfang, in dem eine Datenanwendung für eine natürliche Person 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.“

47. § 26 Abs. 10 lautet:

„(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.“

48. In § 27 Abs. 9 entfällt das Wort „öffentliche“.

49. 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.“

50. Nach § 30 Abs. 1 wird der folgende Abs. 1a eingefügt:

„(1a) Ein betrieblicher Datenschutzbeauftragter kann sich wegen des Verdachts der Verletzung datenschutzrechtlicher Vorschriften im Betrieb mit einer Eingabe an die Datenschutzkommission wenden, nachdem er den Betriebsinhaber von dem Verdacht in Kenntnis gesetzt hat, dieser jedoch in angemessener Frist keine geeigneten Maßnahmen zur Beseitigung des vermuteten rechtswidrigen Zustandes getroffen hat.“

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

„(2a) Sofern sich eine zulässigen 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."

52. § 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 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.

53. § 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."

54. 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 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."

55. Die § 31 samt Überschrift lautet:

„Beschwerde an die Datenschutzkommission

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

(2) Die Datenschutzkommission erkennt weiters über Beschwerden von natürlichen 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 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 §§ 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.“

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

(3) 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.“

57. § 32 Abs. 1 lautet:

„**§ 32.** (1) Ansprüche wegen Verletzung der Rechte einer natürlichen 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.“

58. In § 32 Abs. 4 wird im ersten Satz das Wort „Betroffene“ *durch das Wort* „Kläger“ *ersetzt. Im zweiten Satz wird die Wortfolge* „Auftraggeber oder der Dienstleister“ *durch das Wort* „Beklagte“ *ersetzt. Überdies wird nach dem Wort* „Sitz“ *die Wortfolge* „oder eine Niederlassung“ *eingefügt.*

59. In § 32 Abs. 6 wird das Wort „Betroffener“ *durch das Wort* „Einschreiter (§ 30 Abs. 1)“ *und das Wort* „Betroffenen“ *durch die Worte* “natürlichen Personen“ *ersetzt.*

60. 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 bei der Datenschutzkommission die registrierte Meldung dieser Datenanwendung anzufordern. Erachtet das Gericht die Meldepflicht nach § 17 Abs. 1 als nicht erfüllt, so hat es dies begründet der Datenschutzkommission mitzuteilen, die erforderlichenfalls nach den §§ 22 und § 22a vorgeht.

61. In § 34 Abs. 1 wird das Wort „abzuweisen“ *durch das Wort* „zurückzuweisen“ *ersetzt.*

62. § 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.“

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

64. In § 36 Abs. 3 wird das Wort „Bundesbeamten“ *durch das Wort* „Bundesbediensteten“ *ersetzt.*

65. 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.“

66. § 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 Richterdienstgesetzes, BGBl Nr. 305/1961, gleich. Die Mitgliedschaft der übrigen Mitglieder endet am 31. Dezember des Jahres, in dem sie das 65. Lebensjahr vollenden.“

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

*68. **(Verfassungsbestimmung)** In § 38 Abs. 1 wird die Wortfolge* „§ 20 Abs. 2 oder § 22 Abs. 3“ *durch die Wortfolge* „§ 22 Abs. 3 oder § 30 Abs. 6a“ *ersetzt.*

69. § 39 wird der folgende Abs. 5 angefügt:

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

70. § 40 Abs. 1 und 2 lauten:

„**§ 40.** (1) Gegen Bescheide, die das geschäftsführende Mitglied der Datenschutzkommission gemäß § 22 Abs. 3 oder gemäß § 30 Abs. 6a 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.“

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 f 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 EO) 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. Soweit dies nicht durch Gesetz geschehen ist, ist dieser Pflichtenübergang 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. 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") betreffen, durch technische Bildaufnahmegeräte. Für derartige Überwachungen gelten die folgenden Absätze, sofern nicht durch andere Gesetze Besonderes bestimmt ist.

(2) Videoüberwachung sowie die Auswertung und Übermittlung der dabei ermittelten Daten darf vorbehaltlich des Abs. 5 nur zum Schutz der überwachten Objekte oder zur Beweissicherung im Hinblick auf Ereignisse nach Abs. 1 erfolgen.

(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, oder
4. sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte Objekt betreffenden Ereignisse erschöpft, diese also weder gespeichert (aufgezeichnet) noch in sonst einer anderen Form weiterverarbeitet werden, und sie zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt, oder
5. bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt könnte das Ziel oder der Ort eines gefährlichen Angriffes im Sinn von § 16 Abs. 1 Z 1 des Sicherheitspolizeigesetzes (SPG), BGBl. Nr. 566/1991 in der jeweils geltenden Fassung, werden. Als bestimmte Tatsache ist es insbesondere anzusehen, wenn
   a) das überwachte Objekt bereits einmal Ziel oder Ort eines gefährlichen Angriffs war und eine Wiederholung wahrscheinlich ist. Zu berücksichtigen sind jedenfalls nur gefährliche Angriffe, die sich innerhalb der vergangenen zehn Jahre ereignet haben. Ist für die dem gefährlichen Angriff zu Grunde liegende gerichtlich strafbare Handlung (§ 16 Abs. 2 SPG) nach § 57 des Strafgesetzbuches (StGB), BGBl Nr. 60/1974 in der jeweils geltenden Fassung, eine kürzere Verjährungsfrist vorgesehen, so sind nur gefährliche Angriffe innerhalb dieser Frist relevant. § 58 StGB hat dabei außer Betracht zu bleiben, oder
   b) das überwachte Objekt eine Person mit überdurchschnittlichem Bekanntheitsgrad in der Öffentlichkeit oder ein Aufenthaltsort einer derartigen Person ist, oder
   c) das überwachte Objekt ein verfassungsmäßiges Organ oder dessen Aufenthaltsort ist, oder
   d) das überwachte Objekt ein beweglicher Gegenstand mit Geldwert von mehr als EUR 100.000,-- oder ein Aufenthaltsort derartiger Gegenstände ist, oder
   e) das überwachte Objekt ein Gegenstand von überdurchschnittlichem künstlerischem Wert ist,

   oder
6. unmittelbar anwendbare Rechtsvorschriften des Völker- oder des Gemeinschaftsrechts, Gesetze, Verordnungen, Bescheide oder gerichtliche Entscheidungen dem Auftraggeber spezielle Sorgfaltspflichten zum Schutz der überwachten Objekte auferlegen, oder
7. die Videoüberwachung zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche des Auftraggebers vor einem Gericht im Sinn von Art. 234 EGV erforderlich ist.

(4) Abs. 3 Z 4 bis 7 sind für Auftraggeber des öffentlichen Bereichs bei Wahrnehmung ihrer hoheitlichen Aufgaben nicht anwendbar. Außerdem dürfen mit einer Videoüberwachung nach Abs. 3 Z 4 bis 7 nicht Ereignisse an Orten festgestellt werden, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen.

(5) Schutzwürdige Geheimhaltungsinteressen Betroffener sind auch dann nicht verletzt, wenn durch Videoüberwachung aufgezeichnete Daten über eine Verwendung entsprechend den Abs. 2 und 3 hinaus an die zuständige Behörde oder das zuständige Gericht übermittelt werden, weil beim Auftraggeber der begründete Verdacht entstanden ist, die Daten könnten

1. eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren, oder
2. der Abwehr oder Beendigung eines gefährlichen Angriffs dienen,

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.

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

(7) Im Übrigen gelten auch für Videoüberwachung die §§ 6 und 7, insbesondere der Verhältnismäßigkeitsgrundsatz (§ 7 Abs. 3).

Besondere Protokollierungs- und Löschungspflicht

§ 50b. (1) Jeder Verwendungsvorgang einer Videoüberwachung ist zu protokollieren.

(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. 5 benötigt werden, spätestens nach 48 Stunden zu löschen. Die Datenschutzkommission hat auf Antrag des Auftraggebers eine längere Aufbewahrung zu genehmigen, wenn dies aus besonderen Gründen zur Zweckerreichung regelmäßig erforderlich ist. Ein solcher Antrag ist bei meldepflichtigen Videoüberwachungen tunlichst mit der Meldung zu verbinden.

