1613 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP

Ausgedruckt am 18. 3. 1999

Regierungsvorlage

Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG)

Der Nationalrat hat beschlossen:

Inhaltsverzeichnis

Artikel 1 (Verfassungsbestimmung)

§ 1 Grundrecht auf Datenschutz

§ 2 Zuständigkeit

§ 3 Räumlicher Anwendungsbereich

Artikel 2

1. Abschnitt: Allgemeines

§ 4 Definitionen

§ 5 Öffentlicher und privater Bereich

2. Abschnitt: Verwendung von Daten

§ 6 Grundsätze

§ 7 Zulässigkeit der Verwendung von Daten

§ 8 Schutzwürdige Geheimhaltungsinteressen bei Verwendung nichtsensibler Daten

§ 9 Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten

§ 10 Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen

§ 11 Pflichten des Dienstleisters

§ 12 Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland

§ 13 Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland

3. Abschnitt: Datensicherheit

§ 14 Datensicherheitsmaßnahmen

§ 15 Datengeheimnis

4. Abschnitt: Publizität der Datenverarbeitungen

§ 16 Datenverarbeitungsregister

§ 17 Meldepflicht des Auftraggebers

§ 18 Aufnahme der Verarbeitung

§ 19 Notwendiger Inhalt der Meldung

§ 20 Prüfungs- und Verbesserungsverfahren

§ 21 Registrierung

§ 22 Richtigstellung des Registers

§ 23 Pflicht zur Offenlegung nichtmeldepflichtiger Datenanwendungen

§ 24 Informationspflicht des Auftraggebers

§ 25 Pflicht zur Offenlegung der Identität des Auftraggebers

5. Abschnitt: Die Rechte des Betroffenen

§ 26 Auskunftsrecht

§ 27 Recht auf Richtigstellung oder Löschung

§ 28 Widerspruchsrecht

§ 29 Die Rechte des Betroffenen bei Verwendung nur indirekt personenbezogener Daten

6. Abschnitt: Rechtsschutz

§ 30 Kontrollbefugnisse der Datenschutzkommission

§ 31 Beschwerde an die Datenschutzkommission

§ 32 Anrufung der Gerichte

§ 33 Schadenersatz

§ 34 Gemeinsame Bestimmungen

7. Abschnitt: Kontrollorgane

§ 35 Datenschutzkommission und Datenschutzrat

§ 36 Zusammensetzung der Datenschutzkommission

§ 37 Weisungsfreiheit der Datenschutzkommission

§ 38 Organisation und Geschäftsführung der Datenschutzkommission

§ 39 Beschlüsse der Datenschutzkommission

§ 40 Wirkung von Bescheiden der Datenschutzkommission und des geschäftsführenden Mitglieds

§ 41 Einrichtung und Aufgaben des Datenschutzrates

§ 42 Zusammensetzung des Datenschutzrates

§ 43 Vorsitz und Geschäftsführung des Datenschutzrates

§ 44 Sitzungen und Beschlußfassung des Datenschutzrates

8. Abschnitt: Besondere Verwendungszwecke von Daten

§ 45 Private Zwecke

§ 46 Wissenschaftliche Forschung und Statistik

§ 47 Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen

§ 48 Publizistische Tätigkeit

9. Abschnitt: Besondere Verwendungsarten von Daten

§ 49 Automatisierte Einzelentscheidungen

§ 50 Informationsverbundsysteme

10. Abschnitt: Strafbestimmungen

§ 51 Datenverwendung in Gewinn- oder Schädigungsabsicht

§ 52 Verwaltungsstrafbestimmung

11. Abschnitt: Übergangs- und Schlussbestimmungen

§ 53 Befreiung von Gebühren, Verwaltungsabgaben und vom Kostenersatz

§ 54 Mitteilungen an die anderen Mitgliedstaaten der Europäischen Union und an die Europäische Kommission

§ 55 Feststellungen der Europäischen Kommission

§ 56 Verwaltungsangelegenheiten gemäß Art. 30 B-VG

§ 57 Sprachliche Gleichbehandlung

§ 58 Manuelle Dateien

§ 59 Umsetzungshinweis

§ 60 Inkrafttreten

§ 61 Übergangsbestimmungen

§ 62 Verordnungserlassung

§ 63 Verweisungen

§ 64 Vollziehung

Artikel 1

(Verfassungsbestimmung)

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.

(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.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. 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.

(4) Beschränkungen der Rechte nach Abs. 3 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 zuständig, es sei denn, daß Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind.

Zuständigkeit

§ 2. (1) Bundessache ist die Gesetzgebung in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr.

(2) Die Vollziehung solcher Bundesgesetze steht dem Bund zu. Soweit solche Daten von einem Land, im Auftrag eines Landes, von oder im Auftrag von juristischen Personen, die durch Gesetz eingerichtet sind und deren Einrichtung hinsichtlich der Vollziehung in die Zuständigkeit der Länder fällt, verwendet werden, sind diese Bundesgesetze von den Ländern zu vollziehen, soweit nicht durch Bundesgesetz die Datenschutzkommission, der Datenschutzrat oder Gerichte mit der Vollziehung betraut werden.

Räumlicher Anwendungsbereich

§ 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.

(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.

(3) Weiters ist dieses Bundesgesetz nicht anzuwenden, soweit personenbezogene Daten durch das Inland nur durchgeführt werden.

(4) Von den Abs. 1 bis 3 abweichende gesetzliche Regelungen sind nur in Angelegenheiten zulässig, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

Artikel 2

1. Abschnitt

Allgemeines

Definitionen

§ 4. Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten die Begriffe:

1. "Daten" ("personenbezogene Daten"): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; "nur indirekt personenbezogen" sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;

2. "sensible Daten" ("besonders schutzwürdige Daten"): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;

3. "Betroffener": jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden;

4. "Auftraggeber": natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten (Z 9), und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Als Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie einem anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten. Wurde jedoch dem Auftragnehmer anläßlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt oder hat der Auftragnehmer die Entscheidung über die Art und Weise der Verwendung, insbesondere die Vornahme einer Verarbeitung der überlassenen Daten, auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 6 Abs. 4 eigenverantwortlich zu treffen, so gilt der mit der Herstellung des Werkes Betraute als datenschutzrechtlicher Auftraggeber;

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

6. "Datei": strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;

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);

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.

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;

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;

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;

13. "Informationsverbundsystem": die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, daß jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden;

14. "Zustimmung": die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, daß er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt;

15. "Niederlassung": jede durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne Rechtspersönlichkeit, die am Ort ihrer Einrichtung auch tatsächlich Tätigkeiten ausübt.

Öffentlicher und privater Bereich

§ 5. (1) Datenanwendungen sind dem öffentlichen Bereich im Sinne dieses Bundesgesetzes zuzurechnen, wenn sie für Zwecke eines Auftraggebers des öffentlichen Bereichs (Abs. 2) durchgeführt werden.

(2) Auftraggeber des öffentlichen Bereichs sind alle Auftraggeber,

1. die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder

2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

(3) Die dem Abs. 2 nicht unterliegenden Auftraggeber gelten als Auftraggeber des privaten Bereichs im Sinne dieses Bundesgesetzes.

2. Abschnitt

Verwendung von Daten

Grundsätze

§ 6. (1) Daten dürfen nur

1. nach Treu und Glauben und auf rechtmäßige Weise verwendet werde;

2. für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden; die Weiterverwendung für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§ 46 und 47 zulässig;

3. soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;

4. so verwendet werden, daß sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;

5. solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

(2) Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der in Abs. 1 genannten Grundsätze; dies gilt auch dann, wenn er für die Datenanwendung Dienstleister heranzieht.

(3) Der Auftraggeber einer diesem Bundesgesetz unterliegenden Datenanwendung hat, wenn er nicht im Gebiet der Europäischen Union niedergelassen ist, einen in Österreich ansässigen Vertreter zu benennen, der unbeschadet der Möglichkeit eines Vorgehens gegen den Auftraggeber selbst namens des Auftraggebers verantwortlich gemacht werden kann.

(4) Zur näheren Festlegung dessen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist, können für den privaten Bereich die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten. Solche Verhaltensregeln dürfen nur veröffentlicht werden, nachdem sie dem Bundeskanzler zur Begutachtung vorgelegt wurden und dieser ihre Übereinstimmung mit den Bestimmungen dieses Bundesgesetzes begutachtet und als gegeben

erachtet hat.

Zulässigkeit der Verwendung von Daten

§ 7. (1) Daten dürfen nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.

(2) Daten dürfen nur übermittelt werden, wenn

1. sie aus einer gemäß Abs. 1 zulässigen Datenanwendung stammen und

2. der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis – soweit diese nicht außer Zweifel steht – im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und

3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

(3) Die Zulässigkeit einer Datenverwendung setzt voraus, daß die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und daß die Grundsätze des § 6 eingehalten werden.

Schutzwürdige Geheimhaltungsinteressen bei Verwendung nichtsensibler Daten

§ 8. (1) Gemäß § 1 Abs. 1 bestehende schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder

2. der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder

3. lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder

4. überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern.

(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.

(3) Schutzwürdige Geheimhaltungsinteressen sind aus dem Grunde des Abs. 1 Z 4 insbesondere dann nicht verletzt, wenn die Verwendung der Daten

1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder

2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder

3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder

4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenem erforderlich ist oder

5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder

6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat.

(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. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten besteht oder

2. die Verwendung derartiger Daten für Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist oder

3. sich sonst die Zulässigkeit der Verwendung dieser Daten aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegenden berechtigten Interessen des Auftraggebers ergibt und die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen nach diesem Bundesgesetz gewährleistet.

Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten

§ 9. Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn

1. der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder

2. die Daten in nur indirekt personenbezogener Form verwendet werden oder

3. sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen, oder

4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht oder

5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben, oder

6. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder

7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder

8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist oder

9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder

10. Daten für private Zwecke gemäß § 45 oder für wissenschaftliche Forschung oder Statistik gemäß § 46 oder zur Benachrichtigung oder Befragung des Betroffenen gemäß § 47 verwendet werden oder

11. die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse zur Datenverwendung unberührt bleiben, oder

12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder

13. nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten und es sich hiebei um Daten von Mitgliedern, Förderern oder sonstigen Personen handelt, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben; diese Daten dürfen, sofern sich aus gesetzlichen Vorschriften nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden.

Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen

§ 10. (1) Auftraggeber dürfen bei ihren Datenanwendungen Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten. Der Auftraggeber hat mit dem Dienstleister die hiefür notwendigen Vereinbarungen zu treffen und sich von ihrer Einhaltung durch Einholung der erforderlichen Informationen über die vom Dienstleister tatsächlich getroffenen Maßnahmen zu überzeugen.

(2) Die beabsichtigte Heranziehung eines Dienstleisters durch einen Auftraggeber des öffentlichen Bereichs im Rahmen einer Datenanwendung, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegt, ist der Datenschutzkommission mitzuteilen, es sei denn, daß die Inanspruchnahme des Dienstleisters auf Grund ausdrücklicher gesetzlicher Ermächtigung erfolgt oder als Dienstleister eine Organisationseinheit tätig wird, die mit dem Auftraggeber oder einem diesem übergeordneten Organ in einem Über- oder Unterordnungsverhältnis steht. Kommt die Datenschutzkommission zur Auffassung, daß die geplante Inanspruchnahme eines Dienstleisters geeignet ist, schutzwürdige Geheimhaltungsinteressen der Betroffenen zu gefährden, so hat sie dies dem Auftraggeber

unverzüglich mitzuteilen. Im übrigen gilt § 30 Abs. 6 Z 4.

Pflichten des Dienstleisters

§ 11. (1) Unabhängig von allfälligen vertraglichen Vereinbarungen haben Dienstleister bei der Verwendung von Daten für den Auftraggeber jedenfalls folgende Pflichten:

1. die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden; insbesondere ist die Übermittlung der verwendeten Daten ohne Auftrag des Auftraggebers verboten;

2. alle gemäß § 14 erforderlichen Datensicherheitsmaßnahmen zu treffen; insbesondere dürfen für die Dienstleistung nur solche Mitarbeiter herangezogen werden, die sich dem Dienstleister gegenüber zur Einhaltung des Datengeheimnisses verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen;

3. weitere Dienstleister nur mit Billigung des Auftraggebers heranzuziehen und deshalb den Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen, daß er dies allenfalls untersagen kann;

4. – sofern dies nach der Art der Dienstleistung in Frage kommt – im Einvernehmen mit dem Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen;

5. nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten;

6. dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der unter Z 1 bis 5 genannten Verpflichtungen notwendig sind.

(2) Vereinbarungen zwischen dem Auftraggeber und dem Dienstleister über die nähere Ausgestaltung der in Abs. 1 genannten Pflichten sind zum Zweck der Beweissicherung schriftlich festzuhalten.

Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland

§ 12. (1) Die Übermittlung und Überlassung von Daten an Empfänger in Mitgliedstaaten der Europäischen Union ist keinen Beschränkungen im Sinne des § 13 unterworfen. Dies gilt nicht für den Datenverkehr zwischen Auftraggebern des öffentlichen Bereichs in Angelegenheiten, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

(2) Keiner Genehmigung gemäß § 13 bedarf weiters der Datenverkehr mit Empfängern in Drittstaaten mit angemessenem Datenschutz. Welche Drittstaaten angemessenen Datenschutz gewährleisten, wird unter Beachtung des § 55 Z 1 durch Verordnung des Bundeskanzlers festgestellt. Maßgebend für die Angemessenheit des Schutzes ist die Ausgestaltung der Grundsätze des § 6 Abs. 1 in der ausländischen Rechtsordnung und das Vorhandensein wirksamer Garantien für ihre Durchsetzung.

(3) Darüberhinaus ist der Datenverkehr ins Ausland dann genehmigungsfrei, wenn

1. die Daten im Inland zulässigerweise veröffentlicht wurden oder

2. Daten, die für den Empfänger nur indirekt personenbezogen sind, übermittelt oder überlassen werden oder

3. die Übermittlung oder Überlassung von Daten ins Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind, oder

4. Daten aus Datenanwendungen für private Zwecke (§ 45) oder für publizistische Tätigkeit (§ 48) übermittelt werden oder

5. der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat oder

6. ein vom Auftraggeber mit dem Betroffenen oder mit einem Dritten eindeutig im Interesse des Betroffenen abgeschlossener Vertrag nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann oder

7. die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und rechtmäßig ermittelt wurden, oder

8. die Übermittlung oder Überlassung in einer Standardverordnung (§ 17 Abs. 2 Z 6) oder Musterverordnung (§ 19 Abs. 2) ausdrücklich angeführt ist oder

9. es sich um Datenverkehr mit österreichischen Dienststellen im Ausland

handelt oder

10. Übermittlungen oder Überlassungen aus Datenanwendungen erfolgen, die gemäß § 17 Abs. 3 von der Meldepflicht ausgenommen sind.

(4) Wenn eine Übermittlung oder Überlassung von Daten ins Ausland in Fällen, die von den vorstehenden Absätzen nicht erfaßt sind,

1. zur Wahrung eines wichtigen öffentlichen Interesses oder

2. zur Wahrung eines lebenswichtigen Interesses einer Person

notwendig und so dringlich ist, daß die gemäß § 13 erforderliche Genehmigung der Datenschutzkommission nicht eingeholt werden kann, ohne die genannten Interessen zu gefährden, darf sie ohne Genehmigung vorgenommen werden, muß aber der Datenschutzkommission umgehend mitgeteilt werden.

(5) Voraussetzung für die Zulässigkeit jeder Übermittlung oder Überlassung in das Ausland ist die Rechtmäßigkeit der Datenanwendung im Inland gemäß § 7. Bei Überlassungen ins Ausland muß darüber hinaus die schriftliche Zusage des ausländischen Dienstleisters an den inländischen Auftraggeber – oder in den Fällen des § 13 Abs. 5 an den inländischen Dienstleister – vorliegen, daß er die Dienstleisterpflichten gemäß § 11 Abs. 1 einhalten werde. Dies entfällt, wenn die Dienstleistung im Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind.

Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland

§ 13. (1) Soweit der Datenverkehr mit dem Ausland nicht gemäß § 12 genehmigungsfrei ist, hat der Auftraggeber vor der Übermittlung oder Überlassung von Daten in das Ausland eine Genehmigung der Datenschutzkommission (§§ 35 ff) einzuholen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen binden.

(2) Die Genehmigung ist unter Beachtung der gemäß § 55 Z 2 ergangenen Kundmachungen zu erteilen, wenn die Voraussetzungen des § 12 Abs. 5 vorliegen und wenn, ungeachtet des Fehlens eines im Empfängerstaat generell geltenden angemessenen Datenschutzniveaus,

1. für die im Genehmigungsantrag angeführte Übermittlung oder Überlassung im konkreten Einzelfall angemessener Datenschutz besteht; dies ist unter Berücksichtigung aller Umstände zu beurteilen, die bei der Datenverwendung eine Rolle spielen, wie insbesondere die Art der verwendeten Daten, die Zweckbestimmung sowie die Dauer der geplanten Verwendung, das Herkunfts- und das Endbestimmungsland und die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen, Standesregeln und Sicherheitsstandards; oder

2. der Auftraggeber glaubhaft macht, daß die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Hiefür können insbesondere auch vertragliche Zusicherungen des Empfängers an den Antragsteller über die näheren Umstände der Datenverwendung im Ausland von Bedeutung sein.

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

(4) Bei meldepflichtigen Datenanwendungen hat die Datenschutzkommission eine Ausfertigung jedes Bescheides, mit dem eine Übermittlung oder Überlassung von Daten in das Ausland genehmigt wurde, zum Registrierungsakt zu nehmen und die Erteilung der Genehmigung im Datenverarbeitungsregister (§ 16) anzumerken.

(5) Abweichend von Abs. 1 kann auch ein inländischer Dienstleister die Genehmigung beantragen, wenn er zur Erfüllung seiner vertraglichen Verpflichtungen gegenüber mehreren Auftraggebern jeweils einen bestimmten weiteren Dienstleister im Ausland heranziehen will. Die tatsächliche Überlassung darf jeweils nur mit Zustimmung des Auftraggebers erfolgen. Der Auftraggeber hat der Datenschutzkommission mitzuteilen, aus welcher seiner meldepflichtigen Datenanwendungen die dem Dienstleister genehmigte Überlassung erfolgen soll; dies ist im Datenverarbeitungsregister anzumerken.

(6) Die Übermittlung von Daten an ausländische Vertretungsbehörden oder zwischenstaatliche Einrichtungen in Österreich gilt hinsichtlich der Pflicht zur Einholung von Genehmigungen nach Abs. 1 als Datenverkehr mit dem Ausland.

3. Abschnitt

Datensicherheit

Datensicherheitsmassnahmen

§ 14. (1) Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie

unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, daß die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, daß ihre Verwendung ordnungsgemäß erfolgt und daß die Daten Unbefugten nicht zugänglich sind.

(2) Insbesondere ist, soweit dies im Hinblick auf Abs. 1 letzter Satz erforderlich ist,

1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,

2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,

3. jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,

4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,

5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,

6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,

7. Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,

8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(3) Nicht registrierte Übermittlungen aus Datenanwendungen, die einer Verpflichtung zur Auskunftserteilung gemäß § 26 unterliegen, sind so zu protokollieren, daß dem Betroffenen Auskunft gemäß § 26 gegeben werden kann. In der Standardverordnung (§ 17 Abs. 2 Z 6) oder in der Musterverordnung (§ 19 Abs. 2) vorgesehene Übermittlungen bedürfen keiner Protokollierung.

(4) Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck – das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes – unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, es sei denn, daß es sich um die Verwendung zum Zweck der Verhinderung oder Verfolgung eines Verbrechens handelt, das mit mindestens fünfjähriger Freiheitsstrafe bedroht ist.

(5) Sofern gesetzlich nicht ausdrücklich anderes angeordnet ist, sind Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird.

(6) Datensicherheitsvorschriften sind so zu erlassen und zur Verfügung zu halten, daß sich die Mitarbeiter über die für sie geltenden Regelungen jederzeit informieren können.

Datengeheimnis

§ 15. (1) Auftraggeber, Dienstleister und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben Daten aus Datenanwendungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Auftraggeber und Dienstleister haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, daß sie Daten aus Datenanwendungen nur auf Grund von Anordnungen übermitteln und das Datengeheimnis auch nach Beendigung des Arbeits(Dienst)verhältnisses zum Auftraggeber oder Dienstleister einhalten werden.

(3) Auftraggeber und Dienstleister dürfen Anordnungen zur Übermittlung von Daten nur erteilen, wenn dies nach den Bestimmungen dieses Bundesgesetzes zulässig ist. Sie haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden

Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur Datenübermittlung wegen Verstoßes gegen die Bestimmungen dieses Bundesgesetzes kein Nachteil erwachsen.

4. Abschnitt

Publizität der Datenanwendungen

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.

(2) Jedermann kann in das Register Einsicht nehmen. In den Registrierungsakt einschließlich darin allenfalls enthaltener Genehmigungsbescheide ist Einsicht zu gewähren, wenn der Einsichtswerber glaubhaft macht, daß er Betroffener ist, und soweit nicht überwiegende schutzwürdige Geheimhaltungsinteressen des Auftraggebers oder anderer Personen entgegenstehen.

(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.

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.

(2) Nicht meldepflichtig sind Datenanwendungen, die

1. ausschließlich veröffentlichte Daten enthalten oder

2. die Führung von Registern oder Verzeichnissen zum Inhalt haben, die von Gesetzes wegen öffentlich einsehbar sind, sei es auch nur bei Nachweis eines berechtigten Interesses oder

3. nur indirekt personenbezogene Daten enthalten oder

4. von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten vorgenommen werden (§ 45) oder

5. für publizistische Tätigkeit gemäß § 48 vorgenommen werden oder

6. einer Standardanwendung entsprechen: Der Bundeskanzler kann durch Verordnung Typen von Datenanwendungen und Übermittlungen aus diesen zu Standardanwendungen erklären, wenn sie von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verwendungszwecks und der verarbeiteten Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist. In der Verordnung sind für jede Standardanwendung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen.

(3) Weiters sind Datenanwendungen für Zwecke

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder

2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder

3. der Sicherstellung der Interessen der umfassenden Landesverteidigung 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

von der Meldepflicht ausgenommen, soweit dies zur Verwirklichung des Zweckes der Datenanwendung notwendig ist.