Meldepflicht und Registrierungsverfahren

§ 50c. (1) Eine Videoüberwachung ist über § 17 Abs. 2 hinaus von der Meldepflicht ausgenommen, wenn

1. § 50a Abs. 3 Z 4 erfüllt ist oder
2. eine Speicherung (Aufzeichnung) nur auf einem analogen Speichermedium erfolgt.

(2) Meldepflichtige Überwachungen unterliegen stets der Vorabkontrolle (§ 18 Abs. 2). Bestimmte Tatsachen im Sinn von § 50a Abs. 1 Z 5 und die Anspruchsverfolgung nach § 50a Abs. 1 Z 7 müssen bei Erstattung der Meldung glaubhaft gemacht werden.

(3) Mehrere überwachte Objekte, 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. Die Kennzeichnung hat jedenfalls den Auftraggeber zu benennen und hat örtlich derart zu erfolgen, dass jeder potentiell Betroffene, der sich einem überwachten Objekt nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen.

(2) Die Kennzeichnung kann entfallen,

1. wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte oder der Beschaffenheit des überwachten Objekts, insbesondere dessen Mobilität, einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordern würde, oder
2. im Fall einer Überwachung nach § 50a Abs. 3 Z 7, wenn dadurch die Gewinnung von Beweismitteln zur Anspruchsverfolgung vereitelt würde.

(3) Der beabsichtigte Entfall einer Kennzeichnung nach Abs. 2 ist bei meldepflichtigen Überwachungen in der Meldung an die Datenschutzkommission anzugeben. Wenn diese die Voraussetzungen nicht als gegeben erachtet, hat sie eine Kennzeichnung mit Bescheid anzuordnen.

Auskunftsrecht

§ 50e. (1) Abweichend von § 26 Abs. 1 ist dem Auskunftswerber, nachdem dieser den Zeitraum, in dem er möglicherweise von der Überwachung betroffen war, möglichst präzise 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.“

83. 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.*

84. § 58 wird aufgehoben.

85. ***(Verfassungsbestimmung)*** *§ 60 Abs. 1 zweiter Satz lautet:*

„§ 1, § 2, § 3 Abs. 1 und 2 sowie § 38 Abs. 1 in der Fassung der Novelle BGBl I Nr. xxx/2008 treten am 1. Juli 2008 in Kraft.“

86. Nach § 60 Abs. 3 werden folgende Abs. 4 und 5 angefügt:

„(4) Das Inhaltsverzeichnis, die Überschrift und Absatzgliederung von § 4, § 4 Abs. 1 Z 3 bis 5, § 4 Abs. 1 Z 7 bis 9, § 4 Z 11 und 12, § 4 Abs. 2, § 8 Abs. 1 und 2, § 8 Abs. 3 Z 2 und 5, § 8 Abs. 4, § 9 Z 4 und 9, § 12 Abs. 1, § 16 Abs. 1 und 3, § 17 Abs. 1 bis 1b, § 18 samt Überschrift, § 19 Abs. 1 Z 3a, die §§ 20 bis 22 samt Überschriften, § 22a Abs. 1 bis 5 samt Überschrift, § 26 Abs. 1 bis 8, § 26 Abs. 10, § 27 Abs. 9, § 28 Abs. 3, § 30 Abs. 2a und Abs. 5 bis 6a, die §§ 31 und 31a samt Überschriften, § 32 Abs. 1, 4, 6 und 7, § 34 Abs. 3 und 4, § 36 Abs. 3, 3a, 6 und 9, § 39 Abs. 5, § 40 Abs. 1 und 2, § 42 Abs. 1 Z 1, § 42 Abs. 5, § 46 Abs. 1 bis 3a, § 47 Abs. 4, § 49 Abs. 3, § 50 Abs. 1 bis 2a, der 9a. Abschnitt sowie § 55 in der Fassung der Novelle BGBl I Nr. xxx/2008 treten am 1. März 2008 in Kraft. Gleichzeitig treten § 4 Abs. 1 Z 10, § 13 Abs. 3 und § 58 außer Kraft.

(5) § 15a, § 19 Abs. 1 Z 8, § 22a Abs. 6 und § 30 Abs. 1a in der Fassung der Novelle BGBl I Nr. xxx/2008 treten am 1. Juli 2009 in Kraft.“

87. § 61 Abs. 6 lautet:

„(6) Videoüberwachungen, die vor dem Inkrafttreten der §§ 50a bis 50e registriert wurden, sind bis zum 1. Juli 2010 auch dann rechtmäßig, wenn sie den am 30. Juni 2008 geltenden datenschutzrechtlichen Bestimmungen genügen.“

88. Nach § 61 Abs. 7 werden folgende Abs. 8 und 9 angefügt:

„(8) Die Angaben zum betrieblichen Datenschutzbeauftragten (§ 19 Abs. 1 Z 8) sind der Datenschutzkommission bei vor dem 1. Juli 2009 registrierten Datenanwendungen anlässlich der ersten über eine Streichung hinausgehenden Änderungsmeldung zu melden, die ab diesem Datum erstattet wird. Eine Meldung allein im Hinblick auf § 19 Abs. 1 Z 8 ist nicht erforderlich.

(9) Die Verordnung nach § 16 Abs. 3 ist vom Bundeskanzler nach Maßgabe der technischen Möglichkeiten des Datenverarbeitungsregisters bis spätestens zum 1. Jänner 2011 neu zu erlassen. Bis zum Inkrafttreten dieser Verordnung sind die §§ 16 bis 22, § 30 Abs. 6 sowie § 40 Abs. 1 in der Fassung vor der Novelle BGBl I Nr. xxx/2008 anzuwenden; § 22a, § 30 Abs. 2a und 6a, § 31a Abs. 1 sowie § 32 Abs. 7 sind bis dahin nicht 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), sind 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.“

*89. **(Verfassungsbestimmung)** Nach § 61 Abs. 9 wird der folgende Abs. 10 eingefügt:*

„(10) **(Verfassungsbestimmung)** Bis zur Neuerlassung der Verordnung nach § 16 Abs. 3 ist auch § 38 Abs. 1 in der Fassung vor der Novelle BGBl I Nr. xxx/2008 anzuwenden.“

Vorblatt

Ziel und Inhalt:

Der vorliegende Gesetzentwurf

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

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

- enthält Klarstellung von in der Vollzugspraxis aufgetretener Rechtsfragen;

- sieht eine betrieblichen Datenschutzbeauftragten für größere Betriebe vor;

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

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

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

Alternativen:

Keine

Auswirkungen des Regelungsvorhabens

- Finanzielle Auswirkungen:

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

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

- Wirtschaftspolitische Auswirkungen:

--Auswirkungen auf die Beschäftigungslage und den Wirtschaftsstandort Österreich:

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

-- Auswirkungen auf die Verwaltungslasten für Unternehmen:

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

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

- Auswirkungen in umweltpolitischer, konsumentenschutzpolitischer sowie sozialer Hinsicht:

Keine

- Geschlechtsspezifische Auswirkungen:

Keine

Verhältnis zu Rechtsvorschriften der Europäischen Union:

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

Besonderheiten des Normsetzungsverfahrens:

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

Erläuterungen

Allgemeiner Teil

Hauptgesichtspunkte des Entwurfes:

Das DSG 2000 ist seit seinem Inkrafttreten am 1. Jänner 2000 nur zweimal punktuell novelliert worden. Der vorliegende Entwurf stellt demgegenüber die erste umfassende Novelle dar, die ihre Motivation vor allem aus den im Vollzug aufgetretenen Problemen schöpft, wie sie in Anfragen von Rechtsunterworfenen, in Entscheidungen der Datenschutzkommission, des VwGH und des VfGH sowie in den Datenschutzberichten zu Tage treten. Besonders hervorzuheben ist die aus dem Alltag fast nicht mehr wegzudenkende Videoüberwachung, der das DSG 2000 in seiner derzeitigen Fassung, die noch auf dem Konzept klassischer Datenbanken aufbaut, keine besondere Aufmerksamkeit schenkt. Ziel war in Anbetracht der stetig steigenden Belastung des Datenverarbeitungsregisters weiters eine massive Vereinfachung des Registrierungsverfahrens bei gleichzeitiger Steigerung der Qualität des Datenverarbeitungsregisters, was auch durch eine klarere Regelung der Reaktionsmöglichkeiten der Datenschutzkommission im Fall der Nichterfüllung einer Meldepflicht erreicht werden soll. Durch die Einführung eines betrieblichen Datenschutzbeauftragten in Betrieben mit mehr als 20 MitarbeiterInnen soll ArbeitnehmerInnen die Durchsetzung ihrer Rechte und Interessen nach dem DSG 2000 erleichtert werden. Schließlich enthält die Novelle eine verständlichere Formulierung einiger Bestimmungen (ohne wesentliche Veränderung des Inhalts), insbesondere auch des Grundrechts auf Datenschutz, dessen Anwendungsbereich überdies auf natürliche Personen beschränkt werden soll, sowie eine Bereinigung der unübersichtlichen Kompetenzrechtslage.

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

Finanzielle Auswirkungen:

- Auswirkungen auf andere Gebietskörperschaften:

Durch die vorgeschlagene Kompetenzbereinigung (§ 2), wonach die Gesetzgebung und die Vollziehung in Angelegenheiten des Schutzes personenbezogener Daten künftig zur Gänze Bundessache sein soll, ist eine vollständige Entlastung der Länder zu erwarten.

- Auswirkungen auf den Bundeshaushalt:

Für die Anschaffung einer Datenbank zur Führung des Datenverarbeitungsregisters (§ 16 Abs. 3) fallen beim Bund Kosten in derzeit noch nicht zu beziffernder Höhe an.

- Auswirkungen auf den Stellenplan des Bundes:

Die vorgeschlagenen Änderungen durch die DSG-Novelle 2008 haben keine Auswirkungen auf den Stellenplan des Bundes, sie zielen vielmehr auf die Entlastung des Datenverarbeitungsregister (und damit der Datenschutzkommission) ab:

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

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

- Auswirkungen auf Verwaltungslasten für Unternehmen:

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

Nicht näher zu beziffern sind die Verwaltungslasten, die Unternehmen durch die – gewiss sehr seltenen – Fälle entstehen, in denen sie als bloße Dienstleister einer Datenverarbeitung Auskunft über den Auftraggeber zu geben haben (§ 26 Abs. 10). Die Durchsicht der im Rechtsinformationssystem des Bundes veröffentlichten Entscheidungen der Datenschutzkommission seit dem Jahr 2004 ergab, dass sich lediglich ein einziger Fall auf die Abgrenzung zwischen Auftraggeber und Dienstleister bezog, sodass

davon auszugehen ist, dass diese neue Auskunftsverpflichtung ebenfalls keine wesentlichen Auswirkungen auf die Verwaltungslasten für Unternehmen hat.

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

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

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

Kompetenzgrundlage:

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

Besonderheiten des Normerzeugungsverfahrens:

Z 10, 11, 12, 13, 68, 83 und 89 sind Verfassungsbestimmungen und können gemäß Art. 44 Abs. 1 B-VG vom Nationalrat nur in Anwesenheit von mindestens der Hälfte der Mitglieder und mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen beschlossen werden. Da durch die Bestimmung der Z 3 überdies die Zuständigkeit der Länder in der Vollziehung eingeschränkt wird, ist gemäß Art. 44 Abs. 2 B-VG auch die in Anwesenheit von mindestens der Hälfte der Mitglieder und mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen zu erteilende Zustimmung des Bundesrates erforderlich.

Besonderer Teil

Zu Z 10 (§ 1):

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

Die bisher in Abs. 1 enthaltene Einschränkung „soweit ein schutzwürdiges Interesse daran besteht“ stammt aus dem „alten“ DSG (1978) und war seit Inkrafttreten des DSG 2000 richtlinienkonform dahingehend zu interpretieren, dass alle personenbezogene Daten als schutzwürdig zu betrachten waren, es sei denn, dass die allgemeine Verfügbarkeit dieser Daten gegeben war. Die „Datenschutzrichtlinie“ 95/46/EG kennt nämlich die bisher in § 1 DSG 2000 enthaltene Einschränkung nicht und bezieht sich grundsätzlich auf alle personenbezogene Daten, wobei des Weiteren in der Richtlinie Tatbestände festgelegt werden, bei deren Vorliegen personenbezogene Daten verwendet werden dürfen (siehe dazu insbesondere die Art. 6 ff der Richtlinie). Diesem System folgend sind die Eingriffstatbestände in das Grundrecht auf Datenschutz in Abs. 2 iVm den einfachgesetzlichen Bestimmungen der §§ 6 ff DSG 2000 geregelt. Für eine „doppelte Abwägung“ nach schutzwürdigen Interessen besteht demnach kein

Spielraum. Weiters scheint selbstverständlich, dass Daten nur dann personenbezogen sein können, wenn eine Rückführbarkeit dieser Daten gegeben ist, weshalb auch diese Passage entfallen kann.

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

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

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

Zu Z 11 (§ 2):

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

Zu Z 12 und 13 (§ 3 Abs. 1 und 2):

Die Ausweitung auf EWR-Vertragsstaaten resultiert aus der Tatsache, dass diese, auch wenn sie nicht der EU angehören, ebenfalls die Richtlinie 95/46/EG umzusetzen haben und damit auch Art. 4 der Richtlinie über das anwendbare einzelstaatliche Recht auch hinsichtlich dieser Staaten umzusetzen ist.

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

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

Zu Z 15 (§ 4 Abs. 1 Z 3):

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

Zu Z 16 (§ 4 Abs. 1 Z 4):

Mit dieser Bestimmung soll eine Vereinfachung des Auftraggeberbegriffes vorgenommen werden.

Zu Z 17 (§ 4 Abs. 1 Z 5):

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

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

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

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

Zu Z 18 (§ 4 Abs. 1 Z 7):

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

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

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

Zu Z 20 und 21 (§ 4 Abs. 1 Z 9, Entfall der Z 10):

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

Zu Z 22 (§ 4 Abs. 1 Z 11):

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

Zu Z 25 (§ 8 Abs. 1):

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

Zu Z 26 (§ 8 Abs. 2):

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

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

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

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

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

Zu Z 29 (§ 8 Abs. 4):

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

Zu Z 32 (§ 12 Abs. 1):

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

Zu Z 33 (Aufhebung von § 13 Abs. 3):

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

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

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

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

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

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

Zu Z 35 (§ 16 Abs. 1):

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

Zu Z 36 (§ 16 Abs. 3):

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

Zu Z 37 (§ 17 Abs. 1):

Mit der Einführung des Terminus „Änderungsmeldung“ soll die Verpflichtung, den Stand des Datenverarbeitungsregisters durch Meldung jeder relevanten Änderung stets aktuell zu halten, verdeutlicht werden.

Zu Z 38 (§ 17 Abs. 1a und b):

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

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

Zu Z 39 (§ 18 samt Überschrift):

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

Zu Z 40 (§ 19 Abs. 1 Z 3a):

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

Zu Z 42 (§§ 20 bis 22):

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

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

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

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

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

In § 22 Abs. 1 bis 3 wurden nur geringfügige Änderungen vorgenommen. Abs. 1 ordnet zunächst an, dass Änderungen für die Dauer von drei Jahren ersichtlich zu machen sind. Daher sind insbesondere gestrichene Auftraggeber bzw. Datenanwendungen erst nach Ablauf dieser Frist zu löschen.