Aufnahme der Verarbeitung

§ 18. (1) Der Vollbetrieb einer meldepflichtigen Datenanwendung darf – außer in den Fällen

des Abs. 2 – unmittelbar nach Abgabe der Meldung aufgenommen werden.

(2) Meldepflichtige Datenanwendungen, die weder einer Musteranwendung nach § 19 Abs. 2 entsprechen noch innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften 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.

Notwendiger Inhalt der Meldung

§ 19. (1) Eine Meldung im Sinne des § 17 hat zu enthalten:

1. den Namen (die sonstige Bezeichnung) und die Anschrift des Auftraggebers sowie eines allfälligen Vertreters gemäß § 6 Abs. 3 oder eines Betreibers gemäß § 50 Abs. 1, weiters die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde, und

2. den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit des Auftraggebers, soweit dies erforderlich ist, und

3. den Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z 2 ergeben, und

4. die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten und

5. die Kreise der von beabsichtigten Übermittlungen Betroffenen, die zu übermittelnden Datenarten und die zugehörigen Empfängerkreise – einschließlich allfälliger ausländischer Empfängerstaaten – sowie die Rechtsgrundlagen der Übermittlung und

6. – soweit eine Genehmigung der Datenschutzkommission notwendig ist – die Geschäftszahl der Genehmigung durch die Datenschutzkommission sowie

7. allgemeine Angaben über die getroffenen Datensicherheitsmaßnahmen im Sinne des § 14, die eine vorläufige Beurteilung der Angemessenheit der Sicherheitsvorkehrungen erlauben.

(2) Wenn eine größere Anzahl von Auftraggebern gleichartige Datenanwendungen vorzunehmen hat und die Voraussetzungen für die Erklärung zur Standardanwendung nicht vorliegen, kann der Bundeskanzler durch Verordnung Musteranwendungen festlegen. Meldungen über Datenanwendungen, die inhaltlich einer Musteranwendung entsprechen, müssen nur folgendes enthalten:

1. die Bezeichnung der Datenanwendung gemäß der Musterverordnung und

2. die Bezeichnung und Anschrift des Auftraggebers sowie den Nachweis seiner gesetzlichen Zuständigkeit oder seiner rechtlichen Befugnis, soweit dies erforderlich ist, und

3. die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde.

(3) Eine Meldung ist mangelhaft, wenn Angaben fehlen, offenbar unrichtig, unstimmig oder so unzureichend sind, daß Einsichtnehmer im Hinblick auf die Wahrnehmung ihrer Rechte nach diesem Bundesgesetz keine hinreichende Information darüber gewinnen können, ob durch die Datenanwendung ihre schutzwürdigen Geheimhaltungsinteressen verletzt sein könnten. Unstimmigkeit liegt insbesondere auch dann vor, wenn der Inhalt einer gemeldeten Datenanwendung durch die gemeldeten Rechtsgrundlagen nicht gedeckt ist.

Prüfungs- und Verbesserungsverfahren

§ 20. (1) Die Datenschutzkommission hat alle Meldungen binnen zwei Monaten zu prüfen. Kommt sie hiebei zur Auffassung, daß eine Meldung im Sinne des § 19 Abs. 3 mangelhaft ist, so ist dem Auftraggeber längstens innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung des Mangels unter Setzung einer Frist aufzutragen.

(2) 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.

(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.

(4) Wird einem Verbesserungsauftrag nicht fristgerecht entsprochen, so hat die Datenschutzkommission die Registrierung mit Bescheid abzulehnen; andernfalls gilt die Meldung als ursprünglich richtig eingebracht.

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

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

Registrierung

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

1. das Prüfungsverfahren die Zulässigkeit der Registrierung ergeben hat oder

2. zwei Monate nach Einlangung der Meldung bei der Datenschutzkommission verstrichen sind, ohne daß ein Verbesserungsauftrag gemäß § 20 Abs. 1 erteilt wurde oder

3. der Auftraggeber die verlangten Verbesserungen fristgerecht vorgenommen hat.

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

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

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

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

Richtigstellung des Registers

§ 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.

(2) Gelangen der Datenschutzkommission aus amtlichen Verlautbarungen Änderungen in der Bezeichnung oder der Anschrift des Auftraggebers zur Kenntnis, so sind die Eintragungen von Amts wegen zu berichtigen. Ergibt sich aus einer amtlichen Verlautbarung der Wegfall der Rechtsgrundlage des Auftraggebers, ist von Amts wegen die Streichung aus dem Register anzuordnen.

(3) Änderungen oder Streichungen nach Abs. 2 sind ohne weiteres Ermittlungsverfahren durch Bescheid zu verfügen.

(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.

Pflicht zur Offenlegung nicht-meldepflichtiger Datenanwendungen

§ 23. (1) Auftraggeber einer Standardanwendung haben jedermann auf Anfrage mitzuteilen, welche Standardanwendungen sie tatsächlich vornehmen.

(2) Nicht-meldepflichtige Datenanwendungen sind der Datenschutzkommission bei Ausübung ihrer Kontrollaufgaben gemäß § 30 offenzulegen.

Informationspflicht des Auftraggebers

§ 24. (1) Der Auftraggeber einer Datenanwendung hat aus Anlaß der Ermittlung von Daten die Betroffenen in geeigneter Weise

1. über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und

2. über Namen und Adresse des Auftraggebers,

zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles

nicht bereits vorliegen.

(2) Über Abs. 1 hinausgehende Informationen sind in geeigneter Weise zu geben, wenn dies für eine Verarbeitung nach Treu und Glauben erforderlich ist; dies gilt insbesondere dann, wenn

1. gegen eine beabsichtigte Verarbeitung oder Übermittlung von Daten ein Widerspruchsrecht des Betroffenen gemäß § 28 besteht oder

2. es für den Betroffenen nach den Umständen des Falles nicht klar erkennbar ist, ob er zur Beantwortung der an ihn gestellten Fragen rechtlich verpflichtet ist, oder

3. Daten in einem Informationsverbundsystem verarbeitet werden sollen, ohne daß dies gesetzlich vorgesehen ist.

(3) Werden Daten nicht durch Befragung des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Auftraggebers oder aus Anwendungen anderer Auftraggeber ermittelt, darf die Information gemäß Abs. 1 entfallen, wenn

1. die Datenverwendung durch Gesetz oder Verordnung vorgesehen ist oder

2. die Information im Hinblick auf die mangelnde Erreichbarkeit von Betroffenen unmöglich ist oder

3. wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert. Dies liegt insbesondere dann vor, wenn Daten für Zwecke der wissenschaftlichen Forschung oder Statistik gemäß § 46 oder Adreßdaten im Rahmen des § 47 ermittelt werden und die Information des Betroffenen in diesen Bestimmungen nicht ausdrücklich vorgeschrieben ist. Der Bundeskanzler kann durch Verordnung weitere Fälle festlegen, in welchen die Pflicht zur Information entfällt.

(4) Keine Informationspflicht besteht bei jenen Datenanwendungen, die gemäß § 17 Abs. 2 und 3 nicht meldepflichtig sind.

Pflicht zur Offenlegung der Identität des Auftraggebers

§ 25. (1) Bei Übermittlungen und bei Mitteilungen an Betroffene hat der Auftraggeber seine Identität in geeigneter Weise offenzulegen, sodaß den Betroffenen die Verfolgung ihrer Rechte möglich ist. Bei meldepflichtigen Datenanwendungen ist in Mitteilungen an Betroffene die Registernummer des Auftraggebers anzuführen.

(2) Werden Daten aus einer Datenanwendung für Zwecke einer vom Auftraggeber verschiedenen Person verwendet, ohne daß diese ihrerseits ein Verfügungsrecht über die verwendeten Daten und damit die Eigenschaft eines Auftraggebers in Bezug auf die Daten erlangt, dann ist bei Mitteilungen an den Betroffenen neben der Identität der Person, für deren Zwecke die Daten verwendet werden, auch die Identität des Auftraggebers anzugeben, aus dessen Datenanwendung die Daten stammen. Handelt es sich hiebei um eine meldepflichtige Datenanwendung, ist die Registernummer des Auftraggebers beizufügen. Diese Pflicht trifft sowohl den Auftraggeber als auch denjenigen, in dessen Namen die Mitteilung an den Betroffenen erfolgt.

5. Abschnitt

Die Rechte des Betroffenen

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.

(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

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder

2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder

3. der Sicherung der umfassenden Landesverteidigung 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.

(3) Der Betroffene 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.

(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.

(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 260 S verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.

(7) Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Betroffenen innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 31 an die Datenschutzkommission bis zum rechtskräftigen Abschluß des Verfahrens nicht vernichten.

(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.

(9) 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.

Recht auf Richtigstellung oder Löschung

§ 27. (1) Jeder Auftraggeber hat unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes verarbeitete Daten richtigzustellen oder zu löschen, und zwar

1. aus eigenem, sobald ihm die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder

2. auf begründeten Antrag des Betroffenen.

Der Pflicht zur Richtigstellung nach Z 1 unterliegen nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist. Die Unvollständigkeit verwendeter Daten bewirkt nur dann einen Berichtigungsanspruch, wenn sich aus der Unvollständigkeit im Hinblick auf den Zweck der Datenanwendung die Unrichtigkeit der Gesamtinformation ergibt. Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, daß ihre Archivierung rechtlich zulässig ist und daß der Zugang zu diesen Daten besonders geschützt ist. Die Weiterverwendung von Daten für einen anderen Zweck ist nur zulässig, wenn eine Übermittlung der Daten für diesen Zweck zulässig ist; die Zulässigkeit der Weiterverwendung für wissenschaftliche oder statistische Zwecke ergibt sich aus den §§ 46 und 47.

(2) Der Beweis der Richtigkeit der Daten obliegt – sofern gesetzlich nicht ausdrücklich anderes angeordnet ist – dem Auftraggeber, soweit die Daten nicht ausschließlich auf Grund

von Angaben des Betroffenen ermittelt wurden.

(3) Eine Richtigstellung oder Löschung von Daten ist ausgeschlossen, soweit der Dokumentationszweck einer Datenanwendung nachträgliche Änderungen nicht zuläßt. Die erforderlichen Richtigstellungen sind diesfalls durch entsprechende zusätzliche Anmerkungen zu bewirken.

(4) Innerhalb von acht Wochen nach Einlangen eines Antrags auf Richtigstellung oder Löschung ist dem Antrag zu entsprechen und dem Betroffenen davon Mitteilung zu machen oder schriftlich zu begründen, warum die verlangte Löschung oder Richtigstellung nicht vorgenommen wird.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in § 26 Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Geheimhaltung erfordern, mit einem Richtigstellungs- oder Löschungsantrag folgendermaßen zu verfahren: Die Richtigstellung oder Löschung ist vorzunehmen, wenn das Begehren des Betroffenen nach Auffassung des Auftraggebers berechtigt ist. Die gemäß Abs. 4 erforderliche Mitteilung an den Betroffenen hat in allen Fällen dahingehend zu lauten, daß die Überprüfung der Datenbestände des Auftraggebers im Hinblick auf das Richtigstellungs- oder Löschungsbegehren durchgeführt wurde. 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) Wenn die Löschung oder Richtigstellung von Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann, sind bis dahin die zu löschenden Daten für den Zugriff zu sperren und die zu berichtigenden Daten mit einer berichtigenden Anmerkung zu versehen.

(7) Werden Daten verwendet, deren Richtigkeit der Betroffene bestreitet, und läßt sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen, so ist auf Verlangen des Betroffenen ein Vermerk über die Bestreitung beizufügen. Der Bestreitungsvermerk darf nur mit Zustimmung des Betroffenen oder auf Grund einer Entscheidung des zuständigen Gerichtes oder der Datenschutzkommission gelöscht werden.

(8) Wurden im Sinne des Abs. 1 richtiggestellte oder gelöschte Daten vor der Richtigstellung oder Löschung übermittelt, so hat der Auftraggeber die Empfänger dieser Daten hievon in geeigneter Weise zu verständigen, sofern dies keinen unverhältnismäßigen Aufwand, insbesondere im Hinblick auf das Vorhandensein eines berechtigten Interesses an der Verständigung, bedeutet und die Empfänger noch feststellbar sind.

(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.

Widerspruchsrecht

§ 28. (1) Sofern die Verwendung von Daten nicht gesetzlich vorgesehen ist, hat jeder Betroffene das Recht, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben, beim Auftraggeber der Datenanwendung Widerspruch zu erheben. Der Auftraggeber hat bei Vorliegen dieser Voraussetzungen die Daten des Betroffenen binnen acht Wochen aus seiner Datenanwendung zu löschen und allfällige Übermittlungen zu unterlassen.

(2) Gegen eine nicht gesetzlich angeordnete Aufnahme in eine öffentlich zugängliche Datei kann der Betroffene jederzeit auch ohne Begründung seines Begehrens Widerspruch erheben. Die Daten sind binnen acht Wochen zu löschen.

Die Rechte des Betroffenen bei der Verwendung nur indirekt personenbezogener Daten

§ 29. Die durch die §§ 26 bis 28 gewährten Rechte können nicht geltend gemacht werden, soweit nur indirekt personenbezogene Daten verwendet werden.

6. Abschnitt

Rechtsschutz

Kontrollbefugnisse der Datenschutzkommission

§ 30. (1) Jedermann kann sich wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten eines Auftraggebers oder Dienstleisters nach diesem Bundesgesetz mit einer Eingabe an die Datenschutzkommission wenden.

(2) Die Datenschutzkommission kann im Fall eines begründeten Verdachtes auf Verletzung der

im Abs. 1 genannten Rechte und Pflichten Datenanwendungen überprüfen. Hiebei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenanwendungen und diesbezügliche Unterlagen begehren.

(3) Datenanwendungen, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegen, dürfen auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden. Dies gilt auch für jene Bereiche der Vollziehung, in welchen ein Auftraggeber des öffentlichen Bereichs die grundsätzliche Anwendbarkeit der §§ 26 Abs. 5 und 27 Abs. 5 in Anspruch nimmt.

(4) Zum Zweck der Einschau ist die Datenschutzkommission nach Verständigung des Inhabers der Räumlichkeiten und des Auftraggebers (Dienstleisters) berechtigt, Räume, in welchen Datenanwendungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern herzustellen. Der Auftraggeber (Dienstleister) hat die für die Einschau notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte des Auftraggebers (Dienstleisters) und Dritter auszuüben.

(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, das mit mindestens fünfjähriger Freiheitsstrafe bedroht ist, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch dem Ersuchen der Strafgerichte nach § 26 StPO 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 Bereichs Klage vor dem zuständigen Gericht gemäß § 32 Abs. 4 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.

(7) Der Einschreiter ist darüber zu informieren, wie mit seiner Eingabe verfahren wurde.

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.

(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.

(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.

(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. Wird diesem Bescheid 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 berichtigt oder gelöscht wurden.

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.

(2) Sind Daten entgegen den Bestimmungen dieses Bundesgesetzes verwendet worden, so hat der Betroffene Anspruch auf Unterlassung und Beseitigung des diesem Bundesgesetz widerstreitenden Zustandes.

(3) Zur Sicherung der auf dieses Bundesgesetz gestützten Ansprüche auf Unterlassung können einstweilige Verfügungen erlassen werden, auch wenn die in § 381 EO bezeichneten Voraussetzungen nicht zutreffen. Dies gilt auch für Verfügungen über die Verpflichtung zur Anbringung eines Bestreitungsvermerks.

(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.

(5) Die Datenschutzkommission hat in Fällen, in welchen der begründete Verdacht einer schwerwiegenden Datenschutzverletzung durch einen Auftraggeber des privaten Bereichs besteht, gegen diesen eine Feststellungsklage (§ 228 ZPO) bei dem gemäß Abs. 4 zweiter Satz zuständigen Gericht zu erheben.

(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.

Schadenersatz

§ 33. (1) Ein Auftraggeber oder Dienstleister, der Daten schuldhaft entgegen den Bestimmungen dieses Bundesgesetzes verwendet, hat dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen. Werden durch die öffentlich zugängliche Verwendung der in § 18 Abs. 2 Z 1 bis 3 genannten Datenarten schutzwürdige Geheimhaltungsinteressen eines Betroffenen in einer Weise verletzt, die einer Eignung zur Bloßstellung gemäß § 7 Abs. 1 des Mediengesetzes, BGBl. Nr. 314/1981, gleichkommt, so gilt diese Bestimmung auch in Fällen, in welchen die öffentlich zugängliche Verwendung nicht in Form der Veröffentlichung in einem Medium geschieht. Der Anspruch auf angemessene Entschädigung für die erlittene Kränkung ist gegen den Auftraggeber der Datenverwendung geltend zu machen.

(2) Der Auftraggeber und der Dienstleister haften auch für das Verschulden ihrer Leute, soweit deren Tätigkeit für den Schaden ursächlich war.

(3) Der Auftraggeber kann sich von seiner Haftung befreien, wenn er nachweist, daß der Umstand, durch den der Schaden eingetreten ist, ihm und seinen Leuten (Abs. 2) nicht zur Last gelegt werden kann. Dasselbe gilt für die Haftungsbefreiung des Dienstleisters. Für den Fall eines Mitverschuldens des Geschädigten oder einer Person, deren Verhalten er zu vertreten hat, gilt § 1304 ABGB.

(4) Die Zuständigkeit für Klagen nach Abs. 1 richtet sich nach § 32 Abs. 4.

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.

(2) Eingaben nach § 30, Beschwerden nach § 31, Klagen nach § 32 sowie Schadenersatzansprüche nach § 33 können nicht nur auf die Verletzung der Vorschriften dieses Bundesgesetzes, sondern auch auf die Verletzung von datenschutzrechtlichen Vorschriften eines anderen Mitgliedstaates der Europäischen Union gegründet werden, soweit solche Vorschriften gemäß § 3 im Inland anzuwenden sind.

(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.

(4) Die Datenschutzkommission hat den Unabhängigen Datenschutzkontrollstellen der anderen Mitgliedstaaten der Europäischen Union über Ersuchen Amtshilfe zu leisten.

7. Abschnitt

Kontrollorgane

Datenschutzkommission und Datenschutzrat

§ 35. (1) Zur Wahrung des Datenschutzes sind nach den näheren Bestimmungen dieses Bundesgesetzes – unbeschadet der Zuständigkeit des Bundeskanzlers und der ordentlichen Gerichte – die Datenschutzkommission und der Datenschutzrat berufen.

(2) **(Verfassungsbestimmung)** Die Datenschutzkommission übt ihre Befugnisse auch gegenüber den in Art. 19 B-VG bezeichneten obersten Organen der Vollziehung aus.

Zusammensetzung der Datenschutzkommission

§ 36. (1) Die Datenschutzkommission besteht aus sechs Mitgliedern, die auf Vorschlag der Bundesregierung vom Bundespräsidenten für die Dauer von fünf Jahren bestellt werden. Wiederbestellungen sind zulässig. Die Mitglieder müssen rechtskundig sein. Ein Mitglied muß dem Richterstand angehören.

(2) Die Vorbereitung des Vorschlages der Bundesregierung für die Bestellung der Mitglieder der Datenschutzkommission obliegt dem Bundeskanzler. Er hat dabei Bedacht zu nehmen auf:

1. einen Dreiervorschlag des Präsidenten des Obersten Gerichtshofs für das richterliche Mitglied,

2. einen Vorschlag der Länder für zwei Mitglieder,

3. einen Dreiervorschlag der Bundeskammer für Arbeiter und Angestellte für ein Mitglied,

4. einen Dreiervorschlag der Wirtschaftskammer Österreich für ein Mitglied.

Alle vorgeschlagenen Personen sollen Erfahrung auf dem Gebiet des Datenschutzes besitzen.

(3) Ein Mitglied ist aus dem Kreise der rechtskundigen Bundesbeamten vorzuschlagen.

(4) Für jedes Mitglied ist ein Ersatzmitglied zu bestellen. Das Ersatzmitglied tritt bei Verhinderung des Mitglieds an dessen Stelle. Die Funktionsperiode des Ersatzmitglieds endet mit der Funktionsperiode des Mitglieds; für den Fall der vorzeitigen Beendigung der Funktionsperiode des Mitglieds gilt Abs. 8.

(5) Der Datenschutzkommission können nicht angehören:

1. Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre;

2. Personen, die zum Nationalrat nicht wählbar sind.

(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.

(7) Auf die Ersatzmitglieder sind die Abs. 2, 3, 5 und 6 wie auf Mitglieder anzuwenden.

(8) Scheidet ein Mitglied wegen Todes, freiwillig oder gemäß Abs. 6 vorzeitig aus, so wird das betreffende Ersatzmitglied (Abs. 4) Mitglied der Datenschutzkommission bis zum Ablauf der Funktionsperiode des ausgeschiedenen Mitglieds. Unter Anwendung der Abs. 2 und 3 ist für diese Zeit ein neues Ersatzmitglied zu bestellen. Scheidet ein Ersatzmitglied vorzeitig aus, ist unverzüglich eines neues Ersatzmitglied zu bestellen.

(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.

Weisungsfreiheit der Datenschutzkommission

§ 37. (1) **(Verfassungsbestimmung)** Die Mitglieder der Datenschutzkommission sind in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden.

(2) Die in der Geschäftsstelle der Datenschutzkommission tätigen Bediensteten unterstehen fachlich nur den Weisungen des Vorsitzenden oder des geschäftsführenden Mitglieds 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 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.

(2) Für die Unterstützung in der Geschäftsführung der Datenschutzkommission hat der Bundeskanzler eine Geschäftsstelle einzurichten und die notwendige Sach- und Personalausstattung bereitzustellen.

(3) Die Datenschutzkommission ist vor Erlassung von Verordnungen anzuhören, die auf der Grundlage dieses Bundesgesetzes ergehen oder sonst wesentliche Fragen des Datenschutzes unmittelbar betreffen.

(4) Die Datenschutzkommission hat spätestens alle zwei Jahre einen Bericht über ihre Tätigkeit zu erstellen und in geeigneter Weise zu veröffentlichen. Der Bericht ist dem Bundeskanzler zur Kenntnis zu übermitteln.

Beschlüsse der Datenschutzkommission

§ 39. (1) Die Datenschutzkommission ist bei Anwesenheit aller sechs Mitglieder beschlußfähig. Für den Fall der Verhinderung eines Mitglieds gilt § 36 Abs. 4.

(2) Das richterliche Mitglied führt den Vorsitz.

(3) Für einen gültigen Beschluß der Datenschutzkommission ist die Zustimmung der Mehrheit der abgegebenen Stimmen notwendig. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig.