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

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

Zu Z 43 (§ 22a):

Durch diese Bestimmung soll das bisher (im geltenden § 22 Abs. 4) nur wenig geregelte Verfahren zur Überprüfung der Meldepflicht insbesondere im Hinblick auf die Befugnisse der Datenschutzkommission neu geregelt werden. Dies stellt auch einen Ausgleich für den Entfall der Detailprüfung bei nicht vorabkontrollpflichtigen Datenanwendungen dar. Abs. 1 ermöglicht in diesem Sinn eine jederzeitige Überprüfung registrierter Meldungen durch die Datenschutzkommission (vgl. auch § 30 Abs. 2a, § 31a .Abs. 1 sowie § 32 Abs. 7, die „Impulse“ für derartige Überprüfungen setzen sollen). Wenn diese „interne“ Prüfung den Verdacht einer Nichterfüllung der Meldepflicht erhärtet, so ist ein Verfahren zur Berichtigung des Datenverarbeitungsregisters durchzuführen, welches durch begründete Verfahrensanordnung (also nicht durch Bescheid) eingeleitet wird. Freilich können nicht nur Mängel innerhalb registrierter Meldungen (§ 19 Abs. 3), die in der Regel (außer die Mangelhaftigkeit tritt erst nachträglich durch Änderungen der Rechtslage ein; s. dazu zB die Übergangsbestimmung für Videoüberwachung in Z 85) eigentlich schon im Zuge des Registrierungsverfahrens hätten hervorkommen müssen, ein solches Berichtigungsverfahren erforderlich machen, sondern auch Fälle, in denen eine Meldung zur Gänze oder teilweise unterlassen wurde, eine Datenanwendung also gar nicht oder in einer nicht (mehr) dem Echtbetrieb entsprechenden Form registriert ist. Je nachdem, welcher der beiden Fälle vorliegt, ist auch das Berichtigungsverfahren zu führen bzw. abzuschließen. Der erste Fall (Mangel nach § 19 Abs. 3), den Abs. 3 regelt, führt, sofern keine auftragsgemäße Verbesserung erfolgt, – analog der Ablehnung nach § 20 Abs. 5 – zur Streichung der Datenanwendung, im zweiten Fall (Abs. 4) wird die Datenanwendung untersagt. Eine solche Untersagung hat freilich- wie grundsätzlich jeder Bescheid (vgl. *Walter/Mayer*, Verwaltungsvefahren, 8. Aufl., Rz. 481 ff – objektive Grenzen, nämlich den Sachverhalt und die Rechtslage,.auf die sie sich bezieht. Wird also zB eine Datenanwendung, die zunächst mangels Meldung untersagt wurde, auf Grund einer nachträglich erstatteten Meldung registriert, so wird die Untersagung gegenstandslos.

Die Abs. 5 und 6 regeln die Sonderfälle, dass sich als Ergebnis des Berichtigungsverfahrens bloß Mängel bei den Datensicherheitsmaßnahmen bzw. das Fehlen eines nach § 15a Abs. 1 erforderlichen betrieblichen Datenschutzbeauftragten ergibt.

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

Zu Z 44 und 45 (§ 26 Abs. 1 bis 7):

Abgesehen von der Beschränkung des Auskunftsrechts auf natürliche Personen im Lichte von § 1 Abs. 3 Z 1 erfolgt lediglich eine der Rechtsprechung der Datenschutzkommission (zB Bescheid vom 2. Februar 2007, GZ K121.220/0001-DSK/2007) entsprechende Klarstellung, dass auch in dem Fall, dass

ein Auftraggeber zu einer natürlichen Person keine Daten verarbeitet, eine sog. Negativauskunft zu erteilen ist. Dementsprechend wird in § 26 nunmehr im Allgemeinen von „Auskunftswerbern" gesprochen, der Begriff des Betroffenen wird nur noch im strengen Sinn des § 4 Z 3 gebraucht, dh wenn zur Person des Auskunftswerbers tatsächlich Daten vorhanden sein müssen (zB Anspruch auf Bekanntgabe von Dienstleistern in Abs. 1).

Zu Z 46 (§ 26 Abs. 8):

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

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

Zu Z 47 (§ 26 Abs. 10):

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

Zu Z 48 (§ 27 Abs. 9):

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

Zu Z 49 (§ 28 Abs. 3):

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

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

Auch diese Bestimmung soll den Entfall der inhaltlichen Prüfung von nicht vorabkontrollpflichtigen Registermeldungen im Sinne einer verwaltungseffizienten und am Rechtsschutzbedarf orientierten Lösung ausgleichen (s. schon oben zu Z 41 und 42): Anlässlich jeder zulässigen Eingabe nach § 30 Abs. 1 bzw. jedes begründeten Verdachts hat die Datenschutzkommission nunmehr den Registerstand zu überprüfen, entspricht dieser nicht dem Gesetz, sind Maßnahmen nach den §§ 22 und 22a zu ergreifen. Somit führt (und endet) das Verfahren nach § 30 im Fall eines Verdachts der Nichterfüllung der Meldepflicht bei den §§ 22 und 22a. Der Ausspruch einer Empfehlung scheint in diesen Fällen wenig zweckmäßig und entfällt daher künftig. Eine Empfehlung ist weiters nicht mehr erforderlich, wenn die Datenanwendung schon wegen Gefahr im Verzug untersagt worden ist.

Zu Z 52 (§ 30 Abs. 5):

Hier wird eine Klarstellung getroffen: Auch die Verwertung der Ergebnisse einer Einschau nach Abs. 4 zur verbindlichen Klärung der darauf bezogenen (Datenschutz-)Rechtslage vor Gericht nach § 32 (gleich ob durch den Einschreiter oder die Datenschutzkommission) zählt zur Kontrolltätigkeit. Daher besteht gegenüber dem angerufenen Gericht hinsichtlich solcher Ergebnisse keine Verschwiegenheitspflicht. Das Gericht kann einem besonderen Geheimhaltungsinteresse des Beklagten durch Ausschluss der Öffentlichkeit auf Grundlage der ZPO Rechnung tragen.

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

Zu Z 54 (§ 30 Abs. 6a):

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

Zu Z 55 (§ 31):

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

§ 31 vermeidet nunmehr insb. in den Abs. 1 und 2 die Verwendung des materiellrechtlichen Begriffs „Auftraggeber“ (ob jemandem diese Rolle zukommt, wird oft erst im Verfahren entschieden) und orientiert sich an der Formulierung von § 1 Abs. 5. Der lückenlosen Umsetzung dieser verfassungsrechtlichen Rechtsschutzbestimmung dient auch die „negative“ Abgrenzung der Beschwerdelegitimation nach Abs. 2, bezogen auf § 32 Abs. 1.

Weiters wird nun auch eine Beschwerdemöglichkeit im Hinblick auf die Rechte auf Bekanntgabe des Ablaufs einer automatisierten Einzelentscheidung (§ 49 Abs. 3) bzw. des verantwortlichen Auftraggebers in einem Informationsverbundsystem (§ 50 Abs. 1 2. Satz) vorgesehen. Diesbezüglich bestand bisher (jedenfalls dem Wortlaut nach) eine Rechtsschutzlücke.

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

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

§ 31 Abs. 6 sieht aus Gründen der Verfahrensökonomie vor, dass ein Kontrollverfahren nach § 30 Abs. 1 nicht parallel zu einem Beschwerdeverfahren über denselben Gegenstand geführt werden soll. Freilich können über den Beschwerdegegenstand hinausgehende Verdachtsmomente von der Datenschutzkommission nach § 30 weiterverfolgt werden.

§ 31 Abs. 8 sieht eine besondere verfahrensrechtliche Regelung für den in der Praxis regelmäßig auftretenden Fall vor, dass ein Beschwerdeführer während des Auskunfts-, Richtigstellungs- oder Löschungsbeschwerdeverfahrens klaglos gestellt wird, dh die mit der Beschwerde verfolgte Auskunft erteilt oder die Löschung/Richtigstellung durchgeführt wird. Wurde die Beschwerde in einem solchen

Fall nicht ausdrücklich zurückgezogen (§ 13 Abs. 7 AVG), so musste dennoch ein abweisender Bescheid erlassen werden, auch wenn auf Grund des Unterbleibens einer Stellungnahme des Beschwerdeführers im Parteiengehör zu vermuten war, dass dieser kein Interesse an der Weiterverfolgung seines Anspruches hat. Nunmehr soll es der Datenschutzkommission ermöglicht werden, in derartigen Fällen das Verfahren formlos (dh ohne Bescheiderlassung, wohl aber unter Verständigung des Beschwerdeführers) einzustellen, wenn der Beschwerdeführer nicht ausdrücklich auf einer Fortsetzung beharrt. Diese § 33 Abs. 1 VwGG nachgebildete Ergänzung des verfahrensrechtlichen Instrumentariums des AVG scheint im Hinblick auf das kontradiktorisch ausgestaltete Beschwerdeverfahren vor der Datenschutzkommission zweckmäßig. Die formlose Einstellung ist auch nicht präjudiziell, eine neue Beschwerdeerhebung innerhalb der Frist des § 34 Abs. 1 daher jederzeit möglich.

Besonders Bedacht genommen wird in der Bestimmung auch auf die immer wieder vorkommende wesentliche Änderung des Verfahrensgegenstandes (§ 13 Abs. 8 AVG) in einer derartigen Konstellation. Wenn etwa zunächst Beschwerde erhoben wurde, weil auf ein Auskunftsbegehren überhaupt nicht reagiert worden ist und während des Verfahrens eine Auskunft erteilt wird, die der Beschwerdeführer aber als unvollständig oder falsch ansieht, so ändert er bei einem entsprechenden Vorbringen den Verfahrensgegenstand wesentlich ab (s. zB den Bescheid der Datenschutzkommission vom 20. Juli 2007, GZ K121.289/0006-DSK/2007). Solche Fälle werden nunmehr entsprechend der bei *Thienel*, Verwaltungsverfahren, 3. Aufl., 112, wiedergegebenen herrschenden Ansicht, der die Datenschutzkommission in der Praxis schon bisher folgte, als (konkludente) Zurückziehung der ursprünglichen Beschwerde und gleichzeitige Einbringung einer weiteren Beschwerde mit dem geänderten Gegenstand gewertet. Damit beginnt auch die Entscheidungsfrist neu zu laufen. Zu verspäteten Äußerungen gilt das zu Z 42 Gesagte sinngemäß.

Zu Z 56 (§ 31a):

Zur Wahrung der Übersichtlichkeit des § 31 werden mit dem Beschwerdeverfahren zusammenhängende Instrumente nunmehr in § 31a geregelt. Zunächst wird in dessen Abs. 1 eine Z 30 und 31 entsprechende Anordnung zur Überprüfung der Registermeldung getroffen. Der bisherige § 31 Abs. 3 (in der Praxis bedeutungslos) scheint im Hinblick darauf nicht mehr erforderlich, weil der neue § 22 Abs. 4 und 5 (Z 26 und 27) der Datenschutzkommission genau die gleichen Möglichkeiten geben. Hinsichtlich des Bestreitungsvermerks wird nunmehr in § 31a Abs. 2 im Hinblick auf eine Beschleunigung dieser Möglichkeit vorgesehen, dass darüber mit Mandatsbescheid entschieden werden kann.

Der bisherige § 31 Abs. 4 findet sich in § 31a Abs. 3 unverändert wieder. Es wird lediglich angeordnet, dass die ersten beiden Sätze im Verfahren nach § 30 sinngemäß anzuwenden sind.

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

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

Zu Z 60 (§ 32 Abs. 7):

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

Zu Z 61 (§ 34 Abs. 1):

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

Zu Z 62 (§ 34 Abs. 3):

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

Zu Z 63 (§ 34 Abs. 4):

Vgl. die Erwägungen zu Z 5, 6 und 24.

Zu Z 64 (§ 36 Abs. 3):

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

Zu Z 65 (§ 36 Abs. 3a):

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

Zu Z 66 (§ 36 Abs. 6):

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

Zu Z 67 (§ 36 Abs. 9):

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

Zu Z 68 (§ 38 Abs. 1):

Es handelt sich lediglich um eine Anpassung der Verweise.

Zu Z 69 (§ 39 Abs. 5):

Durch diese Regelung wird lediglich die bisherige Praxis gesetzlich festgeschrieben.

Zu Z 70 (§ 40 Abs. 1 und 2):

Abs. 1 enthält lediglich eine Anpassung der Verweise.

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

Zu Z 71 (§ 42 Abs. 1 Z 1):

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

Zu Z 72 (§ 42 Abs. 5):

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

Zu Z 73 (§ 46 Abs. 1):

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

Zu Z 74 (§ 46 Abs. 2):

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

Zu Z 75 (§ 46 Abs. 3):

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

Zu Z 76 (§ 46 Abs. 3a):

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

Zu Z 77 (§ 47 Abs. 4):

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

Zu Z 78 (§ 49 Abs. 3) und Z 79 (§ 50 Abs. 1 dritter Satz):

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

Zu Z 80 und 81 (§ 50 Abs. 2 und 2a):

Diese Bestimmungen sollen der Vereinfachung des Registrierungsverfahrens für Informationsverbundsysteme dienen. Zunächst wird in abs. 2 klargestellt, dass dem Betreiber auch die Vornahme der Meldung (idR durch eine Vollmacht) übertragen werden kann. Die Nennung von Behörden im zweiten Satz scheint entbehrlich, sie sind idR „Dritte“. Der Datenschutzkommission als verfahrensführender Behörde wird die Pflichtenübertragung schon vor der Registrierung bekannt, daher kann sie ihr gegenüber schon mit dem Einlangen der Meldung wirksam werden.

Nach dem neuen Abs. 2a kann sich die Meldung eines Teilnehmers an einem Informationsverbundsystem hinsichtlich des Inhalts der Datenanwendung nunmehr auf einen Verweis auf eine bereits registrierte Meldung eines anderen Teilnehmers beschränken. Damit gelten für solche weiteren Meldungen im Ergebnis ähnliche Vereinfachungen wie für Musteranwendungen. Wenn sich der weitere Teilnehmer anlässlich der vereinfachten Meldung auch noch den anlässlich der „Vorbildmeldung“ bereits erteilten Auflagen unterwirft, so werden diese kraft Gesetzes mit der Registrierung für ihn ebenso wirksam, ein eigener Auflagenbescheid braucht nicht erlassen zu werden.

Zu Z 82 (9a. Abschnitt):

Allgemeines:

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

Zu § 50a:

§ 50a Abs. 1 enthält zunächst eine Definition der Videoüberwachung. Dass dies mit „systematischer“ Erfassung von Ereignissen umschrieben wurde, soll klarstellen, dass durch eine Summe von Verwendungsschritten (vgl. § 4 Z 7) das Ergebnis „Überwachung“ verwirklicht werden soll. Aufnahmen etwa aus rein touristischen oder künstlerischen Beweggründen fallen damit nicht darunter, sehr wohl aber auch gezieltes Fotografieren. Überwachtes Objekt ist jene Person, Gegenstand oder Ort, auf die sich die systematische Erfassung von Ereignissen intentional richtet.

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

§ 50a Abs. 3 bestimmt - als lex specialis zu den §§ 8 und 9 – Fälle, in denen schutzwürdige Geheimhaltungsinteressen eines von Videoüberwachung Betroffenen nicht verletzt werden. Z 1 bis 3 regeln zunächst jene Fälle, in denen nach § 1 Abs. 2 keine Interessenabwägung erforderlich ist. Die Zustimmung des Betroffenen (Z 2) muss grundsätzlich ausdrücklich erfolgen. Zu berücksichtigen ist allerdings, dass gewisse Verhaltensweisen insbesondere im öffentlichen Raum typischerweise darauf gerichtet sind, von jedermann wahrgenommen zu werden, und daher einer Zustimmung gleichzuhalten sind (Z 3). Dazu zählt etwa „Straßenkunst“ oder Auftritte im Rahmen von Veranstaltungen.