(4) Entscheidungen der Datenschutzkommission von grundsätzlicher Bedeutung für die Allgemeinheit sind von der Datenschutzkommission unter Beachtung der Erfordernisse der Amtsverschwiegenheit in geeigneter Weise zu veröffentlichen.

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.

(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.

(3) Bescheide, mit welchen gemäß § 13 Übermittlungen oder Überlassungen von Daten ins Ausland genehmigt wurden, sind zu widerrufen, wenn die rechtlichen und tatsächlichen Voraussetzungen für die Erteilung der Genehmigung, insbesondere auch infolge einer gemäß § 55 ergangenen Kundmachung des Bundeskanzlers, nicht mehr bestehen.

(4) Wenn die Datenschutzkommission eine Verletzung von Bestimmungen dieses Bundesgesetzes durch einen Auftraggeber des öffentlichen Bereichs festgestellt hat, so hat dieser mit den ihm zu Gebote stehenden rechtlichen Mitteln unverzüglich den der Rechtsanschauung der Datenschutzkommission entsprechenden Zustand herzustellen.

Einrichtung und Aufgaben des Datenschutzrates

§ 41. (1) Beim Bundeskanzleramt ist ein Datenschutzrat eingerichtet.

(2) Der Datenschutzrat berät die Bundesregierung und die Landesregierungen auf deren Ersuchen in rechtspolitischen Fragen des Datenschutzes. Zur Erfüllung dieser Aufgabe

1. kann der Datenschutzrat Fragen von grundsätzlicher Bedeutung für den Datenschutz in Beratung ziehen;

2. ist dem Datenschutzrat Gelegenheit zur Stellungnahme zu Gesetzesentwürfen der Bundesministerien zu geben, soweit diese datenschutzrechtlich von Bedeutung sind;

3. haben Auftraggeber des öffentlichen Bereichs ihre Vorhaben dem Datenschutzrat zur Stellungnahme zuzuleiten, soweit diese datenschutzrechtlich von Bedeutung sind;

4. hat der Datenschutzrat das Recht, von Auftraggebern des öffentlichen Bereichs Auskünfte und Berichte sowie die Einsicht in Unterlagen zu verlangen, soweit dies zur datenschutzrechtlichen Beurteilung von Vorhaben mit wesentlichen Auswirkungen auf den Datenschutz in Österreich notwendig ist;

5. kann der Datenschutzrat Auftraggeber des privaten Bereichs oder auch ihre

gesetzliche Interessenvertretung zur Stellungnahme zu Entwicklungen von allgemeiner Bedeutung auffordern, die aus datenschutzrechtlicher Sicht Anlaß zu Bedenken, zumindest aber Anlaß zur Beobachtung geben;

6. kann der Datenschutzrat seine Beobachtungen, Bedenken und allfälligen Anregungen zur Verbesserung des Datenschutzes in Österreich der Bundesregierung und den Landesregierungen mitteilen, sowie über Vermittlung dieser Organe den gesetzgebenden Körperschaften zur Kenntnis bringen.

(3) Abs. 2 Z 3 und 4 gilt nicht, soweit innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften betroffen sind.

Zusammensetzung des Datenschutzrates

§ 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;

2. je ein Vertreter der Bundeskammer für Arbeiter und Angestellte und der Wirtschaftskammer Österreich;

3. zwei Vertreter der Länder;

4. je ein Vertreter des Gemeindebundes und des Städtebundes;

5. ein vom Bundeskanzler zu ernennender Vertreter des Bundes.

(2) Die in Abs. 1 Z 3, 4 und 5 genannten Vertreter sollen berufliche Erfahrung auf dem Gebiet der Informatik und des Datenschutzes haben.

(3) Für jedes Mitglied ist ein Ersatzmitglied namhaft zu machen.

(4) Dem Datenschutzrat können Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre und weiters Personen, die zum Nationalrat nicht wählbar sind, nicht angehören.

(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.

(6) Die Tätigkeit der Mitglieder des Datenschutzrates ist ehrenamtlich. Mitglieder des Datenschutzrates, die außerhalb von Wien wohnen, haben im Fall der Teilnahme an Sitzungen des Datenschutzrates Anspruch auf Ersatz der Reisekosten (Gebührenstufe 3) nach Maßgabe der für Bundesbeamte geltenden Rechtsvorschriften.

Vorsitz und Geschäftsführung des Datenschutzrates

§ 43. (1) Der Datenschutzrat gibt sich mit Beschluß eine Geschäftsordnung.

(2) Der Datenschutzrat hat aus seiner Mitte einen Vorsitzenden und zwei stellvertretende Vorsitzende zu wählen. Die Funktionsperiode des Vorsitzenden und der stellvertretenden Vorsitzenden dauert – unbeschadet des § 42 Abs. 5 – fünf Jahre. Wiederbestellungen sind zulässig.

(3) Die Geschäftsführung des Datenschutzrates obliegt dem Bundeskanzleramt. Der Bundeskanzler hat das hiefür notwendige Personal zur Verfügung zu stellen. Bei ihrer Tätigkeit für den Datenschutzrat sind die Bediensteten des Bundeskanzleramtes fachlich an die Weisungen des Vorsitzenden des Datenschutzrates gebunden.

Sitzungen und Beschlußfassung des Datenschutzrates

§ 44. (1) Die Sitzungen des Datenschutzrates werden vom Vorsitzenden nach Bedarf einberufen. Begehrt ein Mitglied die Einberufung einer Sitzung, so hat der Vorsitzende die Sitzung so einzuberufen, daß sie binnen vier Wochen stattfinden kann.

(2) Zu den Sitzungen kann der Vorsitzende nach Bedarf Sachverständige zuziehen.

(3) Für Beratungen und Beschlußfassungen im Datenschutzrat ist die Anwesenheit von mehr als der Hälfte seiner Mitglieder erforderlich. Zur Beschlußfassung genügt die einfache Mehrheit der abgegebenen Stimmen. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig. Die Beifügung von Minderheitenvoten ist zulässig.

(4) Der Datenschutzrat kann aus seiner Mitte ständige oder nichtständige Arbeitsausschüsse bilden, denen er die Vorbereitung, Begutachtung und Bearbeitung einzelner Angelegenheiten übertragen kann. Er ist auch berechtigt, die Geschäftsführung, Vorbegutachtung und die Bearbeitung einzelner Angelegenheiten einem einzelnen Mitglied (Berichterstatter) zu

übertragen.

(5) Jedes Mitglied des Datenschutzrates ist verpflichtet, an den Sitzungen – außer im Fall der gerechtfertigten Verhinderung – teilzunehmen. Ist ein Mitglied an der Teilnahme verhindert, hat es hievon unverzüglich das Ersatzmitglied zu verständigen.

(6) Mitglieder der Datenschutzkommission, die dem Datenschutzrat nicht angehören, sind berechtigt, an den Sitzungen des Datenschutzrates oder seiner Arbeitsausschüsse teilzunehmen. Ein Stimmrecht steht ihnen nicht zu.

(7) Die Beratungen in der Sitzung des Datenschutzrates sind, soweit er nicht selbst anderes beschließt, vertraulich.

(8) Die Mitglieder des Datenschutzrates, die anwesenden Mitglieder der Datenschutzkommission und die zur Sitzung gemäß Abs. 2 zugezogenen Sachverständigen sind zur Verschwiegenheit über alle ihnen ausschließlich aus ihrer Tätigkeit im Datenschutzrat bekanntgewordenen Tatsachen verpflichtet, sofern die Geheimhaltung im öffentlichen Interesse oder im Interesse einer Partei geboten ist.

8. Abschnitt

Besondere Verwendungszwecke von Daten

Private Zwecke

§ 45. (1) Für ausschließlich persönliche oder familiäre Tätigkeiten dürfen natürliche Personen Daten verarbeiten, wenn sie ihnen vom Betroffenen selbst mitgeteilt wurden oder ihnen sonst rechtmäßigerweise, insbesondere in Übereinstimmung mit § 7 Abs. 2, zugekommen sind.

(2) Daten, die eine natürliche Person für ausschließlich persönliche oder familiäre Tätigkeiten verarbeitet, dürfen, soweit gesetzlich nicht ausdrücklich anderes vorgesehen ist, für andere Zwecke nur mit Zustimmung des Betroffenen übermittelt werden.

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.

(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.

(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 zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten, notwendig ist.

(4) Rechtliche Beschränkungen der Zulässigkeit der Benützung von Daten aus anderen, insbesondere urheberrechtlichen Gründen bleiben unberührt.

(5) Auch in jenen Fällen, in welchen gemäß den vorstehenden Bestimmungen die Verwendung

von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der direkte Personsbezug unverzüglich zu verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit nur indirekt personenbezogenen Daten das Auslangen gefunden werden kann. Sofern gesetzlich nicht ausdrücklich anderes vorgesehen ist, ist der Personsbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.

Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen

§ 47. (1) Soweit gesetzlich nicht ausdrücklich anderes bestimmt ist, bedarf die Übermittlung von Adreßdaten eines bestimmten Kreises von Betroffenen zum Zweck ihrer Benachrichtigung oder Befragung der Zustimmung der Betroffenen.

(2) Wenn allerdings angesichts der Auswahlkriterien für den Betroffenenkreis und des Gegenstands der Benachrichtigung oder Befragung eine Beeinträchtigung der Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist, bedarf es keiner Zustimmung, wenn

1. Daten desselben Auftraggebers verwendet werden oder

2. bei einer beabsichtigten Übermittlung der Adreßdaten an Dritte

   a) an der Benachrichtigung oder Befragung auch ein öffentliches Interesse besteht oder

   b) der Betroffene nach entsprechender Information über Anlaß und Inhalt der Übermittlung innerhalb angemessener Frist keinen Widerspruch gegen die Übermittlung erhoben hat.

(3) Liegen die Voraussetzungen des Abs. 2 nicht vor und würde die Einholung der Zustimmung der Betroffenen gemäß Abs. 1 einen unverhältnismäßigen Aufwand erfordern, ist die Übermittlung der Adreßdaten mit Genehmigung der Datenschutzkommission gemäß Abs. 4 zulässig, falls die Übermittlung an Dritte

1. zum Zweck der Benachrichtigung oder Befragung aus einem wichtigen Interesse des Betroffenen selbst oder

2. aus einem wichtigen öffentlichen Benachrichtigungs- oder Befragungsinteresse oder

3. zur Befragung der Betroffenen für wissenschaftliche oder statistische Zwecke

erfolgen soll.

(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.

(5) Die übermittelten Adreßdaten dürfen ausschließlich für den genehmigten Zweck verwendet werden und sind zu löschen, sobald sie für die Benachrichtigung oder Befragung nicht mehr benötigt werden.

(6) In jenen Fällen, in welchen es gemäß den vorstehenden Bestimmungen zulässig ist, Namen und Adresse von Personen, die einem bestimmten Betroffenenkreis angehören, zu übermitteln, dürfen auch die zum Zweck der Auswahl der zu übermittelnden Adreßdaten notwendigen Verarbeitungen vorgenommen werden.

Publizistische Tätigkeit

§ 48. (1) Soweit Medienunternehmen, Mediendienste oder ihre Mitarbeiter Daten unmittelbar für ihre publizistische Tätigkeit im Sinne des Mediengesetzes verwenden, sind von den einfachgesetzlichen Bestimmungen des vorliegenden Bundesgesetzes nur die §§ 4 bis 6, 10, 11, 14 und 15 anzuwenden.

(2) Die Verwendung von Daten für Tätigkeiten nach Abs. 1 ist insoweit zulässig, als dies zur Erfüllung der Informationsaufgabe der Medienunternehmer, Mediendienste und ihrer Mitarbeiter in Ausübung des Grundrechtes auf freie Meinungsäußerung gemäß Art. 10 Abs. 1 EMRK erforderlich ist.

(3) Im übrigen gelten die Bestimmungen des Mediengesetzes, insbesondere seines dritten Abschnitts über den Persönlichkeitsschutz.

9. Abschnitt

Besondere Verwendungsarten von Daten

Automatisierte Einzelentscheidungen

§ 49. (1) Niemand darf einer für ihn rechtliche Folgen nach sich ziehenden oder einer ihn erheblich beeinträchtigenden Entscheidung unterworfen werden, die ausschließlich auf Grund einer automationsunterstützten Verarbeitung von Daten zum Zweck der Bewertung einzelner Aspekte seiner Person ergeht, wie beispielsweise seiner beruflichen Leistungsfähigkeit, seiner Kreditwürdigkeit, seiner Zuverlässigkeit oder seines Verhaltens.

(2) Abweichend von Abs. 1 darf eine Person einer ausschließlich automationsunterstützt erzeugten Entscheidung unterworfen werden, wenn

1. dies gesetzlich ausdrücklich vorgesehen ist oder

2. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrages ergeht und dem Ersuchen des Betroffenen auf Abschluß oder Erfüllung des Vertrages stattgegeben wurde oder

3. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen – beispielsweise die Möglichkeit, seinen Standpunkt geltend zu machen – garantiert wird.

(3) Dem Betroffenen ist bei automatisierten Einzelentscheidungen auf Antrag der logische Ablauf der automatisierten Entscheidungsfindung in allgemein verständlicher Form darzulegen.

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 acht Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen; dasselbe gilt für diesbezügliche 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.

(3) Die Bestimmungen der Abs. 1 und 2 gelten nicht, soweit infolge der besonderen, insbesondere internationalen Struktur eines bestimmten Informationsverbundsystems gesetzlich ausdrücklich anderes vorgesehen ist.

10. Abschnitt

Strafbestimmungen

Datenverwendung in Gewinn- oder Schädigungsabsicht

§ 51. (1) Wer in der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, benützt, insbesondere einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Verwaltungsstrafbestimmung

§ 52. (1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 260 000 S zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält oder

2. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 15) übermittelt, insbesondere Daten, die ihm gemäß §§ 46 oder 47 anvertraut wurden, vorsätzlich für andere Zwecke verwendet oder

3. Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht

beauskunftet, nicht richtigstellt oder nicht löscht oder

4. Daten vorsätzlich entgegen § 26 Abs. 7 löscht.

(2) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 130 000 S zu ahnden ist, wer

1. Daten ermittelt, verarbeitet oder übermittelt, ohne seine Meldepflicht gemäß § 17 erfüllt zu haben oder

2. Daten ins Ausland übermittelt oder überläßt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 13 eingeholt zu haben oder

3. seine Offenlegungs- oder Informationspflichten gemäß den §§ 23, 24 oder 25 verletzt oder

4. die gemäß § 14 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht läßt.

(3) Der Versuch ist strafbar.

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

(5) Zuständig für Entscheidungen nach Abs. 1 bis 4 ist die Bezirksverwaltungsbehörde, in deren Sprengel der Auftraggeber (Dienstleister) seinen gewöhnlichen Aufenthalt oder Sitz hat. Falls ein solcher im Inland nicht gegeben ist, ist die am Sitz der Datenschutzkommission eingerichtete Bezirksverwaltungsbehörde zuständig.

11. Abschnitt

Übergangs- und Schlußbestimmungen

Befreiung von Gebühren, Abgaben und vom Kostenersatz

§ 53. (1) Die durch dieses Bundesgesetz unmittelbar veranlaßten Eingaben der Betroffenen zur Wahrung ihrer Interessen sowie die Eingaben im Registrierungsverfahren und die gemäß § 21 Abs. 3 zu erstellenden Registerauszüge sind von den Stempelgebühren und von den Verwaltungsabgaben des Bundes befreit.

(2) Für Abschriften aus dem Datenverarbeitungsregister, die ein Betroffener zur Verfolgung seiner Rechte benötigt, ist kein Kostenersatz zu verlangen.

Mitteilungen an die Europäische Kommission und an die anderen Mitgliedstaaten der Europäischen Union

§ 54. (1) Von der Erlassung eines Bundesgesetzes, das die Zulässigkeit der Verarbeitung sensibler Daten betrifft, hat der Bundeskanzler anläßlich der Kundmachung des Gesetzes im Bundesgesetzblatt der Europäischen Kommission Mitteilung zu machen.

(2) Die Datenschutzkommission hat den anderen Mitgliedstaaten der Europäischen Union und der Europäischen Kommission mitzuteilen, in welchen Fällen

1. keine Genehmigung für den Datenverkehr in ein Drittland erteilt wurde, weil die Voraussetzungen des § 13 Abs. 2 Z 1 nicht als gegeben erachtet wurden;

2. der Datenverkehr in ein Drittland ohne angemessenes Datenschutzniveau genehmigt wurde, weil die Voraussetzungen des § 13 Abs. 2 Z 2 als gegeben erachtet wurden.

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

1. das Vorliegen oder Nichtvorliegen eines angemessenen Datenschutzniveaus in einem Drittland oder

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.

Verwaltungsangelegenheiten gemäß Art. 30 B-VG

§ 56. Der Präsident des Nationalrats ist Auftraggeber jener Datenanwendungen, die für

Zwecke der ihm gemäß Art. 30 B-VG übertragenen Angelegenheiten durchgeführt werden. Übermittlungen von Daten aus solchen Datenanwendungen dürfen nur über Auftrag des Präsidenten des Nationalrats vorgenommen werden. Der Präsident trifft Vorsorge dafür, daß im Falle eines Übermittlungsauftrags die Voraussetzungen des § 7 Abs. 2 vorliegen und insbesondere die Zustimmung des Betroffenen in jenen Fällen eingeholt wird, in welchen dies gemäß § 7 Abs. 2 mangels einer anderen Rechtsgrundlage für die Übermittlung notwendig ist.

Sprachliche Gleichbehandlung

§ 57. Soweit in diesem Artikel auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise. Bei der Anwendung der Bezeichnungen auf bestimmte natürliche Personen ist die jeweils geschlechtsspezifische Form zu verwenden.

Manuelle Dateien

§ 58. Soweit manuell, dh. ohne Automationsunterstützung geführte Dateien für Zwecke solcher Angelegenheiten bestehen, in denen die Zuständigkeit zur Gesetzgebung Bundessache ist, gelten sie als Datenanwendungen im Sinne des § 4 Z 7. § 17 gilt mit der Maßgabe, daß die Meldepflicht nur für solche Dateien besteht, deren Inhalt gemäß § 18 Abs. 2 der Vorabkontrolle unterliegt.

Umsetzungshinweis

§ 59. Mit diesem Bundesgesetz wird die 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, umgesetzt.

Inkrafttreten

§ 60. (1) **(Verfassungsbestimmung)** Die Verfassungsbestimmungen des Art. 1, der §§ 35 Abs. 1, 37, 38 Abs. 1 und 61 Abs. 4 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.

(2) Die übrigen Bestimmungen dieses Bundesgesetzes treten ebenfalls mit 1. Jänner 2000 in Kraft.

Übergangsbestimmungen

§ 61. (1) Meldungen, die vor Inkrafttreten dieses Bundesgesetzes an das Datenverarbeitungsregister erstattet wurden, gelten als Meldungen im Sinne des § 17, soweit sie nicht im Hinblick auf das Entfallen von Meldepflichten gemäß § 17 Abs. 2 oder 3 gegenstandslos geworden sind. Desgleichen gelten vor Inkrafttreten dieses Bundesgesetzes durchgeführte Registrierungen als Registrierungen im Sinne des § 21.

(2) Soweit nach der neuen Rechtslage eine Genehmigung für die Übermittlung von Daten ins Ausland erforderlich ist, muß für Übermittlungen, für die eine Genehmigung vor Inkrafttreten dieses Bundesgesetzes erteilt wurde, eine Genehmigung vor dem 1. Jänner 2003 neu beantragt werden. Wird der Antrag rechtzeitig gestellt, dürfen solche Übermittlungen bis zur rechtskräftigen Entscheidung über den Genehmigungsantrag fortgeführt werden.

(3) Datenschutzverletzungen, die vor dem Inkrafttreten dieses Bundesgesetzes stattgefunden haben, sind, soweit es sich um die Feststellung der Rechtmäßigkeit oder Rechtswidrigkeit eines Sachverhalts handelt, nach der Rechtslage zum Zeitpunkt der Verwirklichung des Sachverhalts zu beurteilen; soweit es sich um die Verpflichtung zu einer Leistung oder Unterlassung handelt, ist die Rechtslage im Zeitpunkt der Entscheidung in erster Instanz zugrundezulegen. Ein strafbarer Tatbestand ist nach jener Rechtslage zu beurteilen, die für den Täter in ihrer Gesamtauswirkung günstiger ist; dies gilt auch für das Rechtsmittelverfahren.

(4) **(Verfassungsbestimmung)** Datenanwendungen, die für die in § 17 Abs. 3 genannten Zwecke notwendig sind, dürfen auch bei Fehlen einer im Sinne des § 1 Abs. 2 ausreichenden gesetzlichen Grundlage bis 31. Dezember 2007 vorgenommen werden, in den Fällen des § 17 Abs. 3 Z 1 bis 3 jedoch bis zur Erlassung eines Bundesgesetzes über die Aufgaben und Befugnisse in diesen Bereichen.

(5) Manuelle Datenanwendungen, die gemäß § 58 der Meldepflicht unterliegen, sind, soweit sie schon im Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bestanden haben, dem Datenverarbeitungsregister bis spätestens 1. Jänner 2003 zu melden. Dasselbe gilt für automationsunterstützte Datenanwendungen gemäß § 17 Abs. 3, für die durch die nunmehr geltende Rechtslage die Meldepflicht neu eingeführt wurde.

(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.

Verordnungserlassung

§ 62. Verordnungen auf Grund dieses Bundesgesetzes in seiner jeweiligen Fassung dürfen bereits von dem Tag an erlassen werden, der der Kundmachung der durchzuführenden Gesetzesbestimmungen folgt; sie dürfen jedoch nicht vor den durchzuführenden Gesetzesbestimmungen in Kraft treten.

Verweisungen

§ 63. Soweit in diesem Bundesgesetz auf Bestimmungen anderer Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden.

Vollziehung

§ 64. Mit der Vollziehung dieses Bundesgesetzes sind, soweit sie nicht der Bundesregierung oder den Landesregierungen obliegt, der Bundeskanzler und die anderen Bundesminister im Rahmen ihres Wirkungsbereiches betraut.

Vorblatt

Problem:

Gemäß Art. 32 Abs. 1 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 (Fundstelle: Amtsblatt NR. L 281 vom 23. November 1995, S. 0031 bis 0050; CELEX-Dokumentnummer: 395L0046) ist diese Richtlinie bis spätestens 24. Oktober 1998 in den nationalen Rechtsordnungen der EU-Mitgliedstaaten umzusetzen. Für Österreich besteht daher insofern akuter Umsetzungsbedarf, als einige inhaltliche Erfordernisse der Richtlinie 95/46/EG im geltenden DSG, BGBl. Nr. 565/1978 in der geltenden Fassung, nicht vollständig oder in etwas anderer Ausprägung enthalten sind.