Die Z 4 bis 6 sind – ebenso wie § 8 Abs. 3 und ein Großteil des § 9 - das Ergebnis typisierender Interessenabwägungen nach § 1 Abs. 2. Dabei war zunächst darauf Bedacht zu nehmen, dass von einer Videoüberwachung erfasste Daten potentiell sensibel sind, weil die Bilder regelmäßig Informationen über den Gesundheitszustand oder die ethnische Zugehörigkeit (Hautfarbe) der Betroffenen liefern werden. Freilich muss auch berücksichtigt werden, dass - im Hinblick auf die Zweckvorgabe in Abs. 2 - Videoüberwachung nicht intentional auf die Gewinnung solcher Daten gerichtet sein darf, diese also nur als „Zufallsprodukt“ anfallen. Somit erfordert die Interessenabwägung verglichen mit § 8 eine einschränkendere Regelung, die freilich noch gewisse unbestimmte Rechtsbegriffe enthält („bestimmte Tatsachen“ in Z 5, die nur demonstrativ konkretisiert werden, Anknüpfen am gesamten Rechtsquellensystem für die Ermittlung von Sorgfaltspflichten in Z 6). Selbstverständlich ist auch der Verhältnismäßigkeitsgrundsatz der §§ 1 Abs. 2 und 7 Abs. 3, insbesondere im Hinblick auf die Tauglichkeit von Videoüberwachung zur Zweckerreichung und das gelindeste Mittel, stets zu beachten. Im Einzelnen ist zu den Erlaubnistatbeständen der Z 4 bis 6 auszuführen:

- Die Überwachung eines Objekts durch bloße Echtzeitwiedergabe (dh. es erfolgt keinerlei Speicherung; Z 1) ist zwar eine Datenanwendung im Sinn des § 4 Z 7 und unterliegt auch der Richtlinie 95/46/EG (vgl. deren Erwägungsgrund 16 sowie Art. 2 lit. b), die Gefährdung schutzwürdiger Geheimhaltungsinteressen ist bei derartigen Systemen, jedoch deutlich herabgesetzt, jedenfalls dann, wenn sie nur Rechtsgüter des Auftraggebers schützen sollen. Der (an sich legitime) Beweissicherungszweck kann durch sie nicht erreicht werden, möglich ist lediglich die Einleitung von (datenschutzrechtlich nicht weiter relevanten) Sofortmaßnahmen, also ein Schutzzweck. Daher kann hier generell von einem Interesse des Auftraggebers ausgegangen werden, das Geheimhaltungsinteressen überwiegt.

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

- Z 5 erlaubt die Videoüberwachung zum Schutz des überwachten Objekts vor gefährlichen Angriffen im Sinn des SPG und ermöglicht es dem Auftraggeber damit, auf konkret belegte Gefährdungssituationen zu reagieren. Im Hinblick darauf, dass es sich um eine Bedrohung mit gerichtlich strafbaren Vorsatztaten handeln muss, ist ein überwiegendes berechtigtes Interesse des Auftraggebers anzunehmen. Dies gilt jedenfalls gegenüber dem strafrechtswidrig handelnden Angreifer, aber auch gegenüber Dritten, denen (auch im Hinblick auf § 50c) verglichen mit der tatsächlichen Verwirklichung bzw. Nichtaufklärung eines gefährlichen Angriffs geringfügige Beeinträchtigung ihres Geheimhaltungsanspruches zugemutet werden kann. Häufig wird es darüber hinaus so sein, dass diese Dritten direkt oder indirekt durch die Abwehr des Angriffs ebenfalls geschützt werden (zB Videoüberwachung zur Bekämpfung von Diebstählen auf einem Bahnhof).

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

- Ebenfalls auf potentiell gefährliche Situationen, die aber nicht durch gefährliche Angriffe erzeugt sein müssen, stellt Z 6 ab. Die Rechtsordnung begegnet solchen häufig mit besonderen Sorgfaltspflichten bzw. Haftungsbestimmungen, die sie bestimmten Personen mit Ingerenz für die gefährliche Situation auferlegt. Solche Bestimmungen sind über die gesamte Rechtsordnung und auf jede ihrer Stufen verteilt (vgl. zB § 1319a ABGB, § 19 Eisenbahngesetz, §§ 6 und 8 Sbg. Veranstaltungsgesetz 1997). Um ihnen nachzukommen, soll der dadurch Verpflichtete Videoüberwachung einsetzen dürfen. Das öffentliche Interesse an der Gewährleistung des durch derartige Vorschriften intendierten Schutzes sowie das Interesse des Verpflichteten, nicht für eine Verletzung derartiger Vorschriften haften zu müssen, überwiegt - vorausgesetzt es handelt sich um ein taugliches bzw. das gelindeste Mittel - das Interesse Dritter, denen derartige Verpflichtungen nicht auferlegt sind und die auch hier regelmäßig die Nutznießer der Schutzvorschriften sein werden.

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

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

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

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

§ 50a Abs. 5 regelt den Umgang mit so genannten „Zufallstreffern“, wenn also im Rahmen einer Videoüberwachung zufällig relevante Ereignisse aufgezeichnet werden, die außerhalb des Zwecks bzw. der Zulässigkeit nach den Abs. 2 und 3 liegen. Eine Verwertung solcher Aufnahmen aus freier Entscheidung des Auftraggebers ist nur dann zulässig, wenn bei ihm der begründete (dh durch objektiv nachvollziehbare Tatsachen belegte) Verdacht entstanden ist, die gefilmten Ereignisse könnten im Zusammenhang mit von Amts wegen zu verfolgenden gerichtlich strafbaren Handlungen stehen, sei es, dass diese schon begangen wurden (Z 1) oder ihre Verwirklichung droht bzw. im Gange ist, dh in der Terminologie des SPG die Videodaten der Abwehr oder Beendigung eines gefährlichen Angriffs dienen könnten. Regelmäßig wird ein derartiger begründeter Verdacht durch einen entsprechenden Hinweis Dritter entstehen.

Klargestellt wird in Abs. 5 weiters, dass der Auftraggeber gegenüber einer Behörde oder einem Gericht nicht die Herausgabe von Videodaten verweigern kann, wenn diese im Zuge eines Verfahrens die Herausgabe als Beweismittel fordern und über entsprechende Durchsetzungsmöglichkeiten (zB §§ 384 ff ZPO, § 19 AVG, §§ 109 ff StPO) verfügen. Die Verantwortung für die Rechtmäßigkeit derartiger Herausgabeforderungen trägt allein das Gericht oder die Behörde.

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

§ 50a Abs. 7 ordnet – nur der Deutlichkeit halber – nochmals die zusätzlich Geltung der allgemeinen Bestimmungen der §§ 6 und 7, insb. des Verhältnismäßigkeitsgrundsatzes, an. Dieser kommt insbesondere auch in § 1 Abs 1 letzter Satz zum Ausdruck, wonach Beschränkungen nur in der gelindesten zum Ziel führenden Art vorgenommen werden dürfen. Sofern taugliche Mittel zur Zielerreichung bestehen, die weniger eingriffsintensiv sind als das Mittel der Videoüberwachung, sind diese jedenfalls einer Videoüberwachung vorzuziehen. Zu denken wäre etwa an den Einsatz von RFID-Chips an Waren in Geschäften zur Sicherung vor Diebstählen. Um dem Sicherheitsbedürfnis mancher Hauseigentümer oder Mieter Rechnung zu tragen, wäre möglicherweise die Verwendung von Sicherheitstüren, Gegensprechanlagen oder Alarmanlagen ausreichend. Grundsätzlich stellt auch der Eingriff durch Echtzeitüberwachung in das Grundrecht auf Datenschutz ein gelinderes Mittel dar als eine Speicherung der dort anfallenden Daten, wobei Echtzeitüberwachung grundsätzlich in allen in § 50a Abs. 3 genannten Fällen möglich ist. Die ausdrückliche Erwähnung der Echtzeitüberwachung in § 50a Abs. 3 Z 4 erfolgt deshalb, weil nur der dort genannte Tatbestand unter die in § 50b Abs. 1 Z 1 normierte Ausnahme von der Meldepflicht fällt. Echtzeitüberwachung wird insbesondere dann ausreichen, wenn eine Videoüberwachung ausschließlich bezweckt, das überwachte Objekt (das auch eine Person sein kann) vor einer Gefahr rechtzeitig schützen zu können bzw. bei Eintreten eines schädigenden Ereignisses (z. B. eines Unfalls) unverzüglich reagieren zu können.