Lösung:

Erlassung eines neuen Datenschutzgesetzes zum Zweck der

1. vollen Umsetzung der Richtlinie 95/46/EG und

2. Einarbeitung jenes Änderungsbedarfes, der sich aus den österreichischen Anwendungserfahrungen zum DSG , BGBl. Nr. 565/1978 in der geltenden Fassung, ergeben hat

Alternativen:

Keine.

EU-Konformität:

Gegeben, da Richtlinienumsetzung.

Mehrkosten: verursacht durch

1. **zusätzliche Pflichten der Auftraggeber:**

Informationspflicht gemäß § 24 des Entwurfs: voraussichtlich kein ins Gewicht fallender Kostenfaktor für den einzelnen Auftraggeber (vgl. hiezu die nähere Begründung im allgemeinen Teil der Erläuterungen, Punkt 13); da im übrigen die Informationspflicht durch die Richtlinie 95/46/EG vorgeschrieben ist, handelt es sich um nicht vermeidbare Mehrkosten, die in allen Mitgliedstaaten der EU anfallen.

Pflicht zur Registrierung von manuellen Dateien, die der Vorabkontrolle unterliegen: betrifft nur sehr wenige Datenanwendungen, deren Anzahl im übrigen tendenziell sinkend ist (vgl. hiezu die näheren Ausführungen im allgemeinen Teil der Erläuterungen, Punkt 13); im übrigen ergibt sich die Registrierungspflicht – zumindest im vorgesehenen eingeschränkten Rahmen – aus der Richtlinie 95/46/EG, sodaß es sich um nicht vermeidbare Mehrkosten handelt, die in allen Mitgliedstaaten der EU anfallen.

Pflicht zur Auskunftserteilung, Richtigstellung und Löschung bei manuellen Dateien:

voraussichtlich kein ins Gewicht fallender Kostenfaktor (vgl. hiezu die nähere Begründung im allgemeinen Teil der Erläuterungen, Punkt 13); die Einräumung dieser Rechte ist durch die Richtlinie 95/46/EG zwingend vorgesehen; es handelt sich also um unvermeidbare Mehrkosten, die in allen EU-Mitgliedstaaten anfallen.

2. **zusätzliche Kompetenzen der Datenschutzkommission** (unter gleichzeitiger Berücksichtigung der vorgesehenen Verwaltungsvereinfachungen durch Kompetenzabbau):

4 Planstellen (1 Informatiker (A/a), 3 Juristen); daraus ergeben sich Mehrkosten von jährlich zirka 4 000 000 S;

da diese Kompetenzänderungen weitestgehend durch die Richtlinie 95/46/EG vorgeschrieben sind, handelt es sich um nicht vermeidbare Mehrkosten.

3. zwei **zusätzliche Mitglieder (und Ersatzmitglieder) der Datenschutzkommission:**

Unter der Annahme, daß durch die Erhöhung der Zahl der als Berichterstatter tätigen Mitglieder der Datenschutzkommission die Belastung des einzelnen Berichterstatters gleichbleibt und daher die monatliche Remunerierung von durchschnittlich 5 500 S nicht erhöht werden muß, ergibt dies jährliche Zusatzkosten von zirka 265 000 S.

4. **zusätzliche Verwaltungsstrafverfahren infolge neuer Straftatbestände:**

diesbezüglich ist mit keinen Mehrkosten zu rechnen (Begründung siehe im allgemeinen Teil der Erläuterungen, Punkt 13).

5. **elektronische Registrierung:**

Kosten der Entwicklung: einmalig anfallend zirka 8 600 000 S

Kosten für den Betrieb: jährlich anfallend zirka 4 700 000 S

6. **Entfall der Registrierungsgebühr:**

jährlich etwa 500 000 S unter Berücksichtigung des Umstandes, daß Standardverarbeitungen in Hinkunft nicht mehr registrierungspflichtig sein sollen. Der Entfall der Registrierungsgebühr ist auch deshalb sinnvoll, weil sonst die durch elektronische Registrierung erzielbaren Einsparungseffekte wieder zunichte gemacht würden, solange es keine Möglichkeit der Bezahlung auf elektronischem Weg gibt.

Einsparungen: ermöglicht durch

1. wesentliche Verringerung der genehmigungspflichtigen Fälle im internationalen Datenverkehr (etwa um 60%): Einsparungen vor allem für Auftraggeber des privaten Bereichs und für die Datenschutzkommission, bei der in den letzten Jahren etwa 100 Genehmigungsverfahren jährlich durchgeführt wurden

2. Abschaffung der Meldepflicht für Standardverarbeitungen (– stellen im privaten Bereich etwa 30% der Registrierungen dar): Einsparungen vor allem für Auftraggeber des privaten Bereichs und für das Datenverarbeitungsregister

3. Vereinfachung des Verfahrens der amtswegigen Berichtigung des Datenverarbeitungsregisters
(– derzeit finden im Jahr etwa 150 diesbezügliche Verfahren vor der Datenschutzkommission statt): Einsparungen vor allem für die Datenschutzkommission und das Datenverarbeitungsregister

4. Abschaffung der Verpflichtung zur Erlassung von Datenschutzverordnungen: Einsparungen vor allem für die Auftraggeber des öffentlichen Bereichs.

Erläuterungen

Allgemeiner Teil

1. Am 24. Oktober 1995 wurde die "**Richtlinie 95/46/EG** des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" verabschiedet. Art. 32 Abs. 1 dieser Richtlinie gibt den Mitgliedsstaaten eine dreijährige Frist zur Umsetzung der Richtlinie in das innerstaatliche Recht. Für Österreich besteht daher insofern akuter Umsetzungsbedarf, als einige inhaltliche Erfordernisse der Richtlinie 95/46/EG im geltenden DSG, BGBl. Nr. 565/1978 in der geltenden Fassung, nicht vollständig oder in etwas anderer Ausprägung enthalten sind.

Ziel der Richtlinie ist die **Harmonisierung der Datenschutzvorschriften** der Mitgliedstaaten der Europäischen Union. Dies ist die Voraussetzung dafür, daß in Hinkunft kein Mitgliedstaat mehr den grenzüberschreitenden Datenverkehr innerhalb des EU-Gebiets im Interesse des Datenschutzes besonderen Prüfungen oder Genehmigungen unterwerfen darf. Das EU-Gebiet soll auch im Hinblick auf die Kommunikation personenbezogener Daten ein Raum sein, in dem der freie Verkehr von Daten im Hinblick auf das Funktionieren des Binnenmarktes durch nationale Grenzen nicht behindert wird bei gleichzeitiger Wahrung des Schutzes der Grundrechte (vgl. hiezu auch Damann/Simitis, EG-Datenschutzrichtlinie-Kommentar, 1997, S. 65).

2. In Österreich wurde ursprünglich davon ausgegangen, daß eine **Novelle zum Datenschutzgesetz,** BGBl. Nr. 565/1978, zur Umsetzung der Richtlinie 95/46/EG genügen werde. In den Vorberatungen zur Erarbeitung dieser Novelle wurde aber mehrfach der Wunsch geäußert, die Zweiteilung des einfachgesetzlichen Teiles des Datenschutzgesetzes in einen öffentlichen Bereich und einen privaten Bereich aufzugeben, um dadurch die beachtlichen Redundanzen im geltenden Gesetzestext in Zukunft zu vermeiden. Dieser Wunsch konnte nur in Form eines **neuen Datenschutzgesetzes** verwirklicht werden, wobei allerdings die

Zweigleisigkeit des Rechtsschutzes (Datenschutzkommission im öffentlichen Bereich und ordentliche Gerichte im privaten Bereich) im wesentlichen aufrecht erhalten wurde.

3. Auch wenn der vorliegende Entwurf ein neues Gesetz zum Inhalt hat, versucht er dennoch, **bewährte Regelungsstrukturen grundsätzlich aufrecht zu erhalten.** Es gibt daher nach wie vor ein Grundrecht auf Datenschutz (§ 1), das in umfangreichen einfachgesetzlichen Bestimmungen (§§ 4 bis 64) ausgeführt wird. Als Neuerung im Grundrecht ist der besondere Schutz für sensible Daten durch entsprechende Anweisung an den einfachen Gesetzgeber zu erwähnen (§ 1 Abs. 2): In Umsetzung der Richtlinie wird die Verarbeitung sensibler Daten verboten, sofern nicht anderes in einfachen Gesetzen aus wichtigen öffentlichen Interessen vorgesehen ist.

Die **Betroffenenrechte,** die schon bisher im Grundrecht gegenüber automationsunterstützter Verwendung von Daten garantiert waren, wurden nunmehr **auf die Verwendung von Daten in manueller, strukturierter Form (zB in Karteien, Listen usw.) ausgedehnt,** wie es die Richtlinie verlangt.

4. Die **Zulässigkeitsvoraussetzungen** für die Ermittlung, Verarbeitung und Übermittlung von Daten waren neu zu formulieren, und zwar zum ersten deshalb, weil öffentlicher und privater Bereich nunmehr zusammengefaßt sind, und zum anderen, weil die Artikel 6, 7 und 8 der Richtlinie 95/46/EG entsprechend zu berücksichtigen waren. Wie in der Richtlinie vorgezeichnet, wird nunmehr den Bestimmungen über die Zulässigkeit der Datenverwendung ein Katalog von **"Grundsätzen"** vorangestellt, der die obersten Prinzipien rechtmäßigen Umgangs mit personenbezogenen Daten enthält.

5. Die Forderung nach möglichster **Publizität von Datenanwendungen** wurde in dem von der Richtlinie erforderlichen Ausmaß nachvollzogen. An sich besitzt Österreich – im Gegensatz zu den meisten anderen EU-Mitgliedsstaaten – ein fast lückenloses System von Meldepflichten an das Datenverarbeitungsregister. Doch auch vor diesem Hintergrund dürfen die zusätzlichen Informations- und Offenlegungspflichten der Auftraggeber nicht als unnötige Erschwernis angesehen werden, da insbesondere die **Informationspflicht des Auftraggebers** einen echten Informations-Mehrwert für den Betroffenen bedeutet, wodurch die Wahrung seiner Rechte wesentlich erleichtert wird.

Der Einführung neuer Informationspflichten steht eine **Verminderung des Registrierungsaufwandes** gegenüber, die dadurch bewirkt wird, daß Standardverarbeitungen in Zukunft nicht mehr registrierungspflichtig sein sollen. Dies ist damit zu rechtfertigen, daß Standardverarbeitungen in Hinkunft nur mehr für jene Fälle vorgesehen werden dürfen, in denen die Beeinträchtigung von Betroffeneninteressen unwahrscheinlich ist, was bedeutet, daß Standardverarbeitungen nur mehr solche Fälle des täglichen Lebens betreffen werden, in denen jedermann ohnehin damit rechnen muß, daß seine Daten in bestimmte Datenverarbeitung (etwa: seiner Vertragspartner) einfließen.

6. Als weitere verwaltungsvereinfachende Maßnahme wurde die **Notwendigkeit der Erlassung von Datenschutzverordnungen beseitigt.**

7. Wesentliche **Änderungen** mußten in Umsetzung der Richtlinie 95/46/EG hinsichtlich **des Datenverkehrs mit dem Ausland** vorgesehen werden. Das Konzept der Richtlinie geht davon aus, daß innerhalb des EU-Gebiets keine Beschränkung des Datenverkehrs stattfindet, der Datenverkehr in Drittländer aber nur zulässig ist, wenn dort ein angemessenes Datenschutzniveau garantiert ist. Ein derart rigoroses Konzept bedarf selbstverständlich zahlreicher Ausnahmen. Gemäß Art. 26 Abs. 1 der Richtlinie, ist für bestimmte Übermittlungszwecke der Datenverkehr mit dem Ausland ohne Beschränkungen zulässig. Für alle anderen Kategorien des Datentransfers ist jeweils die Angemessenheit des Datenschutzniveaus im Empfängerstaat (beim Empfänger) zu prüfen; ist Angemessenheit des Schutzniveaus nicht gegeben, bedarf es besonderer Schutzgarantien im einzelnen Genehmigungsfall. Um eine einheitliche Beurteilung des Vorliegens von angemessenem Datenschutzniveau zu gewährleisten, ist ein intensiver Austausch von Informationen zwischen den Mitgliedsstaaten untereinander und mit der EU-Kommission vorgesehen.

Für Österreich hätten alle Erleichterungen im Datenverkehr mit dem Ausland, die in der Richtlinie enthalten sind, jedoch insofern nur beschränkte Bedeutung, als Datenschutz in Österreich auch für juristische Personen besteht und daher in den wenigsten Staaten ein angemessenes Datenschutzniveau in vollem Umfang, dh. für natürliche **und** juristische Personen, besteht. Um dennoch eine ins Gewicht fallende Vereinfachung zu erzielen, wurden die in Art. 26 Abs. 1 der Richtlinie enthaltenen Ausnahmen von der Genehmigungspflicht auch auf den Export von Daten juristischer Personen erstreckt. Die Rechtfertigung hiefür liegt darin, daß in jenen Fällen, in welchen nicht einmal die schutzwürdigen Geheimhaltungsinteressen natürlicher Personen dadurch gefährdet erscheinen, daß ihre Daten in ein Land ohne angemessenes Schutzniveau exportiert werden, davon auszugehen sein wird, daß auch die schutzwürdigen Geheimhaltungsinteressen juristischer Personen nicht ernstlich gefährdet sind. Darüber hinaus wurde der Datenverkehr in die anderen EU-Mitgliedstaaten auch hinsichtlich juristischer Personen genehmigungsfrei gestellt, da deren Geheimhaltungsinteressen im Rahmen ähnlicher Rechtskulturen hinlänglich geschützt sind.

8. Die **rechtliche Situation des Betroffenen** wird im vorliegenden Entwurf durch folgende Maßnahmen wesentlich gestärkt:

– Die neue Informationspflicht des Auftraggebers macht dem Betroffenen noch stärker als bisher bewußt, wann seine Geheimhaltungsinteressen berührt sind;

– das Auskunftsrecht, das als Angelpunkt für die Verwirklichung von Betroffeneninteressen anzusehen ist, ist in Hinkunft leichter durchsetzbar, da hiefür in Zukunft in jedem Fall die Datenschutzkommission zuständig ist;

– die unabhängige Kontrollstelle (in Österreich: die Datenschutzkommission) kann alle Datenanwendungen überprüfen und ist insofern nicht mehr auf den öffentlichen Bereich beschränkt;

– wenn der Verdacht einer schwerwiegenden Datenschutzverletzung durch einen Auftraggeber des privaten Bereichs vorliegt, kann die Datenschutzkommission anstelle des Betroffenen Feststellungsklage bei dem zuständigen Gericht erheben und dem Betroffenen dadurch eine sichere rechtliche Basis für die Verfolgung seiner Unterlassungs- und Schadenersatzansprüche verschaffen.

9. Was die **Organisation der Vollziehung des Datenschutzes** betrifft, sieht der Entwurf die grundsätzliche Beibehaltung der bisherigen Vollziehungsstruktur in Österreich vor.

Die Trennung des Rechtsweges für die rechtsförmliche Durchsetzung der Rechte der Betroffenen wurde daher beibehalten: Für die Entscheidung über Verletzungen des Datenschutzes durch einen Auftraggeber des öffentlichen Bereichs ist nach wie vor die Datenschutzkommission zuständig, zur Entscheidung über Verletzungen des Datenschutzes im privaten Bereich sind die ordentlichen Gerichte berufen.

Als **unabhängige Kontrollstelle im Sinne des Art. 28** der Richtlinie 95/46/EG wird die Datenschutzkommission eingesetzt, der die Kontrolle über sämtliche Auftraggeber von Datenanwendungen – soweit sie nicht der Gerichtsbarkeit oder der Gesetzgebung zuzurechnen sind – als zusätzliche, neue Kompetenz übertragen wird. (Bisher bestand ein gewisses Kontrollrecht gegenüber den Auftraggebern des öffentlichen Bereichs im Rahmen des § 41 DSG.) Dieser Zuwachs an Zuständigkeiten wird eine gewisse Umstrukturierung des Geschäftsapparates der Datenschutzkommission zur Folge haben müssen. Die Zurverfügungstellung der notwendigen Ressourcen ist gemäß § 38 Abs. 2 Aufgabe des Bundeskanzlers.

10. Wesentliche Neuerungen bringt der Entwurf schließlich im Bereich der **Strafbestimmungen.** Dieser Bereich ist derzeit nicht zufriedenstellend geregelt. Die Struktur der elektronischen Datenverarbeitung hat sich seit dem Inkrafttreten des DSG vollkommen verändert: An die Stelle einiger besonderer Verarbeitungsstätten mit Groß-EDV ist die EDV-Verarbeitung an (nahezu) jeden Arbeitsplatz getreten.

Vor diesem geänderten Hintergrund ist die "berufsmäßige Beschäftigung mit Aufgaben der (Daten)Verarbeitung" nicht mehr einigen wenigen Berufsbildern vorbehalten, sondern eine allgemein verbreitete Begleiterscheinung der modernen Arbeitswelt. Die Aufrechterhaltung einer **gerichtlichen** Strafbestimmung für Geheimnisbruch im Sinne des § 48 war daher nicht mehr sachlich gerechtfertigt, da sie für ein Tatbild mit relativ unspezifischem Unrechtsgehalt die Gefahr einer Kriminalisierung weiter Bevölkerungsteile mit sich brächte. Ein solches Kriminalisierungspotential war nie beabsichtigt. Der derzeit geltende § 49 wiederum enthält einen Tatbestand, dessen Verwirklichung sich als praktisch unmöglich erwiesen hat, sodaß er schon aus diesem Grunde zu beseitigen ist. Gerichtlich strafbar soll in Hinkunft daher nur mehr die absichtliche Schadenszufügung durch bestimmte Verwendungsformen von Daten und die rechtswidrige Übermittlung von Daten in Gewinnerzielungsabsicht sein (§ 51).

Im Gegenzug zur Modernisierung der gerichtlich strafbaren Tatbestände wurden die Verwaltungsstrafbestimmungen ausgedehnt auf jene Fälle, in welchen gravierende Verletzungen der Rechte der Betroffenen vorliegen oder in welchen eine Durchsetzung der Interessen der Betroffenen an einem gesetzmäßigen Verhalten nicht im Wege einer Beschwerde oder Klage erfolgen kann, weil kein subjektives Recht des Betroffenen vorliegt: Eine Sanktionierung erscheint in diesen Fällen durch Bestrafung bei Zuwiderhandeln notwendig.

11. Für die **Umstellung bestehender Datenverarbeitungen** auf die neue Rechtslage setzt die Richtlinie eine **Frist von maximal drei Jahren** nach Erlassung der innerstaatlichen Rechtsvorschriften. Der Anpassungsbedarf wird sich im wesentlichen auf die Einholung neuer Registrierungen und neuer Genehmigungen beschränken. Der Aufwand hiefür sollte sich in Grenzen halten angesichts des eng beschränkten Kreises von vorabprüfungspflichtigen manuellen Datenanwendungen und angesichts des Umstandes, daß nur ein geringer Prozentsatz des internationalen Datenverkehrs **nicht** unter Art. 26 Abs. 1 Richtlinie fällt und daher **nicht** genehmigungsfrei ist.

12. Zur **Kompetenzgrundlage** des Entwurfs ist folgendes auszuführen:

Der vorliegende Entwurf wurde auf Grundlage der geltenden Kompetenzverteilung erstellt. Er kann daher die Richtlinie 95/46/EG nur insoweit umsetzen, als hiefür eine Gesetzgebungskompetenz des Bundes besteht.

13. Für die finanziellen Auswirkungen des vorliegenden Gesetzentwurfes sind die folgenden Komponenten maßgebend:

a) Was den Anfall **zusätzlicher Kosten bei den Auftraggebern** betrifft, ist festzuhalten, daß der Umsetzungsbedarf der neuen Regelung nur einige konkrete Punkte betrifft, da die österreichische Datenschutzrechtsordnung im wesentlichen voll aufrechterhalten wird.

Eine wesentliche zusätzliche Pflicht der Auftraggeber wird die **Informationspflicht** gegenüber den Betroffenen einer Datenanwendung sein. Aus folgenden Gründen ist anzunehmen, daß die für die einzelnen Auftraggeber anfallenden Kosten voraussichtlich nicht bedeutend sein werden:

– Die Informationspflicht betrifft nicht einzelne unvorhersehbare Übermittlungen, die etwa infolge eines einmaligen Begehrens, gestützt auf ein überwiegendes berechtigtes Informationsinteresse des Übermittlungswerbers, notwendig sind; der Informationspflicht unterliegen vielmehr nur die zum Zweck der Datenermittlung für eine bestimmte Datenanwendung geplanten, regelmäßig stattfindenden Datenströme.

– Wenn die Daten beim Betroffenen erhoben werden, kann er unmittelbar bei der Datenerhebung informiert werden, was regelmäßig ohne bedeutende Zusatzkosten (– zu jenen der Datenerhebung –) möglich ist. Nur wenn die gesamten Daten für eine Datenanwendung ohne Befassung der Betroffenen erhoben werden, ist eine Information der Betroffenen ein merkbarer Kostenfaktor. Dieser Fall wird aber deshalb selten eintreten, weil diese Form der Datenbeschaffung meist entweder die Zustimmung des Betroffenen braucht oder, mangels einer solchen, einer besonderen gesetzlichen Grundlage bedarf. In beiden Fällen entfällt aber die Notwendigkeit einer Information des Betroffenen, sodaß voraussichtlich nur in einer geringen Anzahl von Fällen die Kontaktaufnahme mit dem Betroffenen **ausschließlich zum Zweck seiner Information** erforderlich sein wird; in aller Regel wird es möglich sein, die Betroffenen über die beabsichtigte Übermittlung ihrer Daten für weitere Datenanwendungen bereits anläßlich der Datenermittlung für die erste Datenanwendung zu informieren.

Was den zusätzlichen **Registrierungsbedarf bei manuellen Datenanwendungen** betrifft, kann er nur dort überhaupt ins Gewicht fallen, wo traditionellerweise umfangreiche personenbezogene Dateien mit sensiblen Daten gehalten werden: Dies wäre etwa bei Ärzten und ähnlichen Berufszweigen der Fall. Da jedoch auch in diesen Bereichen die Patientenverwaltung zunehmend mit Hilfe der EDV vorgenommen wird, werden in naher Zukunft immer weniger Fälle von dieser besonderen neuen Registrierungspflicht betroffen sein. Daß diese Registrierungspflicht sachlich sinnvoll ist, ergibt sich daraus, daß dadurch verhindert werden kann, daß besonders sensible Informationen zur Umgehung der Transparenzpflichten des Datenschutzes in Form von manuellen Karteien oder Listen gespeichert werden.

Im übrigen sollte dieser zusätzliche Aufwand bei weitem durch den künftigen Entfall der Registrierungspflicht für Standardverarbeitungen wettgemacht werden.

Zur Ausdehnung der **Auskunfts-, Richtigstellungs- und Löschungspflicht auf manuelle Dateien** ist anzumerken, daß sich daraus wahrscheinlich deshalb keine hohen Mehrkosten ergeben werden, weil die Anzahl der dem Datenschutzgesetz unterliegenden manuellen Dateien nicht besonders groß sein wird
(– Dateien für den privaten Gebrauch unterliegen der Pflicht zur Auskunftserteilung, Richtigstellung und Löschung nicht –), und weil die Ausübung dieser Rechte des Betroffenen auch bei den automationsunterstützt geführten Dateien in den letzten zwanzig Jahren seit Inkrafttreten des DSG keine bedeutenden Kosten verursacht hat.

b) Ins Gewicht fallende **Folgekosten** werden sich aus den **zusätzlichen Kompetenzen der Datenschutzkommission** ergeben:

Die Kontrolle des privaten Bereichs wird die Einrichtung einer eigenen Prüfstelle im Geschäftsapparat der Datenschutzkommission notwendig machen, für die zumindest ein zusätzlicher Informatiker (A/a) und zwei Juristen gebraucht werden, wenn kein allzu krasses Vollzugsdefizit entstehen soll; die Ausdehnung der Zuständigkeit für Auskunftsbeschwerden auch im privaten Bereich sowie die Bearbeitung der zu erwartenden Amtshilfeersuchen der Kontrollstellen der anderen EU-Mitgliedstaaten wird darüber hinaus die Planstelle eines weiteren Juristen (mit entsprechenden Sprachkenntnissen) erfordern. Die ebenfalls notwendige Vermehrung des Sekretariats- und Hilfspersonals wird voraussichtlich durch die – in der Richtlinie vorgegebene – Eingliederung des Datenverarbeitungsregisters in den Geschäftsapparat der Datenschutzkommission abgedeckt werden können. Insgesamt wird daher mit Mehrkosten von etwa 4 Millionen Schilling pro Jahr zu rechnen sein, die sich wie folgt zusammensetzen:

Jährliche Durchschnittskosten für eine Planstelle A, A1, a laut Amtsblatt der österreichischen Finanzverwaltung, Nr. 48/1998, gerechnet als Mittelwert zwischen den Kosten für Beamte und für

Vertragsbedienstete: 700 000 S × 4 = 2 800 000 S

hinzu kommen 40% der Personalkosten für

Sachkosten, Raumkosten und Verwaltungsgemeinkosten, das sind 1 120 000 S

insgesamt 3 920 000 S

Was den zu erwartenden **Mehranfall von Verwaltungsstrafverfahren** betrifft, ist zunächst festzuhalten, daß erste Instanz in Zukunft die Bezirksverwaltungsbehörden sein werden, wie dies von den Vertretern der Länder gewünscht wurde. Derzeit werden der Datenschutzkommission insgesamt höchstens 30 Strafverfahren pro Jahr von den zuständigen Landeshauptleuten zur Kenntnis gebracht. Wenn angenommen wird, daß die zusätzlichen Straftatbestände diese Zahl verzehnfacht, was sehr hochgegriffen scheint, dann ergibt dies

eine statistische Zahl von etwa drei Fällen pro Jahr pro Bezirkshauptmannschaft, was vernachlässigbar wäre. Diese Zahl wird freilich dahingehend zu korrigieren sein, daß in Ballungszentren relativ mehr Fälle anfallen werden. Aber auch dies wird angesichts der zu erwartenden Gesamtzahl von Fällen voraussichtlich nicht zu einem zusätzlichen Personalbedarf in den Bezirkshauptmannschaften führen.

Dasselbe gilt angesichts der zu erwartenden zusätzlichen Belastung der UVS als Rechtsmittelbehörde: Wenn davon ausgegangen wird, daß bei zirka 300 Verfahren pro Jahr etwa in der Hälfte der Fälle Beschwerde erhoben wird, also in 150 Fällen, entfallen auf den UVS eines Landes zehn bis 20 Fälle pro Jahr, oder – unter Berücksichtigung der Ballungsräume – fünf bis 25 Fälle.

Festzuhalten ist, daß die Ausdehnung der Verwaltungsstraftatbestände in Umsetzung des Art. 24 der Richtlinie 95/46/EG vorgenommen wurde und daß die dadurch entstehenden Mehrkosten daher nicht vermeidbar waren.

Das Projekt einer **elektronischen Registrierung** wird als weiterer Vollzugskostenfaktor berücksichtigt werden müssen, dem aber ein wesentliches Einsparungspotential auf Seiten der Vollziehung wie vor allem auch auf Seiten der Registrierungspflichtigen gegenübersteht.

Die voraussichtlichen Kosten errechnen sich wie folgt:

1. Entwicklung:

Leistung:	Einmalkosten:
Vorstudie	800 000
Einrichtung der Entwicklungs- und Produktionsumgebung Beschaffung, Installation und Customizing der beiden Produktionsserver, Implementierung der erforderlichen Serversoftware. Der Produktionsserver (samt der darauf installierten Serversoftware) wird dem Auftraggeber zur alleinigen Disposition zur Verfügung gestellt.	800 000
Design und Layout der Benutzeroberfläche	200 000
Anwendungsentwicklung Projektleitung, Analyse, Design, Datenbankerstellung, Programmierung/Softwareentwicklung, Test, Datenübernahme	5 700 000
Dokumentation und Schulung Anwendungsdokumentation/technische Dokumentation, Schulung (eintägig, drei Termine)	200 000
Unterstützung bei der Inbetriebnahme	900 000
Insgesamt S	8 600 000

2. Betrieb

Leistung:	Kosten pro Jahr:
Wartung und Betrieb der beiden Produktionsserver Hardware und Software, Lizenzkosten, Personal	1 700 000
Betrieb einer Hotline Telefonanschluß, Personal (zwei Personen halbtags, an Werktagen)	3 000 000
Insgesamt S	4 700 000

Als elektronische Infrastruktur für die on-line Registrierung könnte die bereits bestehende "Help"-Plattform der Bundesverwaltung dienen, die Zugang zur öffentlichen Verwaltung über elektronische Netze, insbesondere das Internet, verschafft.

Besonderer Teil:

Zu § 1 des Entwurfs (Grundrecht auf Datenschutz):

Das Grundrecht auf Datenschutz bewirkt einen Anspruch auf Geheimhaltung personenbezogener Daten. Darunter ist der Schutz des Betroffenen vor Ermittlung seiner Daten und der Schutz vor der Weitergabe der über ihn ermittelten Daten zu verstehen.

Freilich kann ein solcher Anspruch angesichts der Vielfältigkeit der denkbaren Konstellationen, in welchen Daten verwendet werden, nicht ohne Einschränkungen anerkannt werden:

Nach **Abs. 1** gibt es ein Recht auf Datenschutz nur dann, wenn **"ein schutzwürdiges Geheimhaltungsinteresse** (an bestimmten personenbezogenen Daten) **besteht**".

Dies setzt voraus, daß es überhaupt **personenbezogene Daten** gibt, die auf eine in ihrer Identität bestimmte (oder zumindest bestimmbare) Person zurückgeführt werden können, und daß diese Daten weiters **geheim gehalten werden können,** was dann grundsätzlich unmöglich sein wird, wenn sie allgemein zugänglich sind. Freilich bedarf dies der genauen Prüfung im Einzelfall, wobei vor allem auch zu beachten sein wird, ob die allgemeine Zugänglichkeit im Zeitpunkt der beabsichtigten Verwendung tatsächlich noch besteht.

An anderen Daten besteht ein schutzwürdiges Geheimhaltungsinteresse, das jedoch – wie jedes Grundrecht – nicht absolut gilt, sondern durch bestimmte, zulässige Eingriffe beschränkt werden darf:

Als wichtigen Grund für eine zulässige Ausnahme vom Geheimhaltungsschutz führt **Abs. 2** zunächst die **Zustimmung** des Betroffenen zur Verwendung seiner Daten an, in Anerkennung der Tatsache, daß in erster Linie der Betroffene selbst über das Schicksal der ihn betreffenden Daten zu entscheiden hat. Weitere Gründe für zulässige Eingriffe können sich aus den besonderen **Interessen entweder des Betroffenen selbst oder aus den Interessen anderer Rechtsunterworfener** ergeben, wenn die überwiegende Berechtigung dieser Interessen gegenüber den schutzwürdigen Geheimhaltungsinteressen des Betroffenen anzuerkennen ist. Zu den "Interessen anderer" ist zu sagen, daß als "andere" alle vom Betroffenen verschiedenen (natürlichen und juristischen) Personen zu gelten haben; die Kategorie der "anderen" umfaßt daher Private ebenso wie juristische Personen des öffentlichen Rechts, also auch Selbstverwaltungskörper oder Gebietskörperschaften. Wird ein Eingriff zugunsten der "Interessen anderer" durch eine staatliche **Behörde,** dh. durch ein hoheitlich handelndes staatliches Organ, vorgenommen, dann bedarf es hiezu einer besonderen gesetzlichen Grundlage (vgl. auch Art. 8 Abs. 2 MRK), und zwar auch dann, wenn Eingriffe staatlicher Behörden den "Schutz der Rechte und Freiheiten" privater Rechtssubjekte zum Ziel haben (wozu auch in Privatwirtschaftsverwaltung tätige Gebietskörperschaften zu zählen wären) und nicht – wie im Regelfall – der Wahrung öffentlicher Interessen dienen.

Für die Abwägung, ob in einem konkreten Fall die Geheimhaltungsinteressen des Betroffenen oder die berechtigten Interessen der anderen überwiegen, bietet Abs. 2 teilweise Hilfestellung, indem ausdrücklich festgelegt wird, daß

> – hinsichtlich der Interessen des Betroffenen – neben dem Fall seiner Zustimmung – nur seine lebenswichtigen Interessen einen Eingriff in das Grundrecht gestatten;
>
> – bei den Eingriffen, die von staatlichen Behörden vorgenommen werden, ein "Überwiegen" der Eingriffsinteressen und damit die Zulässigkeit des Eingriffs nur dann gegeben ist, wenn der Eingriff aus einem der in Art. 8 Abs. 2 MRK genannten Gründe notwendig und verhältnismäßig ist.

Nur bei jenen **Eingriffen** in das – mit Drittwirkung ausgestattete – Grundrecht, die nicht durch "den Staat" (in seiner Hoheitsfunktion) erfolgen, enthält Abs. 2 keine näheren Parameter dafür, wann ein berechtigtes Informationsinteresse anderer vorliegt, das die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegt. Diesbezüglich sind die einfachgesetzlichen Ausführungsbestimmungen zum Grundrecht, und zwar die §§ 7 und 9, heranzuziehen.

Die ausdrückliche Berücksichtigung der Interessenslage des Betroffenen in Abs. 2 ist eine Neuerung gegenüber der bisherigen Formulierung dieser Bestimmung, die, wie die Anwendungserfahrung gezeigt hat, im Interesse der Ausgewogenheit und Vollständigkeit notwendig ist.

Eine weitere Ergänzung des Abs. 2 gegenüber dem bisher geltenden Text betrifft die sogenannten **"sensiblen Daten"** (vgl. hiezu die Definition in § 4 Z 2). Die Richtlinie 95/46/EG enthält ein grundsätzliches Verarbeitungsverbot für sensible Daten (Art. 8 Abs. 1 Richtlinie), das mit einem taxativen Katalog zulässiger Ausnahmen verknüpft ist. Dieser Katalog enthält neben einzelnen speziellen Ausnahmetatbeständen – die im § 9 des Entwurfs nachgebildet sind – auch eine generelle Ausnahme dahingehend, daß Gesetze die Verwendung sensibler Daten vorsehen dürfen. Da dies allerdings nur aus wichtigen öffentlichen Interessen geschehen darf (Art. 8 Abs. 4 Richtlinie) und da solche Gesetze entsprechende Garantien für den Schutz der Betroffenenrechte enthalten müssen, ist im Grundrecht ein entsprechender Auftrag an den einfachen Gesetzgeber zu statuieren, um für die Einhaltung der aus der Richtlinie resultierenden Verpflichtungen durch die Gesetzgebung zu sorgen.

Die Änderung des letzten Satzes im Abs. 2 entspricht der in der Praxis deutlich gewordenen Notwendigkeit, das Verhältnismäßigkeitsprinzip stärker zu betonen, da sich daraus oft wichtige Konsequenzen für die Zulässigkeit der Ausgestaltung von legistischen Vorhaben

ergeben. Der bisherige Text des letzten Satzes des Abs. 2 wurde hingegen gestrichen, da er insofern problematisch ist, als er einen Vorrang des Grundrechts auf Datenschutz vor anderen Grundrechten zu implizieren scheint, was nicht zu rechtfertigen wäre.

Abs. 3 enthält die richtliniengemäße Ausdehnung des Rechtes auf Auskunft und Richtigstellung bzw. Löschung auf manuelle Dateien, das sind strukturierte Datensammlungen, die ohne Automationsunterstützung hergestellt und benützt werden.

Im **Absatz 5** wird die für das österreichische Datenschutzrecht traditionelle Teilung des Rechtsschutzinstrumentariums zwischen ordentlichen Gerichten und Datenschutzkommission in einer Weise neu festgelegt, die gegenüber den bisher geltenden Bestimmungen einfacher nachzuvollziehen ist, weil sie – grundsätzlich – nicht auf den Inhalt der Tätigkeit abstellt, sondern auf die rechtliche Organisationsform des Auftraggebers.

Um auch bei Aufrechterhaltung des geteilten Rechtsschutzsystems eine Vereinfachung des Zugangs zum Rechtsschutz für die Betroffenen zu bewirken, soll jedoch das Recht auf Auskunft – unabhängig davon, ob der belangte Auftraggeber dem öffentlichen oder dem privaten Bereich zuzurechnen ist – in Hinkunft vor der Datenschutzkommission durchsetzbar sein. Dies scheint deshalb so wichtig, weil der Inhalt der Auskunft in den meisten Fällen entscheidend ist für die Frage, ob der Betroffene sinnvollerweise ein Verfahren wegen Löschung, Berichtigung oder Unterlassung der Verwendung anstrengen soll.

Zu § 2 (Zuständigkeit):

Nach der geltenden Rechtslage (§ 2 DSG) besteht eine Gesetzgebungskompetenz des Bundes nur hinsichtlich des Datenschutzes **bei automationsunterstützter Datenverarbeitung.** Es ist daher für den einfachen Bundesgesetzgeber nicht möglich, die Richtlinie 95/46/EG in ihrem gesamten Anwendungsbereich umzusetzen: Soweit manuelle Dateien für Zwecke angelegt und benützt werden, die einer Angelegenheit der Landesgesetzgebungskompetenz zuzuordnen ist, ist es Aufgabe der Länder, Datenschutzbestimmungen für diese Dateien vorzusehen, die dem Inhalt der Richtlinie entsprechen. Was manuelle Dateien betrifft, die in Angelegenheiten geführt werden, für die Bundesgesetzgebungskompetenz besteht, enthält § 58 des vorliegenden Entwurfs eine Regelung, durch die diese Dateien den einfachgesetzlichen Bestimmungen des Datenschutzgesetzes unterworfen werden.

Zu § 3 des Entwurfs (Räumlicher Anwendungsbereich):

In Umsetzung der Richtlinie 95/46/EG (Art. 4) wird der Anwendungsbereich des österreichischen Datenschutzrechtes so definiert, daß grundsätzlich auf jede Datenverwendung in Österreich ("im Inland") österreichisches Recht anzuwenden ist.

Ausnahmen bestehen zugunsten des **Sitzstaatsprinzips,** das im Gemeinschaftsrecht angesichts der Dienstleistungsfreiheit eine gerne verwendete Kollisionsregel darstellt. Und zwar gilt diese Ausnahme zugunsten des Sitzstaatsprinzips dann, wenn Daten in Österreich für einen Auftraggeber aus einem anderen EU-Staat verarbeitet werden, **ohne** daß der Auftraggeber (der seinen Sitz in einem anderen EU-Staat hat) eine **feste Betriebsstätte** ("Niederlassung" im Sinne des § 4 Z 15) **in Österreich** hätte. Umgekehrt gilt österreichisches Datenschutzrecht in einem anderen EU-Staat dann, wenn ein österreichischer Rechtsträger Datenverarbeitung im EU-Ausland betreibt, ohne daß er für die Verfolgung seiner Interessen dort eine "Niederlassung" (im Sinne des § 4 Z 15) besitzt. Wichtig ist es jedoch festzuhalten, daß die Zurechnung einer datenverwendenden Tätigkeit "materiell" vorzunehmen ist, das heißt: nicht nach ausschließlich juristischen Kriterien. Die Tätigkeiten einer (unselbständigen) Niederlassung im Ausland gelten im vorliegenden Zusammenhang nicht als solche, die "für Zwecke des in Österreich befindlichen Rechtsträgers" entfaltet werden, sondern als "eigene Zwecke" der (unselbständigen) Niederlassung, die der EU-ausländischen Rechtsordnung unterliegen. Daher würde zB die Niederlassung einer österreichischen Bank in Frankreich hinsichtlich der von ihr getätigten Bankgeschäfte französischem Recht unterliegen, auch wenn es sich um eine unselbständige Niederlassung handeln sollte.

Während der **Ort der Niederlassung des Auftraggebers** der maßgebliche Anknüpfungspunkt für die Frage des anwendbaren Rechts ist, soweit es sich um Datenanwendungen für einen **Rechtsträger mit Sitz in einem EU-Mitgliedstaat** handelt, gilt bei Datenanwendungen für Zwecke eines Rechtsträgers, der keinen Sitz in einem EU-Mitgliedsstaat hat, immer der **Ort der Datenverwendung** als Anknüpfungspunkt für die Anwendbarkeit einer nationalen Rechtsordnung (Art. 4 Abs. 1 lit. c Richtlinie).

Zu § 4 des Entwurfs (Definitionen):

Die bisherigen Definitionen des DSG wurden geändert, soweit dies zur Umsetzung der Richtlinie 95/46/EG oder zur Verwertung der Erfahrungen aus der Anwendung des geltenden DSG notwendig war.

Zu Z 1:

Angesichts der Definition des Begriffs "Daten" in der Richtlinie mußte im vorliegenden Entwurf **(Z 1)** die bisher in der Definition enthaltene Einschränkung "auf einem Datenträger festgehalten" unterlassen werden.

Die Richtlinie geht davon aus, daß Daten nicht nur dann "personenbezogen" sind, wenn die Identität des Betroffenen **für den** jeweiligen **Verwender** bestimmbar ist, sondern auch dann, wenn sie nur für einen Dritten (zB den Inhaber des Entschlüsselungscodes bei codierten

Identitätsdaten) bestimmbar sind. Um hier im Hinblick auf das Schutzinteresse eine sinnvolle Abstufung vornehmen zu können, wurde die in der Richtlinie enthaltene Unterscheidung zwischen direkter und (nur) indirekter Identifizierbarkeit nutzbar gemacht; wenn es für den konkreten Verwender der Daten nicht möglich ist, den – zB in Form einer laufenden oder sprechenden Nummer – vorhandenen Personenbezug auf eine in ihrer Identität bestimmte Person zurückzuführen, dann ist der Gebrauch solcher "nur indirekt personenbezogener" Daten durch **diesen** Verwender unter erleichterten datenschutzrechtlichen Bedingungen erlaubt. Einer Erläuterung bedarf allerdings noch die Aussage, daß es darauf ankommt, ob der Verwender die Identität des Betroffenen bestimmten **"kann".** Z 1 grenzt dies ausdrücklich auf die Anwendung legaler Mittel ein; darüber hinaus wird jedoch auch noch die in Erwägungsgrund 26 der Richtlinie ausdrücklich erwähnte weitere Eingrenzung dessen, was als möglich anzusehen ist, zu berücksichtigen sein: Als mögliches Mittel der Identifikation ist nämlich nur ein solches anzusehen, das "vernünftigerweise" angewendet wird, dh. das also weder seiner Art nach, noch seinem Aufwand nach vollkommen ungewöhnlich ist.

Von den "nur indirekt personenbezogenen" Daten zu unterscheiden sind die üblicherweise als "anonymisiert" bezeichneten Daten. Bei anonymisierten Daten gibt es keinen Personenbezug; hiebei handelt es sich um Daten, die **niemand** auf eine in ihrer Identität bestimmte Person zurückführen kann. Derartige Daten sind daher auch nicht datenschutzrelevant.

Die in der bisherigen Definition der personenbezogenen Daten enthaltene Bestimmbarkeit "mit hoher Wahrscheinlichkeit" hat sich in der Praxis als wenig bedeutsam erwiesen, weshalb diese Spezifikation in die Definition nicht mehr aufgenommen wurde.

Zu Z 2:

Neu ist die Aufzählung der "sensiblen Daten" in **Z 2,** die in Umsetzung des Art. 8 Abs. 1 Richtlinie erfolgt. Diese Aufzählung darf angesichts des taxativen Charakters des Art. 8 Abs. 1 Richtlinie weder erweitert noch verkürzt werden.

Zu Z 3:

Die bisher in § 3 Z 2 enthaltene Einschränkung des Betroffenenbegriffs kann angesichts der Richtlinie in dieser Form nicht mehr aufrechterhalten werden. Eine (teilweise) Ersatzbestimmung findet sich nunmehr in § 8 Abs. 3 Z 6 und in § 9 Z 5 (vgl. die Erläuterungen zu diesen Gesetzesstellen).

Zu Z 4 und 5:

Die Ausdehnung der Definitionen von "Auftraggeber" und "Dienstleister" **(Z 4 und 5)** auch auf Personengemeinschaften und auch auf Geschäftsapparate von Organen von Gebietskörperschaften (zB Bundesministerien, Ämter der Landesregierungen, usw.) entspricht einem Wunsch der Praxis.