Nach dem Verhältnismäßigkeitsgrundsatz zu beurteilen wird auch die Zulässigkeit einer Gebäudeüberwachung sein, die mehrere Mieter und deren Besucher betrifft. Insbesondere können sich auch Konstellationen ergeben, in denen Rückschlüsse auf besondere sensible Daten der Hausbesucher möglich sind (etwa beim Besuch einer Arztpraxis oder eines politischen Vereines); die Zulässigkeit einer Videoüberwachung kann auch hier nur unter Bedachtnahme auf die konkrete Situation und unter sorgfältiger Abwägung der Geheimhaltungsinteressen der Betroffenen gegenüber den Interessen Dritter – unter Einhaltung des Grundsatzes des gelindesten zum Ziel führenden Mittels – beurteilt werden.

Zu § 50b:

§ 50b Abs. 1 ordnet die lückenlose Protokollierung jedes Verwendungsvorganges bei Videoüberwachung an und lässt daher anders als § 14 Abs. 2 Z 7 bzw. § 14 Abs. 3 keinen Abwägungsspielraum. Die

Anordnung umfasst auch Videoüberwachungen, die als Standardanwendungen betrieben werden. Bei reinen Echtzeitüberwachungen ist freilich keine Protokollierung denkbar und daher auch nicht erforderlich (vgl. auch § 14 Abs. 5).

Abs. 2 schreibt grundsätzlich eine Löschung der durch Videoüberwachung gewonnenen Daten nach 48 Stunden vor. Nur wenn Anhaltspunkte vorliegen, dass die Videoaufzeichnung zur Verwirklichung des Überwachungszwecks aufbewahrt werden muss, aufgezeichnete Daten also im Einzelfall für Schutz- oder Beweissicherungszwecke im Hinblick auf das überwachte Objekt oder für eine Weitergabe nach § 50a Abs. 5 (auch auf Grund der Beweisanforderung durch ein Gericht oder eine Behörde) länger benötigt werden, ist ausnahmsweise eine längere Aufbewahrung (so lange wie es in diesem Einzelfall erforderlich ist) zulässig. Eine regelmäßige längere Aufbewahrung ist nur mit Genehmigung der Datenschutzkommission erlaubt.

Zu § 50c:

§ 50c enthält einige Sonderbestimmungen für die Registrierung von Videoüberwachungen. Abs. 1 stellt allerdings zunächst (implizit) klar, dass § 17 – insbesondere die Möglichkeit der Definition von Standardanwendungen – auch für Videoüberwachungen gilt. Lediglich zwei Fälle werden von der Registrierungspflicht ausgenommen und zwar die bloße Echtzeitüberwachung nach § 50a Abs. 4 Z 4 (s. bereits dort zur vergleichsweise niedrigen Eingriffstiefe) und die Speicherung nur auf einem analogen Speichermedium. Der Einsatz solcher Medien (zB VHS-Videokassette) erfordert zwar zum Teil den Einsatz von Geräten, die automationsunterstützte Elemente enthalten, dennoch ist auf Grund der sehr beschränkten Strukturierbarkeit und damit Suchbarkeit die Gefährdung von Geheimhaltungsinteressen unbeteiligter Dritter deutlich herabgesetzt. Dies rechtfertigt eine Ausnahme von der Meldepflicht, auch nach Art. 18 Abs. 2 erster Unterabsatz der Richtlinie 95/46/EG.

Umgekehrt ist dieses Gefährdungspotential bei den übrigen Fällen der Videoüberwachung insbesondere im Hinblick auf den oft großen Betroffenenkreis und die Verwendung potentiell sensibler Daten gegenüber „herkömmlichen“ Datenanwendungen doch deutlich hinaufgesetzt. Dies erfordert ihre Prüfung im Vorabkontrollverfahren. Da bei Überwachungen nach § 50a Abs. 3 Z 5 durch die Verwendung des Begriffs „bestimmte Tatsachen“ ein beachtlicher Auslegungsspielraum besteht, wird für auf dieser Grundlage gemeldete Videoüberwachungen die Glaubhaftmachung der Tatsachen im Registrierungsverfahren vorgeschrieben. Die Art der zur Glaubhaftmachung für das Vorliegen eines der genannten Tatbestände wird je nach Überwachungssituation variieren: So könnten etwa eine oder mehrere Strafanzeigen vorgelegt werden. Ein ähnliches Gefährdungspotential ist gegeben, wenn sich der Auftraggeber auf Z 7 beruft. Hier könnten etwa eine erhaltene Klage oder eine eigene Klagevorbereitung zur Glaubhaftmachung herangezogen werden.

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

§ 50c Abs. 4 regelt den in der Praxis wohl häufig auftretenden Fall, dass ein Auftraggeber mehrere gleichartige oder räumlich verbundene Objekte auf derselben Rechtsgrundlage überwachen möchte. Dies soll in einer Meldung möglich sein.

Zu § 50d:

§ 50d ist eine Spezialbestimmung zu § 24. Er konkretisiert die Informationsverpflichtung im Fall von Videoüberwachung zu einer Kennzeichnungspflicht (zB durch deutlich lesbare Aufschriften oder Piktogramme). Die Kennzeichnung soll so erfolgen, dass der Überwachung ausgewichen werden kann, was freilich nicht immer machbar sein wird. Sie darf nur dann entfallen wenn eine Abwägung zwischen der Wahrscheinlichkeit der Beeinträchtigung von Betroffeneninteressen oder der Beschaffenheit des überwachten Objekts auf der einen Seite und den Kosten der Überwachung auf der anderen Seite eine unverhältnismäßige Kostenbelastung ergeben würde. Hier sind bewegliche überwachte Objekte besonders hervorzuheben. Weiters darf die Kennzeichnung im Fall einer Überwachung nach § 50a Abs. 3 Z 7 entfallen, wenn dadurch der Zweck der Gewinnung von Beweismitteln beeinträchtigt würde. Die Rechtmäßigkeit des Entfalls der Kennzeichnung ist von der Datenschutzkommission im Registrierungsverfahren zu prüfen.

Zu § 50e:

§ 50e modifiziert schließlich das Auskunftsrecht für Videoüberwachungen. Die Erteilung einer schriftlichen Auskunft wie in § 26 Abs. 1 vorgesehen ist hier hinsichtlich der verarbeiteten Daten aus nahe liegenden Gründen keine transparente Lösung. Daher besteht diesbezüglich grundsätzlich ein Anspruch auf Erhalt der Videoaufzeichnung, die übrigen Auskunftsbestandteile sind schriftlich zu erteilen. Freilich muss der Geheimhaltungsanspruch Dritter gewahrt bleiben. Erlauben diese die

Übersendung der Aufzeichnung an den Betroffenen nicht, so muss auf die schriftliche Auskunftserteilung in Gestalt einer präzisen Beschreibung des verarbeiteten Verhaltens zurückgegriffen werden.

Zu Z 83 (§ 55):

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

Zu Z 87 (§ 61 Abs. 6):

Die im 9a. Abschnitt getroffenen Regelungen über Videoüberwachung entsprechen in vieler Hinsicht der bisherigen Entscheidungspraxis der Datenschutzkommission. Für Fälle, in denen sich die durch den Entwurf geschaffene Rechtslage als strenger erweist und daher bereits registrierte Videoüberwachungen nicht mehr registriert werden könnten, soll im Hinblick auf das Vertrauen der Auftraggeber in die Rechtslage und damit allenfalls verbundene Investitionen ein Betrieb für weitere zwei Jahre möglich sein.