Ein seit langem diskutiertes Problem ist jenes der Abgrenzung von "Auftraggeber" und "Dienstleister" im Hinblick darauf, wer die Entscheidung über den Einsatz von EDV treffen muß, um als "Auftraggeber" im Sinne des DSG zu gelten. Der vorliegende Entwurf löst diese Frage nunmehr dahingehend, daß der Einsatz von EDV durch einen mit einem Werk Beauftragten grundsätzlich dem Werk-Auftragserteiler datenschutzrechtlich zugerechnet wird, da der Einsatz von EDV heute grundsätzlich zu vermuten ist, wenn ein Werk unter Benützung von Daten zu erbringen ist. Es bedarf also für diese Zurechnung keiner ausdrücklichen Vereinbarung zwischen Werk-Auftragserteiler und dem mit dem Werk Beauftragten.

Wenn hingegen der Auftragserteiler dem Auftragnehmer den Einsatz von EDV ausdrücklich verboten haben sollte – was freilich keine sehr häufige Situation darstellen wird – , dann ist der Auftragnehmer datenschutzrechtlicher Auftraggeber, wenn er **dennoch** EDV einsetzt. Da es ihm für die Auftraggebereigenschaft allerdings an einer entsprechenden Rechtsgrundlage mangeln wird, wird eine automationsunterstützte Verarbeitung auf Grund seiner autonomen Entscheidung unzulässig sein – eine Registrierung käme etwa nicht in Frage.

Der Vorteil dieser Lösung liegt vor allem auch darin, daß die Betroffenenrechte gegenüber jenen Personen zum Tragen kommen, die dieser Rolle auch wirklich gerecht werden können; dies wird besonders deutlich, wenn es etwa um die Frage geht, an wen ein Auskunftsbegehren zu stellen ist: An den Auftragnehmer kann der Betroffene sich deshalb nicht wenden, weil ihm seine Identität in aller Regel unbekannt sein wird. Ähnliches gilt für Löschungs- und Richtigstellungsansprüche: Die Erledigung eines solchen Anspruchs setzt die Verfügungsgewalt über die davon betroffenen Daten voraus, also eine Befugnis, die einem Auftragnehmer aus eigenem nicht zusteht. Auch im Interesse der Ausübbarkeit der Betroffenenrechte muß daher der vorgeschlagene Lösungsansatz als zweckmäßig erscheinen.

Nun gibt es jedoch einzelne Fälle von Beauftragungsverhältnissen, in welchen traditionellerweise der Beauftragte selbständig ("eigenverantwortlich") über die Verwendung der ihm übergebenen Informationen entscheidet und hiezu auch nach den für ihn geltenden Standesregeln verpflichtet und hiefür verantwortlich ist – dies gilt etwa für bestimmte freie Berufe, wie Rechtsanwälte, Wirtschaftstreuhänder, Ziviltechniker usw. Die Zuordnung der datenschutzrechtlichen Verantwortlichkeit eines Auftraggebers muß auf diese Besonderheiten Rücksicht nehmen. Um diesbezüglich die notwendige Rechtssicherheit herzustellen, wird es sich empfehlen, in Verhaltensregeln gemäß § 6 Abs. 4 klarzustellen, wem in gewissen Konstellationen die Auftraggebereigenschaft zukommt. Um für einen entsprechenden Schutz der Betroffenenrechte auch in diesen Fällen vorzusorgen, wurde die

besondere Auskunftsverpflichtung nach § 26 Abs. 9 geschaffen.

Zu Z 6:

In der bei der Erarbeitung der Richtlinie stattgefundenen Diskussion wurde immer wieder betont, daß unter "Datei" bei der manuellen Verwendung von Daten keinesfalls ein Aktenkonvolut zu verstehen sei, sondern vielmehr Karteien, Listen u. dgl. Dieses gemeinsame Begriffsverständnis findet bedauerlicherweise im Definitionswortlaut nur ungenügenden Ausdruck: Um der kollektiven Absicht zu entsprechen, hätte es wohl eher heißen müssen, daß eine "Datei" eine **Sammlung strukturierter Datensätze** sei, die – nämlich die Sammlung – nach mindestens einem Suchkriterium geordnet ist. Eine historisch-teleologisch berichtigende Interpretation des tatsächlichen Textes scheint vor diesem Hintergrund nicht ausgeschlossen.

Zu Z 7:

Der Begriff der "Datenanwendung" in der **Z 7** entspricht im Prinzip dem bisherigen Begriff der "Datenverarbeitung" gemäß § 3 Z 5 des geltenden DSG. Der neue Begriff "Datenanwendung" wurde nur gewählt, um eine bessere Unterscheidbarkeit zum Begriff des "Verarbeitens" von Daten (Z 9) zu bewirken. Im Hinblick auf die Definition der (automatisierten) "Verarbeitung" in Art. 2 lit. b der Richtlinie mußte allerdings die definitorische Bezugnahme auf die Strukturiertheit der Datenaufbereitung fallengelassen werden. Daß dies gewisse Probleme hinsichtlich der datenschutzrechtlichen Behandlung etwa von Textverarbeitung mit sich bringt, sei an dieser Stelle angemerkt.

Wesentlich für das Begriffsinstrumentarium des Entwurfes ist jedenfalls, daß die "Datenanwendung" – so wie bisher die "Datenverarbeitung" – eine **logische** Einheit ist, die unterschiedlichste Handlungen umfaßt, wie etwa das Verarbeiten **(Z 9),** Übermitteln **(Z 12),** usw. Das verbindende Element ist der Gesamtzweck der Datenanwendung, zu dessen Erreichung die einzelnen Schritte gesetzt werden.

Zu Z 8:

Der umfassendste Begriff für die Handhabung von Daten ist der Begriff "Verwenden", der in **Z 8** definiert wird. Der Begriff des "Verwendens" von Daten entspricht dem Begriff "Verarbeiten" in der Richtlinie, in der definitorisch zwischen "Verarbeiten" (im österreichischen Sinn) und "Übermitteln" nicht unterschieden wird. Eine solche Begriffsbildung scheint – schon weil sie im Widerspruch zum Sprachgebrauch steht – nicht optimal, weshalb der österreichischen Tradition folgend weiter die Begriffe "verarbeiten" und "übermitteln" unterschieden werden und dem Überbegriff "verwenden" untergeordnet werden (vgl. auch die Ausführungen zu Z 9, 10 und 12).

Zu Z 9, 10 und 12:

Der Begriff des "Verarbeitens" wurde dahingehend modifiziert, daß das "Ermitteln" in den Verarbeitungsbegriff miteinbezogen wurde; Grund hiefür war eine möglichst weitgehende Angleichung an die Terminologie der Richtlinie. Daß das "Übermitteln" jedoch – so wie bisher – im Verarbeitungsbegriff nicht inkludiert ist und daher vom Sprachgebrauch der Richtlinie abweicht, hat seinen Grund in den unterschiedlichen Zulässigkeitvoraussetzungen für diese beiden Tätigkeitsarten, weshalb sie auch als getrennte Begriffe aufrechterhalten werden mußten. Daß die Richtlinie dies nicht tut, hat sich bereits als Mangel erwiesen (vgl. etwa die Unklarheiten in Art. 25 und 26 über den dort – undefiniert – gebrauchten Terminus "übermitteln".)

Als "Übermitteln" wird so wie bisher auch die Verwendung von Daten für ein anderes Aufgabengebiet beim selben Auftraggeber verstanden. Ein "Aufgabengebiet" ist eines von mehreren Tätigkeitsfeldern eines Auftraggebers, das in seinem Umfang nach der Verkehrsauffassung geeignet ist, für sich allein den gesamten Geschäftsbereich eines Auftraggebers zu bilden. Das "Aufgabengebiet" wäre also im privaten Bereich zB in etwa mit dem Umfang einer Gewerbeberechtigung gleichzusetzen, im öffentlichen Bereich mit einem Kompetenztatbestand (im Sinne der Art. 10 bis 15 B-VG).

Zu Z 14:

Die Definition der "Zustimmung" gibt weitestgehend den diesbezüglichen Text der Richtlinie (Art. 2 lit. h) wieder. Es ist darauf hinzuweisen, daß eine datenschutzrechtliche Zustimmung in Hinkunft nicht mehr unbedingt ausdrücklich und schriftlich vorliegen muß: Die Ausdrücklichkeit ist nur bei der Verwendung sensibler Daten notwendig; die Schriftlichkeit wird nur von Fall zu Fall dann notwendig sein, wenn es darum geht nachzuweisen, daß die Zustimmung zweifelsfrei vorliegt.

Zu § 5 des Entwurfs (öffentlicher und privater Bereich):

In Übereinstimmung mit § 1 Abs. 5 stellt die Abgrenzung zwischen Auftraggebern des öffentlichen Bereichs und solchen des privaten Bereichs nunmehr darauf ab, nach welchem Rechtsregime der Auftraggeber **eingerichtet** ist. Eine gewisse **Korrektur** erfährt dieses Abgrenzungskriterium nur dort, wo Rechtsträger des privaten Rechts ausnahmsweise Hoheitsverwaltung betreiben, ein Fall, der angesichts der steigenden Anzahl von **Ausgliederungen** von Verwaltungsbereichen besonders zu berücksichtigen war. Die Wendung "in Vollziehung der Gesetze" ist im Sinne des Art. 23 B-VG so zu verstehen, daß auch die schlichte Hoheitsverwaltung mitumfaßt ist.

Zu § 6 des Entwurfs (Grundsätze):

Wie schon die Datenschutzkonvention des Europarates (ETS 108) enthält auch die Richtlinie 95/46/EG in einem Katalog "Grundsätze für die Datenqualität". Dieser Katalog wurde nunmehr ausdrücklich – in sprachlich gekürzter Form – auch in das Datenschutzgesetz **(§ 6 Abs. 1)** aufgenommen. Für die österreichische Rechtsordnung ist dieser Katalog im Hinblick darauf, daß die Datenschutzkonvention des Europarates Bestandteil der österreichischen Rechtsordnung ist, keine Neuerung.

Zu Abs. 1:

Eine Verwendung von Daten "nach Treu und Glauben" **(Z 1)** liegt nur dann vor, wenn der Betroffene über die Umstände des Datengebrauchs und das Bestehen und die Durchsetzbarkeit seiner Rechte nicht irregeführt oder im Unklaren gelassen wird. Wichtig für die Verwirklichung dieses Gebots sind vor allem die Bestimmungen des 4. Abschnitts des vorliegenden Entwurfs über die Publizität der Datenanwendung.

Aus dem Gebot der Verwendung "in rechtmäßiger Weise" ergibt sich ua. auch, daß der Auftraggeber eine ausreichende rechtliche Befugnis bzw. Zuständigkeit für jene Art der Benützung von Daten, die er mit seiner Datenanwendung bezweckt, besitzen muß.

Das in **Z 2** statuierte Zweckbeschränkungsprinzip findet im vorliegenden Gesetzentwurf in folgenden Bestimmungen seine Umsetzung:

– Wichtig hiefür ist zunächst die Definition des Übermittlungsbegriffs in § 4 Z 12: Jeder Zweckwechsel ist eine "Übermittlung"; diese liegt nicht nur dann vor, wenn Daten an einen Dritten weitergegeben werden, sondern auch dann, wenn derselbe Auftraggeber Daten selbst für ein anderes Aufgabengebiet (vgl. die Ausführungen zu § 4 Z 12) (weiter)verwendet.

– Jede Übermittlung bedarf einer besonderen rechtlichen Grundlage; sind die Voraussetzungen des § 7 Abs. 2 und 3 nicht gegeben, ist eine Übermittlung von Daten unzulässig.

Wenn in Z 2 statuiert wird, daß eine Weiterverwendung von Daten nur zulässig sein soll, wenn dies mit dem ursprünglichen Ermittlungszweck "nicht unvereinbar" ist, so sei dazu angemerkt, daß diejenigen innerbetrieblichen Datenverwendungen, die der Aufrechterhaltung und Optimierung der Organisation (wie zB Rechnungswesen und Controlling) oder der Analyse und Planung dienen, jedenfalls **nicht** als eigener Verwendungszweck zu sehen sind, der mit dem Zweck der ursprünglichen Datenermittlung (zB im Rahmen des Abschlusses eines Handelsgeschäftes) **"unvereinbar"** ist.

Das Gebot der sachlichen Richtigkeit **(Z 4)** ist so zu verstehen, daß Richtigkeit **im Hinblick auf den deklarierten Zweck der Datenanwendung** gefordert ist: Lautet der deklarierte Zweck etwa "Verzeichnis von Straftätern", dann dürfen Personen, die einer Straftat nur verdächtigt sind, in dieses Verzeichnis nicht aufgenommen werden; anders dann, wenn ein "Verzeichnis der Verdachtsfälle" geführt wird. In diesem Zusammenhang muß jedoch ausdrücklich darauf hingewiesen werden, daß bei Datensammlungen klar erkennbar sein sollte, welches Ausmaß an objektiver Richtigkeit die gespeicherten Daten voraussichtlich besitzen; handelt es sich um sogenannte "weiche" Daten, wird eine regelmäßige Überprüfung auf Aktualität besonders wichtig sein, um ungerechtfertigte Nachteile für Betroffene zu vermeiden.

Zu den Abs. 2 und 3:

Die Absätze 2 und 3 schreiben die – schon bisher unbestrittene – Auftraggeberverantwortung für Datenanwendungen ausdrücklich fest. Es ist festzuhalten, daß es sich um die Formulierung eines **Grundsatzes** handelt, der bei konkreten Verwendungssituationen – etwa bei on-line Übermittlungen – hinsichtlich der Abgrenzung zur Verantwortungssphäre Dritter durchaus interpretationsbedürftig sein kann.

Abs. 3 dient der Umsetzung von Art. 4 Abs. 2 der Richtlinie.

Zu Abs. 4:

Die Richtlinie bezieht sich in Art. 27 auf sogenannte "Verhaltensregeln", die nicht-staatliche Institutionen, wie zB Berufsverbände, zur näheren Durchführung von einzelstaatlichem Datenschutzrecht für einzelne Branchen und Berufszweige ausarbeiten können. Aus der Sicht der österreichischen Rechtsordnung scheint ein sinnvoller Anwendungsbereich von derartigem "soft law" vor allem bei der näheren Umschreibung dessen zu bestehen, was in einer bestimmten Branche als Datenverwendung nach "Treu und Glauben" anzusehen wäre; weiters wären solche Verhaltensregeln zB auch geeignet, um die Rollenverteilung von Auftraggeber und Dienstleister bestimmter Konstellationen ausdrücklich festzuschreiben oder um das Ausmaß der Informationsverpflichtung gegenüber dem Betroffenen bei bestimmten Arten von Datenanwendungen näher festzulegen. Solche Regeln haben freilich keinen verbindlichen Charakter, wären aber bei freiwilliger Befolgung durch die Mehrzahl der Beteiligten sicher ein wertvolles Mittel für die effektive Verwirklichung von Datenschutz in wichtigen Bereichen des täglichen Lebens. Um zu vermeiden, daß durch solche Verhaltensregeln rechtswidrige Handlungsanleitungen aufgestellt werden, bedarf es einer Prüfung, die jedoch nicht von der Datenschutzkommission vorgenommen werden soll, um die Unabhängigkeit der Entscheidungsfindung im einzelnen Beschwerdefall nicht zu

präjudizieren. Abs. 4 beruft daher das für Angelegenheiten des Datenschutzes zuständige oberste Organ, den Bundeskanzler, zu einer Begutachtung der Verhaltensregeln.

Zu § 7 des Entwurfs (Zulässigkeit der Verwendung von Daten):

§ 7 enthält die generelle Regel für die Beurteilung der Zulässigkeit einer konkreten Datenverwendung. Die Zulässigkeit einer konkreten Datenanwendung hat zwei Voraussetzungen:

– die Berechtigung des Auftraggebers und

– die Berücksichtigung der schutzwürdigen Interessen der Betroffenen.

Hinzu treten bei Übermittlungen die in Abs. 2 genannten zusätzlichen Erfordernisse.

Der Grundsatz der Verhältnismäßigkeit ist in Abs. 3 im Hinblick auf – zulässige – Eingriffe in das Grundrecht auf Datenschutz ausdrücklich nochmals festgeschrieben.

Zu § 8 des Entwurfs (Schutzwürdige Geheimhaltungsinteressen bei der Verwendung nichtsensibler Daten):

Die Zulässigkeit einer Datenanwendung erfordert gemäß § 7 ua., daß "schutzwürdige Geheimhaltungsinteressen nicht verletzt werden".

Dieses Erfordernis bedarf näherer Festlegungen, um vollziehbar zu sein. Dies geschieht

– für die **nichtsensiblen Daten** in Form einer Generalklausel (§ 8 Abs. 1) mit einzelnen wichtigen Beispielen (§ 8 Abs. 2 bis 4),

– für **sensible Daten** in Form eines taxativen Katalogs der zulässigen Verwendungsfälle (§ 9).

Durch diese Regelungstechnik wird die von der Richtlinie vorgegebene Kasuistik mit der in österreichischen Gesetzen üblichen Präferenz für generelle Regelungen in Einklang gebracht und überdies die von Art. 8 Richtlinie geforderte Verbotswirkung für die im Art. 8 Richtlinie nicht erwähnten Fälle der Verwendung sensibler Daten erreicht.

§ 8 Abs. 2 nennt – in Durchführung des § 1 Abs. 1 letzter Satz – zwei Fälle, in welchen kein Geheimhaltungsanspruch besteht. Zum ersten Fall – der Verwendung zulässigerweise veröffentlichter Daten – ist anzumerken, daß bei allen Datenanwendungen, die solche Daten enthalten, jeweils die Frage zu stellen ist, ob sie **ausschließlich** veröffentlichte Daten enthalten (zB bei einem elektronischen Telefon-Teilnehmerverzeichnis) oder ob nicht auch zusätzliche, durch **Auswertung** der veröffentlichten Daten gewonnene Daten in der Datenanwendung enthalten sind, die ihrerseits nirgends veröffentlicht sind.

Da im übrigen auch eine andere Form der Aufbereitung veröffentlichter Daten neue – nicht veröffentlichte – Informationen liefern kann, kann nicht ausgeschlossen werden, daß in besonderen Konstellationen schutzwürdige Geheimhaltungsinteressen doch berührt werden, weshalb das Widerspruchsrecht nach § 28 ausdrücklich aufrechterhalten wird.

Um die praktische Anwendung des DSG zu erleichtern, werden in § 8 Abs. 3 einige der wichtigsten Fälle angeführt, in welchen durch die Datenverwendung keine schutzwürdigen Geheimhaltungsinteressen der Betroffenen verletzt werden, weil es sich um zulässige Eingriffe im Sinne des § 1 Abs. 2 handelt. Dieser Katalog ist in keiner Weise erschöpfend und beschränkt sich im übrigen auf Falltypen, bei welchen die Verletzung schutzwürdiger Geheimhaltungsinteressen **immer** auszuschließen ist. Nicht aufgenommen in den Katalog wurden daher Verwendungskonstellationen, in welchen die Verletzung schutzwürdiger Geheimhaltungsinteressen zwar unwahrscheinlich ist, aber doch nicht von vornherein ausgeschlossen werden kann, sodaß eine Beurteilung von Fall zu Fall notwendig ist (ein Beispiel hiefür wäre die Datenverwendung im Rahmen vorvertraglicher Maßnahmen – vgl. Art. 7 lit. b Richtlinie).

Ein gesondertes Problem stellt die Verwendung von strafrechtsbezogenen Daten dar. Solche Daten sind nach der Richtlinie nicht "sensible Daten", werden aber – zu recht – in die Nähe dieser Daten gerückt (vgl. Art. 8 Abs. 5 Richtlinie). Die Verarbeitung strafrechtsbezogener Daten muß daher möglichst beschränkt bleiben, weshalb Abs. 4 Z 3 Grenzen zieht, innerhalb welcher die Verwendung dieser Daten auch durch private Auftraggeber zulässig sein soll.

Zu § 9 des Entwurfs (Schutzwürdige Geheimhaltungsinteressen bei der Verwendung sensibler Daten):

Die Zulässigkeit der Verwendung sensibler Daten ist weitgehend durch die Richtlinie 95/46/EG vorgegeben: § 9 gibt zunächst die in Art. 8 Abs. 2 und 3 Richtlinie statuierten Ausnahmen vom Verwendungsverbot wieder. Hinzu treten

– die Ausnahme der Z 2, in der kein Geheimhaltungsanspruch gemäß § 1 Abs. 1 besteht,

– die Ausnahme der Z 10, soweit sie sich auf Verarbeitungen für private Zwecke bezieht, da für diese Datenverwendungen die Richtlinie nicht anzuwenden ist (Art. 3 Abs. 2, 2. Anstrich, Richtlinie),

– die Ausnahmen nach Z 3, Z 4 und Z 5 sowie nach Z 10 hinsichtlich § 46 und § 47: In allen diesen Fällen ergibt sich die Zulässigkeit der Ausnahme vom Verwendungsverbot aus Art. 8 Abs. 4 Richtlinie, da diese Bestimmungen des § 9 die Zulässigkeit der Verwendung von Daten "aus Gründen eines wichtigen öffentlichen Interesses" vorsehen (in Z 10 zB für Zwecke von wissenschaftlicher Forschung und Statistik, woran gemäß Erwägungsgrund 34 der Richtlinie ein wichtiges öffentliches Interesse besteht).

Zum Inhalt der einzelnen Ziffern des § 9 ist folgendes ergänzend anzumerken:

1. Ein wichtiges öffentliches Interesse im Sinne der Z 3 ist auch in den Interessen der Aufsicht über bestimmte Wirtschaftszweige zu erblicken: Gesetze, die die Verwendung von Daten für Zwecke einer besonderen Wirtschaftsaufsicht vorsehen, erfüllen ein wichtiges öffentliches Interesse; dies trifft etwa zu bei gesetzlichen Datenverwendungsbestimmungen im Rahmen der Banken- oder Versicherungsaufsicht.

2. Die Verwendung sensibler Daten zur Rechtsverteidigung gemäß Z 9 schließt naturgemäß die Zulässigkeit der Verwendung dieser Daten im Vorfeld einer gerichtlichen – oder verwaltungsbehördlichen – Auseinandersetzung ein, also zB auch die Verwendung im Rahmen des Versuchs einer außergerichtlichen Streitbeilegung.

Daß – gegenüber früheren Entwürfen – die Regelungen des § 9 im einfachgesetzlichen Rang vorgenommen werden konnten, wurde dadurch erreicht, daß in § 1 Abs. 2 der Gesetzesvorbehalt für Eingriffe nunmehr – so wie Art. 8 Abs. 2 EMRK dies festlegt – ausdrücklich auf Eingriffe durch **staatliche Behörden** beschränkt wurde. Dadurch stehen Regelungen wie Z 10 bis 13, soweit sie Eingriffe durch private Dritte betreffen, nicht im Widerspruch zu § 1 Abs. 2 und bedürfen daher keines Verfassungsranges. Die Implementierung des in der Richtlinie enthaltenen Verbots, weitere – dh. über Art. 8 Abs. 2 und 3 Richtlinie hinausgehende – Fälle zulässiger Eingriffe **durch private Dritte** in Gesetzen vorzusehen, ergibt sich bereits aus dem Vorrang des Gemeinschaftsrechts gegenüber dem nationalen Recht und bedarf deshalb ebenfalls keiner besonderen verfassungsrechtlichen Absicherung.

Zu § 10 des Entwurfs (Zulässigkeit der Überlassung von Daten zur Erbringung einer Dienstleistung):

Die Verantwortung des Auftraggebers hinsichtlich einer Kontrolle des Dienstleisters wird durch jene Rechtsvorschriften oder Standesregeln beschränkt, die eine Einflußnahme des Auftraggebers auf die Auftragsdurchführung durch den Dienstleister ausschließen. In welchen Fällen aus der Pflicht zur selbständigen Aufgabenerfüllung durch den Auftragnehmer gemäß § 4 Z 4 sogar die datenschutzrechtliche Auftraggebereigenschaft abzuleiten ist, wird in Form von Verhaltensregeln im Sinne des § 6 Abs. 4 ausdrücklich darzustellen sein.

Die bisher bestehende generelle Anzeigepflicht an die Datenschutzkommission bei der Heranziehung von Dienstleistern durch Auftraggeber des öffentlichen Bereichs ist nicht mehr zeitgemäß. Die Datenverarbeitung ist seit dem Inkrafttreten des bisher geltenden Datenschutzgesetzes zu einem so allgemeinen Phänomen geworden, daß eine derartig aufwendige Mitwirkungskompetenz der Datenschutzkommission in keiner sachgerechten Relation zum Schutzzweck steht. Die Anzeigepflicht an die Datenschutzkommission ist daher nunmehr auf die Heranziehung von (privaten) Dienstleistern bei Datenanwendungen, die infolge ihrer Sensibilität der Vorabkontrolle unterliegen, beschränkt.

Zu den §§ 12 und 13 des Entwurfs (Übermittlung und Überlassung von Daten ins Ausland):

Als Ergebnis der durch die Richtlinie angestrebten Harmonisierung der datenschutzrechtlichen Rechtsvorschriften der EU-Mitgliedstaaten soll in Hinkunft die datenschutzrechtliche Kontrolle des Datenverkehrs zwischen EU-Staaten entfallen (**§ 10 Abs. 1** erster Satz). Dieses Prinzip gilt allerdings **nicht** hinsichtlich der Datenverwendung für Zwecke der sogenannten "dritten Säule" (Zusammenarbeit der EU-Mitgliedstaaten im Bereich Justiz und Inneres), weil diese Bereiche von der Richtlinie nicht erfaßt sind und daher nicht dem Harmonisierungsgebot unterliegen, was Voraussetzung für den unbeschränkten Datenverkehr wäre. Was die Daten juristischer Personen betrifft, besteht allerdings ebenfalls kein harmonisiertes Datenschutzniveau in den EU-Mitgliedstaaten. Dennoch scheint es gerechtfertigt, sie in den unbeschränkt zulässigen Datenverkehr zwischen EU-Mitgliedstaaten einzubeziehen, da in den anderen Mitgliedstaaten unter anderer Bezeichnung (zB "Schutz der Betriebsgeheimnisse") Regelungen bestehen, die dem österreichischen Schutzniveau gegenüber keine gravierenden Nachteile befürchten lassen müssen. Durch eine Regelung, die zum Entfall der Genehmigungspflicht auch beim Transfer von Daten juristischer Personen führt, wird außerdem ein wesentlicher kostensparender Effekt bei den Rechtsunterworfenen wie bei der Datenschutzkommission erzielt.

Über die im ersten Satz des Abs. 1 erwähnten Fälle hinaus sind auch die in **Abs. 3 und 4** geregelten Fälle des **Datenverkehrs ins Ausland ohne Beschränkungen zulässig;** dies entspricht den Bestimmungen des Art. 26 Abs. 1 der Richtlinie.

Für alle anderen Fälle des Datenverkehrs mit dem Ausland gilt der Grundsatz, daß der Datenexport nur zulässig ist,

– wenn beim Empfänger ein **"angemessenes Datenschutzniveau"** besteht (Art. 25 Abs. 1 Richtlinie) oder

– wenn der Auftraggeber der Übermittlung (Überlassung) gegenüber der

Datenschutzkommission das Vorliegen **ausreichender Garantien** für den Schutz der Betroffenenrechte im Ausland glaubhaft macht (Art. 26 Abs. 2 Richtlinie).

Für die Frage, wie festgestellt wird, ob ein "angemessenes Datenschutzniveau besteht", bietet der vorliegende Entwurf zwei alternative Antworten:

Wenn ein Staat generell ein angemessenes Datenschutzniveau besitzt, kann er in die Verordnung des Bundeskanzlers gemäß § 12 Abs. 2 aufgenommen werden, was bewirkt, daß der Datenverkehr mit diesem Staat zur Gänze ohne Beschränkungen zulässig ist. (Eine solche generelle Aussage ist auch hinsichtlich der Verwirklichung von Datenschutz in EU-Mitgliedstaaten betreffend die sogenannte "dritte Säule" zulässig). In allen anderen Fällen muß die Beurteilung von Fall zu Fall geschehen, und zwar anläßlich des Genehmigungsverfahrens gemäß § 13 Abs. 2 Z 1.

Die zum Zweck einer einheitlichen Beurteilung dieser Fragen in allen EU-Mitgliedstaaten vorgesehenen Mitteilungs- und Durchführungspflichten sind in den §§ 54 und 55 umgesetzt.

Zu § 14 des Entwurfs (Datensicherheitsmaßnahmen):

Die bisherigen Erfahrungen lassen es sinnvoll erscheinen, genauere Bestimmungen über Protokoll- und Dokumentationsdaten in das DSG aufzunehmen, und zwar sowohl hinsichtlich der Zulässigkeit ihrer Weiterverwendung als auch hinsichtlich der Dauer der Aufbewahrung.

Zu § 15 des Entwurfs (Datengeheimnis):

Die Verpflichtung des Auftraggebers und des Dienstleisters – einschließlich ihrer Mitarbeiter – zur Geheimhaltung von **Daten, die** ihnen **auf Grund** ihrer **berufsmäßigen Beschäftigung bekannt** geworden sind, ist bereits im geltenden DSG (§ 20) enthalten. Die Neuformulierung des **Abs. 3** im vorliegenden Entwurf soll die Verteilung der Verantwortlichkeit zwischen dem anordnenden Auftraggeber oder Dienstleister (– dies schließt anordnungsbefugte Organe derselben mit ein –) und durchführenden Mitarbeitern deutlicher zum Ausdruck bringen, was insbesondere auch im Hinblick auf die neu formulierten Verwaltungsstrafbestimmungen in § 52 notwendig war.

§ 15 gilt sowohl für Auftraggeber (und Dienstleister) des privaten Bereichs als auch für Auftraggeber (und Dienstleister) des öffentlichen Bereichs sowie für deren Mitarbeiter.

Zu § 16 des Entwurfs (Datenverarbeitungsregister):

Zur Sicherung der Publizität von Datenverarbeitungen sieht die Richtlinie drei alternative Instrumente vor:

– die Meldung von Datenanwendungen an ein Register, das von der unabhängigen Kontrollstelle (Art. 28 der Richtlinie) zu führen ist, oder

– die Bestellung eines internen Datenschutzbeauftragten, der eine Liste der Datenverarbeitungen des Auftraggebers zu führen hat, oder

– die Offenlegung von nicht meldepflichtigen Datenverarbeitungen durch den Auftraggeber auf Antrag jedes Interessierten.

Der vorliegende Entwurf macht entsprechend der österreichischen Tradition in erster Linie von dem Instrument eines Registers der Datenanwendungen Gebrauch; dieses ist in Hinkunft richtlinienkonform von der Datenschutzkommission zu führen. In § 23 ist für einen Teil der nichtmeldepflichtigen Datenanwendungen die Offenlegung durch den Auftraggeber auf Anfrage vorgesehen.

Zu § 17 des Entwurfs (Meldepflicht des Auftraggebers):

Jede Datenanwendung muß zur Eintragung in das Datenverarbeitungsregister gemeldet werden, soweit nicht eine ausdrückliche Ausnahme nach den Abs. 2 oder 3 besteht.

Die Ausnahmen nach Abs. 2 wurden aus folgenden Erwägungen vorgesehen:

An (zulässigerweise) veröffentlichten Daten besteht gemäß § 1 Abs. 1 kein Geheimhaltungsanspruch. Es ist daher nur konsequent, wenn Datenanwendungen, die **ausschließlich** solche Daten beinhalten, mangels Eingreifens in schutzwürdige Geheimhaltungsinteressen von der Meldepflicht ausgenommen sind (Z 1). Es sei aber ausdrücklich darauf hingewiesen, daß diese Ausnahme nicht anwendbar ist, wenn neben veröffentlichten Daten auch andere personenbezogene Daten in einer Datenanwendung verarbeitet werden, insbesondere Bewertungen, Analysen, Verknüpfungen, usw. von veröffentlichten Daten. Diese Ausnahme ist angesichts ihrer Grundrechtsrelevanz restriktiv zu interpretieren.

Hinsichtlich der Ausnahme von der Meldepflicht für öffentliche Register (Z 2) ist auf die Richtlinie zu verweisen (vgl. Art. 21 Abs. 3, 2. Unterabsatz, Richtlinie), wo dies ausdrücklich als zulässig erklärt wird.

Bei der Verwendung nur indirekt personenbezogener Daten (Z 3) besteht nach § 1 Abs. 1 ebenfalls kein Geheimhaltungsanspruch, weshalb eine Meldepflicht sachlich gerechtfertigterweise entfallen kann.

Z 4 betrifft die Verwendung von Daten für persönliche oder familiäre Tätigkeiten: Da diese vom Geltungsbereich der Richtlinie ausgenommen sind (Art. 3 Abs. 2, 2. Anstrich, Richtlinie) und in Österreich auch bisher nicht meldepflichtig waren, konnte der bisherige Rechtszustand richtlinienkonform aufrechterhalten werden.

Die Ausnahme von der Meldepflicht für publizistische Tätigkeiten (Z 5) entspricht der das Medienprivileg berücksichtigenden geltenden Rechtslage, die angesichts des Art. 9 der Richtlinie beibehalten werden konnte.

"Standardanwendungen" nach Z 6 des Abs. 2 sind Datenanwendungen, die in einem bestimmten Kontext üblicherweise vorgenommen werden und gleichzeitig inhaltlich die schutzwürdigen Geheimhaltungsinteressen voraussichtlich nicht gefährden, also zB insbesondere keine sensiblen Daten betreffen. Da die Vornahme solcher Anwendungen von jedermann in einer bestimmten Situation vorausgesetzt werden muß (zB Führung einer automationsunterstützten Buchhaltung), bedarf es keiner eigenen Meldung, um den Betroffenen auf die Existenz derartiger Datenanwendungen aufmerksam zu machen. Der Auftraggeber muß allerdings auf Anfrage **jedermann** offenlegen, welche Standardanwendungen er tatsächlich durchführt (§ 23). Die Richtlinie erlaubt diese Ausnahme in Art. 18 Abs. 2, 1. Anstrich.

Die in **Abs. 3** vorgesehenen Ausnahmen von der Meldepflicht betreffen sämtliche Fälle außerhalb des Geltungsbereiches der Richtlinie (vgl. Art. 3 Abs. 2, 1. Anstrich). Im Gegensatz zur bisherigen Regelung in § 4 Abs. 3 DSG sind nicht mehr alle Datenanwendungen der in Z 1 bis 5 genannten Bereiche von der Meldepflicht ausgenommen, sondern nur mehr jene, bei welchen die Nichtmeldung auf Grund der konkreten Zweckbestimmung der einzelnen Datenanwendung notwendig ist.

Weiters ist zu erwähnen, daß die einer Regelung durch Bundesgesetz zugänglichen manuellen Dateien gemäß § 58 nur dann meldepflichtig sind, wenn sie der Vorabkontrolle unterliegen. Eine darüber hinausgehende Meldepflicht scheint angesichts des Umstandes, daß die bisher bestehende Meldefreiheit nicht als grundsätzlicher Mangel empfunden wurde, entbehrlich. Die Richtlinienkonformität dieser Regelung ergibt sich aus Art. 18 Abs. 5.

Zu § 18 des Entwurfs (Aufnahme der Verarbeitung):

Richtlinienkonform ist in **Abs. 1** vorgesehen, daß die Verarbeitung von Daten grundsätzlich unmittelbar **nach** Erstattung der Meldung aufgenommen werden kann. Bei Verarbeitungen, die "spezifische Risiken für die Rechte und Freiheiten von Personen beinhalten können", sieht die Richtlinie 95/46/EG jedoch vor, daß sie einer sogenannten **"Vorabkontrolle"** zu unterwerfen sind, dh. daß sie vor ihrer Aufnahme durch die unabhängige Kontrollinstanz auf ihre Zulässigkeit zu prüfen sind. Dementsprechend ist in **Abs. 2** festgelegt, welche Kategorien von Datenanwendungen erst nach Prüfung und Registrierung aufgenommen werden dürfen. Diese Kategorien wurden unter Berücksichtigung der in der Richtlinie in Art. 18 Abs. 2 erster Anstrich erwähnten Beurteilungskriterien für das Gefährdungspotential von Datenverarbeitungen bestimmt.

Bei **sensiblen Daten (Z 1)** ist eine Ausnahme von der Vorabkontrolle im Falle des Bestehens einer Musterverordnung vorgesehen, sowie für die Fälle der Mitgliederverwaltungen von anerkannten Kirchen- und Religionsgesellschaften, die als innere Angelegenheit der Kirchen zwar einer staatlichen Ordnungsvorschrift wie der Meldepflicht unterworfen werden kann, nicht aber einer besonderen Zulässigkeitsgenehmigung.

Strafrechtsbezogene Daten (Z 2) werden von der Richtlinie zwar nicht als sensible Daten bezeichnet, aber hinsichtlich der Schutzwürdigkeit als "sensibilitätsnah" behandelt (vgl. Art. 8 Abs. 5 Richtlinie), weshalb ihre Unterstellung unter die Vorabkontrolle sachlich geboten erscheint.

Der Vorabkontrolle sind weiters Datenanwendungen unterworfen, die die **Auskunftserteilung über die Kreditwürdigkeit** von natürlichen oder juristischen Personen zum Gegenstand haben **(Z 3)**. Unter "Auskunftserteilung" ist nicht die aus den Unterlagen des Rechnungswesens in einem Unternehmen hervorgehende Information über kreditrelevantes Verhalten der eigenen Kunden (potentiellen Kunden) zu verstehen; von Z 3 erfaßt sollen vielmehr nur jene Datenanwendungen sein, deren ausschließlicher Zweck die Auskunftserteilung ist und zwar an Außenstehende für deren Zwecke (Vereinsmitglieder wären in diesem Sinn als Außenstehende zu betrachten, wenn etwa ein Verein ein Kreditauskunftssystem betreibt).

Schließlich **(Z 4)** unterliegt auch die Verarbeitung von Daten in Form eines **Informationsverbundsystems** (§ 4 Z 13) der Vorabkontrolle. Dies deshalb, weil hiedurch ein umfangreiches Netz von Übermittlungen von Daten geschaffen wird, woraus sich immer ein besonderes Gefährdungspotential ergibt.

Um jedoch auch im Bereich der der Vorabkontrolle unterliegenden Datenanwendungen keine unnötigen Erschwernisse für Auftraggeber zu bewirken, wurde in § 20 Abs. 3 für die Datenschutzkommission die Verpflichtung geschaffen, bereits anläßlich eines allfälligen Verbesserungsauftrages darüber zu entscheiden, ob die Verarbeitung sofort aufgenommen werden darf oder bis zur Entscheidung über die Registrierung zugewartet werden muß.

Zu § 19 des Entwurfes (Inhalt der Meldung):

Neu ist hinsichtlich des Inhalts von Meldungen nur **Abs. 1 Z 7**, wonach in Erfüllung der Erfordernisse der Richtlinie 95/46/EG allgemeine Angaben über die im konkreten Fall bestehenden Datensicherheitsmaßnahmen zu machen sind (– die allerdings im Register nicht

einsehbar sind!). Zu denken wäre hier an Aussagen darüber, ob die gemäß § 14 Abs. 2 erforderlichen Maßnahmen ergriffen wurden, oder welche Ziffern des § 14 Abs. 2 nicht umzusetzen waren, weil dies im konkreten Fall im Lichte des § 14 Abs. 1 nicht erforderlich war.

Für jene Fälle, in welchen Datenanwendungen mit demselben Inhalt von vielen Auftraggebern in gleicher Weise durchgeführt werden, wegen ihres Zwecks oder wegen der verarbeiteten Datenarten für eine Erklärung zur Standardanwendung (§ 17 Abs. 2 Z 6) aber nicht in Frage kommen, wurde die Möglichkeit der Festlegung von Musteranwendungen geschaffen (§ 19 **Abs. 2**): Durch Verordnung kann – so wie bisher bei den Standardverarbeitungen – der maximal zulässige Inhalt einer bestimmten Datenanwendungstype festgelegt werden, und zwar in der Art und Weise, wie eine Meldung an das Datenverarbeitungsregister vorzunehmen wäre. Die tatsächliche Meldung wäre sodann in jener Form vorzunehmen, wie sie derzeit für Standardverarbeitungen gilt.

Die Meldung von Datenanwendungen, die einer Musteranwendung entsprechen, in der in § 19 Abs. 2 vorgesehenen Form stellt keine Vereinfachung der Meldung im Sinne des Art. 18 Abs. 2 Richtlinie dar, da der gesamte von Art. 19 der Richtlinie geforderte Inhalt der Datenanwendung eindeutig offengelegt wird: Die Auftraggeber einer Datenanwendung dürfen von der Meldeform nach § 19 Abs. 2 nur Gebrauch machen, wenn in ihrer Datenanwendung nicht mehr als der durch die Musterverordnung definierte Inhalt verwirklicht ist, sodaß durch diese Form der Meldung die schutzwürdigen Interessen der Betroffenen, insbesondere ihr Interesse an einer entsprechenden Publizität der Verwendung von Daten, nicht gefährdet sein kann.

Zu § 20 (Prüfungs- und Verbesserungsverfahren):

Hinsichtlich des Verfahrens der Vorabkontrolle ist ausdrücklich vorgesehen, daß bei Untätigkeit der Datenschutzkommission die Verarbeitung von Daten jedenfalls zwei Monate nach Abgabe der Meldung aufgenommen werden kann. Wenn hingegen im Falle eines Verbesserungsauftrages im Vorabkontrollverfahren entschieden wird, daß die Verarbeitung noch nicht aufgenommen werden darf, gelten die Entscheidungsfristen des AVG einschließlich der Möglichkeit der Säumnisbeschwerde für die Entscheidung darüber, ob die aufgetragenen Verbesserungen vorgenommen wurden und davon abgeleitet, ob die Verarbeitung aufgenommen werden darf.

Zu § 22 des Entwurfs (Richtigstellung des Registers):

Die bisherigen Erfahrungen haben gezeigt, daß eine vereinfachte Berichtigungsmöglichkeit für Registereintragungen, deren Unrichtigkeit aus amtlichen Quellen eindeutig hervorgeht, zweckmäßig wäre. Durch § 22 Abs. 3 in Verbindung mit § 38 Abs. 1 wird für diese Richtigstellungen eine Art von "Einzelrichterentscheidung" in einem Mandatsverfahren geschaffen mit der Möglichkeit, Vorstellung an das Plenum der Datenschutzkommission zu erheben. Die weitere Anrufbarkeit des Verwaltungsgerichtshofes ist gemäß § 40 Abs. 2 ausgeschlossen, da bei der vorliegenden Konstellation ein Abgehen von der Grundsatzregelung des Art. 133 Z 4 B-VG nicht geboten erscheint.

Zu § 23 des Entwurfs (Offenlegung nicht meldepflichtiger Datenverarbeitungen):

Die Richtlinie 95/46/EG schreibt in Art. 21 Abs. 3 bei Datenanwendungen, die von der Meldepflicht ausgenommen sind, vor, daß der Inhalt der Datenverarbeitung auf andere geeignete Weise auf Antrag jedermann verfügbar gemacht werden muß. Die hier vorgeschlagene Lösung überträgt diese Pflicht dem Auftraggeber, und zwar nur hinsichtlich von Standardanwendungen: Dies ist richtlinienkonform, weil Datenanwendungen für den persönlichen oder familiären Bereich (§ 17 Abs. 2 Z 4) und die in § 17 Abs. 3 genannten Datenanwendungen außerhalb des Geltungsbereiches der Richtlinie liegen; gesetzlich vorgesehene öffentliche Register (§ 17 Abs. 2 Z 2) dürfen gemäß ausdrücklicher Bestimmung der Richtlinie (Art. 21 Abs. 3) von der Offenlegungspflicht ausgenommen werden (– die Existenz dieser Register ergibt sich schon aus gesetzlichen Vorschriften); auch die Ausnahme zugunsten journalistischer Tätigkeit ist durch Art. 9 der Richtlinie bereits vorgezeichnet. Die Verwendung von veröffentlichten oder von nur indirekt personenbezogenen Daten bedarf deshalb keiner besonderen Offenlegung, weil schutzwürdige Geheimhaltungsinteressen der Betroffenen nicht berührt werden (vgl. dazu die Ausführungen zu § 1 Abs. 1; letztere Ausnahme steht auch nicht im Widerspruch zur Richtlinie: vgl. dazu die Ausführungen zu § 8 Abs. 2).