Zu Z 86 und 87 (§ 61 Abs. 8 bis 10):

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

BUNDESKANZLERAMT ¦ VERFASSUNGSDIENST

GZ ● BKA-810.026/0002-V/3/2008
ABTEILUNGSMAIL ● V@BKA.GV.AT
BEARBEITER ● HERR MAG ALEXANDER FLENDROVSKY
PERS. E-MAIL ● ALEXANDER.FLENDROVSKY@BKA.GV.AT
TELEFON ● 01/53115/2836

Antwort bitte unter Anführung der GZ an die Abteilungsmail

An
die Österreichische Präsidentschaftskanzlei
die Parlamentsdirektion
den Rechnungshof
die Volksanwaltschaft
den Verfassungsgerichtshof
den Verwaltungsgerichtshof
alle Bundesministerien
das Büro von Herrn Vizekanzler Mag. MOLTERER
das Büro von Frau Staatssekretärin SILHAVY
das Büro von Herrn Staatssekretär Dr. LOPATKA
das Büro von Herrn Staatssekretär Dr. WINKLER
das Büro von Herrn Staatssekretär Dr. MATZNETTER
das Büro von Frau Staatssekretärin KRANZL
das Büro von Frau Staatssekretärin MAREK
alle Sektionen des Bundeskanzleramtes
alle Abteilungen des Verfassungsdienstes
die Geschäftsstelle Plattform Digitales Österreich beim Bundeskanzleramt
die Bundes-Gleichbehandlungskommission beim Bundeskanzleramt
die Anwaltschaft für Gleichbehandlung
die Geschäftsführung des Bundesseniorenbeirates beim Bundesministerium für Soziales und Konsumentenschutz
den Datenschutzrat
die Datenschutzkommission
den Rat für Forschung und Technologieentwicklung
den Familienpolitischen Beirat beim Bundesministerium für Gesundheit, Familie und Jugend
den unabhängigen Bundesasylsenat
den unabhängigen Umweltsenat
den österreichischen Statistikrat
die Bundesanstalt „Statistik Österreich“
das Präsidium der Finanzprokuratur
die Österreichischen Bundesbahnen Infrastruktur Betrieb AG
die Österreichische Post AG
die Telekom Austria AG
die Bundesgeschäftsstelle des Arbeitsmarktservice Österreich
die Bundes-Jugendvertretung
die Finanzmarktaufsicht
den Unabhängigen Finanzsenat
das Bundesvergabeamt
die Bundeswettbewerbsbehörde

die Kommunikationsbehörde Austria
die Telekom-Control-Kommission
die Rundfunk und Telekom Regulierungs-GmbH
[1]alle Ämter der Landesregierungen
die Verbindungsstelle der Bundesländer
alle unabhängigen Verwaltungssenate
den Verein der Mitglieder der Unabhängigen Verwaltungssenate (UVS-Verein)
* den Österreichischen Gemeindebund
* den Österreichischen Städtebund
die Wirtschaftskammer Österreich
die Bundesarbeitskammer
die Präsidentenkonferenz der Landwirtschaftskammern Österreichs (Landwirtschaftskammer Österreich – LKÖ)
den Österreichischen Landarbeiterkammertag
den Österreichischen Rechtsanwaltskammertag
die Österreichische Notariatskammer
die Österreichische Patentanwaltskammer
die Österreichische Ärztekammer
die Österreichische Zahnärztekammer
die Österreichische Apothekerkammer
die Kammer der Wirtschaftstreuhänder
die Bundeskonferenz der Kammern der freien Berufe
den Verband der Öffentlichen Wirtschaft und Gemeinwirtschaft Österreichs
die rechtswissenschaftliche Fakultät der Universität Wien
die rechtswissenschaftliche Fakultät der Universität Graz
die rechtswissenschaftliche Fakultät der Universität Innsbruck
die rechtswissenschaftliche Fakultät der Universität Salzburg
das Institut für Rechtswissenschaften der Technischen Universität Wien
das Institut für Wirtschaft, Politik und Recht der Universität für Bodenkultur Wien
das Institut für Österreichisches und Europäisches Öffentliches Recht der Wirtschaftsuniversität Wien
die rechtswissenschaftliche Fakultät der Universität Linz
das Institut für Rechtswissenschaften der Universität Klagenfurt
das Institut für Europarecht der Universität Wien
das Institut für Europarecht der Universität Graz
das Zentrum für Europäisches Recht der Universität Innsbruck
das Institut für Europarecht der Universität Salzburg
das Institut für Europarecht der Universität Linz
das Europainstitut der Wirtschaftsuniversität Wien
die Österreichische Rektorenkonferenz
die Österreichische Hochschülerinnen- und Hochschülerschaft
den Verband der Professoren Österreichs
das Österreichische Institut für Rechtspolitik
die Österreichische Gesellschaft für Gesetzgebungslehre
die Österreichische Juristenkommission
das Österreichische Normungsinstitut
die Österreichische Gesellschaft für Schule und Recht
das Österreichische Institut für Menschenrechte
die Österreichische Liga für Menschenrechte
die österreichische Sektion von amnesty international
das Ludwig Boltzmann Institut für Menschenrechte
das österreichische Helsinki Komitee
den Hochkommissär der Vereinten Nationen für die Flüchtlinge
den Hauptverband der österreichischen Sozialversicherungsträger

[1] Zustellung (auch) per Post.

die Österreichische Bischofskonferenz
den Evangelischen Oberkirchenrat A und HB Wien
die Vereinigung der Österreichischen Industrie
den Österreichischen Gewerkschaftsbund
die Gewerkschaft Öffentlicher Dienst
* die Bundessektion Richter und Staatsanwälte der Gewerkschaft Öffentlicher Dienst
die Vereinigung Österreichischer Richter
den Verband Österreichischer Zeitungen
den Österreichischen Seniorenrat
den Hauptverband der Land- und Forstwirtschaftsbetriebe Österreichs
den Österreichischen Verband der Internet Service Provider
die ARGE Daten
den Österreichischen Familienbund
die Gesellschaft des Österreichischen Roten Kreuzes
den Österreichischen Bundesverband für Psychotherapie
das Österreichische Hebammengremium
das Forum Mobilkommunikation

Das Bundeskanzleramt-Verfassungsdienst übermittelt den Entwurf eines Bundesgesetzes, mit dem das Bundesgesetz über den Schutz personenbezogener Daten geändert wird (DSG-Novelle 2008), und ersucht um allfällige Stellungnahme bis spätestens

21. Mai 2008

an die e-mail-adresse v@bka.gv.at.

Auf Folgendes wird besonders hingewiesen:
1. Es sind ausdrücklich – insbesondere vereinfachende - Vorschläge zu einer alternativen Formulierung des Eingriffsvorbehalts in § 1 Abs. 2 DSG 2000 willkommen.
2. Es wird ausdrücklich auch um Stellungnahmen dazu ersucht, ob die Einführung eines „österreichischen Datenschutz-Gütesiegels“ (derzeit nicht im Entwurf enthalten) für sinnvoll und zweckmäßig erachtet wird. Dazu wird auch auf die Website https://www.datenschutzzentrum.de/europrise/ aufmerksam gemacht.

Sollte bis zum oben angegebenen Zeitpunkt keine Stellungnahme einlangen, so wird das Bundeskanzleramt-Verfassungsdienst davon ausgehen, dass gegen den Entwurf keine Einwendungen erhoben werden. Die Aussendung dient gleichzeitig als Übermittlung im Sinne des Art. 1 der Vereinbarung zwischen dem Bund, den Ländern und den Gemeinden über einen Konsultationsmechanismus und einen künftigen Stabilitätspakt der Gebietskörperschaften, BGBl. I Nr. 35/1999, die Stellungnahmefrist im Sinne dieser Vereinbarung endet vier Wochen nach Zustellung.

Weiters wird ersucht,

- die Stellungnahme dem Präsidium des Nationalrates zu übermitteln, und zwar - bei Vorhandensein der technischen Möglichkeit hiezu - im Wege elektronischer Post an die Adresse

  begutachtungsverfahren@parlament.gv.at

- und davon in der Stellungnahme Mitteilung zu machen.

Es wird angemerkt, dass die Aussendung zur Begutachtung nur mehr auf elektronischem Weg erfolgt.

4. März 2008
Für den Bundeskanzler:
Georg LIENBACHER

Elektronisch gefertigt