Zu § 24 des Entwurfs (Informationspflicht des Auftraggebers):

Dies ist eine der wesentlichsten Neuerungen der Richtlinie gegenüber der bisherigen österreichischen Rechtslage. Sie soll es dem Betroffenen erleichtern, seine Rechte zu wahren. "Datenverarbeitung nach Treu und Glauben (vgl. § 6 Abs. 1 Z 1 DSG) setzt voraus, daß die Betroffenen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden" (EG 38 zur Richtlinie 95/46/EG).

Der DSG-Entwurf sieht als Instrumente für diesen Zweck die Information nach **§ 24**, das Datenverarbeitungsregister, die Offenlegung nach § 23 und schließlich die Auskunft gemäß **§ 26** vor. Schon aus dem Sachlichkeitsgebot ergibt sich, daß es sich hier nicht um Pflichten handeln kann, die alle denselben Inhalt haben. Diese Instrumente haben einander vielmehr so zu ergänzen, daß der Betroffene verläßlich jene Informationen erhält, die er zur Durchsetzung seiner Datenschutzrechte braucht und zwar ohne unzumutbare Anstrengungen seinerseits, aber auch ohne unzumutbare und unnötige Belastung der Auftraggeber. Deshalb

kann diese Verpflichtung vorzusorgen, daß "der Betroffene in der Lage ist, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden", nicht so verstanden werden, daß sich daraus ein Zwang zur Verdoppelung der Meldepflicht (an das Register) in Form einer zusätzlichen Pflicht zur "Meldung an den Betroffenen" ergibt; diesfalls müßte die Führung eines Registers als überflüssiger und daher unverhältnismäßiger Aufwand betrachtet werden. Vor dem Hintergrund des Bestehens einer Registrierungspflicht muß vielmehr der Sinn einer zusätzlichen Informationspflicht darin gesehen werden, daß dem Betroffenen immer dann, "wenn ihm diese Information nicht bereits vorliegt", der Hinweis darauf gegeben wird, daß seine Daten von einem bestimmten Auftraggeber für einen bestimmten Zweck verarbeitet werden sollen. Dadurch wird er in die Lage versetzt, sich – falls er dies wünscht – aller Hilfsmittel zu bedienen, um "ordnungsgemäß und umfassend informiert zu werden".

Aus diesen Darlegungen folgt, daß die Frage, ob Informationen mit dem Inhalt des § 24 **Abs. 1** "bereits vorliegen", nach der jeweiligen Situation zu beurteilen ist. Es ist dabei durchaus denkbar, daß zB die Umstände, unter welchen Daten beim Betroffenen erhoben werden, jeden Zweifel darüber ausschließen, daß die Daten vom Datenermittler für einen dem Betroffenen unmittelbar einsichtigen Zweck verarbeitet werden. Diesfalls ist eine ausdrückliche Information des Betroffenen unnötig und würde wahrscheinlich bei ihm auch nur Befremden hervorrufen.

Andererseits werden bestimmte Situationen entsprechend dem Gebot der Verarbeitung nach "Treu und Glauben" über Abs. 1 hinausgehende Informationen erfordern. Diesem Umstand trägt **Abs. 2** Rechnung. Diese Information hat nicht den Charakter einer umfassenden Rechtsbelehrung für den konkreten Einzelfall; vielmehr wäre etwa bei einer Information gemäß Z 1 auf das Bestehen des Widerspruchsrechtes gemäß § 28 – allenfalls unter Zitierung dieser Bestimmung – hinzuweisen.

Da die richtige Information somit unter Umständen die Beurteilung eines komplexen Sachverhaltes voraussetzt, kann es sinnvoll sein, das Ausmaß der Informationspflicht in einzelnen typischen Situationen durch Verhaltensregeln nach § 6 Abs. 4 zu klären. Die Befolgung solcher Verhaltensregeln wird im Hinblick auf eine etwaige Strafbarkeit nach § 52 von wesentlicher Bedeutung sein.

Daß nur meldepflichtige Datenverarbeitungen der Informationspflicht unterliegen (§ 24 **Abs. 4**), geht aus der Natur der gemäß § 17 Abs. 2 und 3 nicht meldepflichtigen Fälle hervor:

– Für Verarbeitungen zu persönlichen und familiären Zwecken gilt die Richtlinie nicht und daher auch nicht die Informationspflicht;

– bei der Verwendung nur indirekt personenbezogener Daten ist eine Information nicht möglich, da der Auftraggeber die Betroffenen nicht kennt;

– hinsichtlich von Datenanwendungen, die ausschließlich veröffentlichte Daten beinhalten, ist gemäß § 1 Abs. 1 davon auszugehen, daß daran keine schutzwürdigen Geheimhaltungsinteressen bestehen;

– bei publizistischen Tätigkeiten und den Datenanwendungen nach § 17 Abs. 3 gelten dieselben Gründe, die gegen eine Meldepflicht sprechen auch gegen die Informationspflicht;

– die Führung von durch Gesetz eingerichteten öffentlichen Registern muß als bekannt vorausgesetzt werden (– "die Information liegt vor" –);

– die Durchführung von Standardverarbeitungen geschieht jeweils in einem Kontext, der für den Betroffenen erkennbar ist und umfaßt die aus einer – im BGBl. veröffentlichten – Verordnung ersichtlichen Daten, sodaß auch in diesem Fall davon auszugehen ist, daß "die Information dem Betroffenen vorliegt"; (sollte beim Betroffenen dennoch ein Zweifel bestehen, hat ihm der Auftraggeber gemäß § 23 die Frage zu beantworten, ob und welche Standardanwendungen er vornimmt).

Zu § 25 des Entwurfs (Offenlegung der Identität des Auftraggebers):

Die Pflicht zur Offenlegung der Identität des Auftraggebers **(Abs. 1)** auch in jenen Fällen, in welchen keine Registernummer geführt wird, soll die bloße Verwendung von Postfächern, Telefonnummern usw. zur Identifizierung des Auftraggebers unterbinden oder zumindest nach § 52 Abs. 2 unter bestimmten Voraussetzungen strafbar machen.

Die bisherigen Erfahrungen haben gezeigt, daß die Verfolgung von Betroffenenrechten dann sehr schwierig ist, wenn Daten eines Auftraggebers – zB im Marketingbereich – für Zwecke eines anderen verwendet werden. Der Betroffene kann bei dieser Konstellation die Identität desjenigen, der seine Daten gespeichert hält und sie immer wieder benutzt, oft nicht feststellen und daher auch sein Widerspruchs- oder Löschungsrecht nicht effektiv geltend machen. Diesem Problem soll § 25 **Abs. 2** abhelfen.

Zu § 26 des Entwurfes (Auskunftsrecht):

Im neuen § 26 sind die bisher zum Auskunftsrecht geltenden §§ 11 und 25 DSG zusammengefaßt.

Abs. 2 regelt nunmehr ausführlicher als bisher, in welchen Fällen im öffentlichen

Interesse oder im Interesse Dritter keine Auskunft zu geben ist. Die Zulässigkeit dieser Ausnahmen stützt sich auf Art. 13 der Richtlinie. Im übrigen wird – in Übereinstimmung mit Art. 13 Richtlinie – auch der Fall einbezogen, daß das Auskunftsrecht zum Schutz des Betroffenen einzuschränken ist; dies wird freilich nur in wenigen Ausnahmefällen gerechtfertigt sein (zB im medizinischen Bereich oder hinsichtlich von Auskünften aus dem Strafregister).

Im Hinblick darauf, daß im vorliegenden Entwurf keine dem bisher geltenden § 4 Abs. 3 DSG entsprechende Bestimmung enthalten ist, mußte in § 26 – ebenso wie in § 27 – ausführlicher auf die dem § 4 Abs. 3 zugrundeliegende Problematik eingegangen werden: Abgesehen von den Bestimmungen des Abs. 2 Z 1 – 5 ist vor allem auch nunmehr ausdrücklich in **Abs. 5** geregelt, wie das Auskunftsrecht in diesen, grundsätzlich der Geheimhaltung unterliegenden, Bereichen durchsetzbar ist, wobei der Rolle der Datenschutzkommission besondere Bedeutung zukommt. Der Inhalt des Abs. 5 orientiert sich weitgehend an § 62 SPG, der für den Bereich der Sicherheitspolizei die Handhabung des Auskunftsrechts einer eingehenden Regelung unterzogen hat. (Eine Abstimmung mit den neuen Bestimmungen der §§ 26 und 27 wird im übrigen durch Novellierung des SPG erfolgen müssen.)

Im übrigen enthält der vorliegende § 26 gegenüber der bisherigen Rechtslage nur einige Korrekturen zur Vereinheitlichung und Klarstellung:

Die Verpflichtung des Betroffenen, im Rahmen des Auskunftsverfahrens mitzuwirken **(Abs. 3),** wurde beibehalten. In der Richtlinie finden sich mehrfach Bestimmungen, die der Ausübung von Betroffenenrechten Grenzen setzen, und zwar dort, wo die Rechtsausübung der Betroffenen einen unverhältnismäßigen Aufwand beim Auftraggeber verursachen würde (vgl. die Informationspflicht nach Art. 11 oder die Verständigungspflicht an Datenempfänger gemäß Art. 12). Dieser Grundsatz ist aus der Verpflichtung zur entsprechenden Berücksichtigung der Rechte und Freiheiten Dritter abzuleiten und wird auch beim Auskunftsrecht Geltung beanspruchen dürfen. Gerade bei Auftraggebern mit sehr vielen Datenverarbeitungen kann die Verpflichtung des Auftraggebers, alle seine Datenverarbeitungen zu durchsuchen, wenn der Betroffene nicht den mindesten Hinweis darauf gibt oder geben will, in welchem Zusammenhang er in den Datenanwendungen des Auftraggebers vorhanden sein könnte, eine beträchtliche Belastung des Auftraggebers (unter Umständen sogar Stillegung der Datenverarbeitung für einige Zeit) bewirken. In dem Bestreben, einen Interessensausgleich zwischen dem Betroffenen und dem Auftraggeber zu erzielen, statuiert daher Abs. 3, daß der Betroffene in dem ihm zumutbaren Ausmaß mitwirken muß, und **Abs. 6,** daß die Auskunft dann unentgeltlich zu erteilen ist, wenn die Auffindung der zu beauskunftenden Daten für den Auftraggeber keine besondere Belastung darstellt ("wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft"). In allen anderen Fällen ist die Auskunft kostenpflichtig, wobei ein niedriger Grundtarif im Gesetz festgelegt ist, von dem bei tatsächlich erwachsenden höheren Kosten abgewichen werden darf. Auch Portokosten sind den tatsächlich erwachsenden Kosten zuzuzählen. Ob derartige Abweichungen gerechtfertigt sind, wäre in einem Verfahren vor der Datenschutzkommission gemäß § 31 Abs. 1 überprüfbar.

Zu § 27 des Entwurfs (Recht auf Richtigstellung oder Löschung):

§ 27 stellt im Gegensatz zur bisherigen Rechtslage die zusammenfassende Regelung des Rechtes auf Richtigstellung oder Löschung dar (– diese war bisher verteilt über die §§ 12, 26 und 27 DSG). Es wurde hiebei eine Vereinheitlichung des Verfahrens und eine Vereinfachung der Regelungen angestrebt.

Im § 27 **Abs. 1** wird zunächst klargestellt, daß die Verpflichtung zur Richtigstellung oder Löschung von Daten den Auftraggeber auch dann trifft, wenn der Betroffene dies nicht eigens beantragt hat. Weiters werden Klarstellungen gegeben, wann Unvollständigkeit und wann Unzulässigkeit der Verarbeitung in bestimmten Konstellationen vorliegt.

Abs. 3 trägt dem Umstand Rechnung, daß manche Datenanwendungen nach ihrem besonderen Zweck eine Löschung von Daten in der Form, daß Daten nicht mehr sichtbar sind, nicht gestatten. Dies wird überall dort der Fall sein, wo die lückenlose Dokumentation eines Geschehens Gegenstand der Datenverarbeitung ist (zB bei der Führung von Krankengeschichten).

Abs. 5 enthält Regelungen in Ergänzung des § 26 Abs. 2 Z 1 bis 5 und Abs. 5: Diese Bestimmungen des § 26 bedürfen besonderer Folgeregelungen hinsichtlich der Ausübung des Richtigstellungs- und Löschungsrechts, wenn hiedurch der Zweck des § 26 Abs. 5 nicht vereitelt werden soll.

Zu § 28 des Entwurfs (Widerspruchsrecht):

Ein eigenes Widerspruchsrecht hat sich bisher im österreichischen Datenschutzrecht nicht gefunden. Die Richtlinie 95/46/EG sieht ein solches in Art. 14 vor.

Ausgehend von der zum Teil sehr allgemeinen Formulierung der Zulässigkeitsvoraussetzung für Datenverarbeitungen in Art. 7 der Richtlinie (insbesondere lit. e und f) enthält die Richtlinie als Korrekturmöglichkeit ein Widerspruchsrecht, wonach der Betroffene verlangen kann, daß er aus "sich aus seiner besonderen Situation ergebenden Gründen" aus einer Datenanwendung, gegenüber der das Widerspruchsrecht geltend macht, gelöscht wird.

Zur Frage, wo der Unterschied zwischen einer Beschwerde (Klage) wegen unzulässiger Verarbeitung von Daten nach den §§ 31 oder 32 und der Ausübung des Widerspruchrechts nach § 28 **Abs. 1** liegt, ist folgendes auszuführen:

Die Richtlinie enthält in Art. 14 keine klare Aussage über diese Frage und gibt auch keinen Hinweis auf möglicherweise unterschiedliche Folgen. Daraus, daß in Art. 14 aber auch auf das Widerspruchsrecht im Bereich der Verwendung von Daten für Marketingzwecke Bezug genommen wird, könnte folgender Schluß gezogen werden:

Die Ausübung des Widerspruchsrechts hat keinen Einfluß auf die rechtliche Zulässigkeit der Datenanwendung an sich. Sie bewirkt nur eine individuell auf den (erfolgreich) Widersprechenden begrenzte Löschungspflicht, bedeutet aber nicht, daß die gesamte Datenanwendung wegen Rechtswidrigkeit einzustellen wäre. Die erfolgreiche Ausübung des Widerspruchsrechts wird daher – zumindest grundsätzlich – auch keinen Schadenersatzanspruch begründen können.

In **Abs. 2** wird eine zusätzliche Spielart des Widerspruchsrechts ausdrücklich geregelt, die in der Praxis nach den bisherigen Erfahrungen bedeutsam ist und nur die Nutzanwendung des bereits zu Abs. 1 Gesagten auf eine besondere Konstellation darstellt: Es gibt wiederholt Anwendungsfälle, in welchen bei einer Durchschnittsbetrachtung eine Verletzung schutzwürdiger Geheimhaltungsinteressen infolge des Zwecks der Datenverarbeitung und der verwendeten Datenarten unwahrscheinlich ist (Beispielsfälle wären etwa Verzeichnisse österreichischer Gewerbetreibender, die für Exportförderungszwecke verwendet werden; Einwohnerverzeichnisse; Verzeichnisse von Fernsprechteilnehmern, Telefaxanschlüssen, E-Mail-Adressen, usw.). Derartige öffentlich zugängliche Verzeichnisse beruhen zum größten Teil nicht auf ausdrücklichen gesetzlichen Regelungen. Um einen fairen Interessensausgleich zu gewährleisten, scheint es sinnvoll, Personen ein Widerspruchsrecht gegen die Aufnahme in solche Verzeichnisse einzuräumen, wenn sie in Abweichung von der durchschnittlichen Einschätzung der Geheimhaltungsinteressen eine Verletzung ihrer Interessen durch Aufnahme ihrer Daten in ein solches Verzeichnis befürchten. Durch die Möglichkeit des Widerspruchs wäre gewährleistet, daß einerseits Verzeichnisse dieser Art, die von der großen Mehrheit der Bevölkerung als sinnvoll und nützlich empfunden werden, legalerweise existieren können und andererseits Interessenslagen, die vom Durchschnitt abweichen, entsprechend berücksichtigt werden können und diese Berücksichtigung auch einfach durchzusetzen ist.

Die in Art. 14 lit. b getroffenen Regelungen über ein Widerspruchsrecht gegenüber Datenverarbeitungen für Zwecke der Direktwerbung bedürfen keiner Berücksichtigung im Datenschutzgesetz, weil sie bereits durch die besonderen Bestimmungen des § 268 Gewerbeordnung umgesetzt sind.

Zu § 30 des Entwurfs (Kontrollbefugnisse der Datenschutzkommission):

Die Richtlinie 95/46/EG mißt der Kontrolle von Datenanwendungen außerhalb förmlicher Beschwerdeverfahren große Bedeutung zu. Diese Kontrolle muß gemäß der Richtlinie auch im privaten Bereich möglich sein. Sie ist von einer unabhängigen Kontrollstelle wahrzunehmen und hat das Recht der Kontrollstelle zu beinhalten, Einschau in Datenverarbeitungen und Unterlagen zu nehmen, Auskünfte zu verlangen und dem Auftraggeber Empfehlungen und Ermahnungen zu erteilen; sie kann bis zu einem gewissen Grad auch rechtsförmliche Akte umfassen, soweit zB eine Kompetenz zur vorläufigen Untersagung der Weiterführung von Datenverarbeitungen besteht.

Das in Österreich traditionelle System des Vollzugs von Datenschutz hat bisher den Schwerpunkt auf rechtsförmliche Entscheidung durch die Datenschutzkommission bzw. durch die Gerichte gelegt und nur im öffentlichen Bereich eine Kontrolle laufender Datenverarbeitungen (§ 41 DSG) vorgesehen. Im vorliegenden Entwurf sind nun die Kontrollbefugnisse in der Weise umgesetzt, daß die Datenschutzkommission als unabhängige Kontrollstelle den öffentlichen und den privaten Bereich zu kontrollieren hat, und zwar entweder aus Anlaß eines Anbringens eines Bürgers oder auch in Fällen, die ein erhöhtes Gefährdungspotential besitzen, ohne einen solchen Anlaß. Rechtsförmliche Entscheidungen über behauptete Datenschutzverletzungen werden hingegen so wie bisher von der Datenschutzkommission zu erlassen sein, wenn sie Auftraggeber des öffentlichen Bereichs betreffen, und von den ordentlichen Gerichten, wenn sie Auftraggeber des privaten Bereichs betreffen.

Die Konsequenzen der Nichtbefolgung einer Empfehlung der Kontrollstelle sind in **Abs. 4** näher geregelt, wobei darauf hinzuweisen ist, daß **Z 4** die bisherigen Bestimmungen des § 41 DSG ersetzt.

Die Verpflichtung zur möglichsten Schonung der Rechte des Auftraggebers (Dienstleisters) bedeutet auch, daß eine Einschau grundsätzlich nur innerhalb der Betriebszeiten vorgenommen werden darf.

Die Einschau durch die DSK dient einem eng begrenzten Ziel, nämlich der Durchsetzung von Datenschutz. Es erscheint daher sachlich gerechtfertigt, die Verwertung der durch die Einschau gewonnenen Informationen auf datenschutzrechtliche Belange zu begrenzen; die insbesondere in § 26 StPO und § 158 BAO statuierte Pflicht zur Offenlegung von Informationen und die Verpflichtung zur Erstattung von Anzeigen nach § 84 StPO und § 81 FinStrG wurde daher – soweit keine datenschutzrechtlich relevanten Straftatbestände betroffen sind – auf besonderes schwerwiegende (gerichtlich ahndbare) Straftaten beschränkt, nämlich auf Verbrechen mit einer Mindeststrafdrohung von fünf Jahren. Hiedurch wird auch gewährleistet, daß die im Bankwesengesetz (§ 41 Abs. 6) und im Wertpapieraufsichtsgesetz (§ 30 Abs. 3) im Interesse der Wahrung des Bankgeheimnisses enthaltenen Regelungen nicht unterlaufen werden.

Zu § 31 des Entwurfs (Beschwerde an die Datenschutzkommission):

Die Datenschutzkommission übt neben ihrer Kontrollfunktion auch eine quasi-richterliche Entscheidungsfunktion in ihrer Rolle als Behörde gemäß Art. 133 Z 4 B-VG aus. Sie erkennt in rechtsförmlichen Verfahren mit Bescheid über Beschwerden wegen behaupteter Verletzungen des Datenschutzgesetzes durch einen Auftraggeber des öffentlichen Bereichs. Eine Besonderheit des Entwurfes gegenüber der bisherigen Rechtslage ist die nunmehrige umfassende Zuständigkeit für Verletzungen des Auskunftsrechtes **(Abs. 1),** gleichgültig, ob diese einem Auftraggeber des öffentlichen Bereichs oder einem Auftraggeber des privaten Bereichs zur Last gelegt werden. Hinsichtlich aller anderen behaupteten Verletzungen ist die Datenschutzkommission nur dann zuständig, wenn sie einen Auftraggeber des öffentlichen Bereichs betreffen **(Abs. 2),** insgesamt aber immer nur im Hinblick auf die Prüfung von Handlungen, die weder der Gerichtsbarkeit noch der Gesetzgebung zuzurechnen sind, wobei die Zurechnung nach funktionalen Gesichtspunkten vorzunehmen ist.

§ 31 **Abs. 4** enthält besondere Regelungen für solche Beschwerdeverfahren, die in Konsequenz von §§ 26 Abs. 5 und 27 Abs. 5 vor der Datenschutzkommission geführt werden. Diese Regelung derogiert § 62 Abs. 4 und 5 SPG.

Zu § 32 des Entwurfs (Anrufung der Gerichte):

Der Betroffene hat Anspruch auf Unterlassung und Beseitigung eines dem DSG widerstreitenden Zustands. Ist Verursacher ein Auftraggeber des privaten Bereichs, so sind diese Ansprüche vor den ordentlichen Gerichten durchzusetzen. Einzige Ausnahme hievon ist die Durchsetzung des Auskunftsrechts, für die in Hinkunft immer die Datenschutzkommission zuständig sein soll.

Gegenüber den bisherigen Bestimmungen über das zivilgerichtliche Verfahren in Datenschutzsachen bringt die vorliegende Regelung insofern eine Neuerung, als die Datenschutzkommission anstelle des Betroffenen bei dem zuständigen ordentlichen Gericht Klage zur Feststellung der Rechtmäßigkeit einer Datenverwendung erheben kann. Diese Möglichkeit ist auf vermutete schwerwiegende Datenschutzverletzungen beschränkt und soll für solche Fälle, an deren Klärung somit auch ein öffentliches Interesse besteht, das Prozeßrisiko des Betroffenen vermeiden. Auf der Grundlage des gerichtlichen Feststellungsurteils kann der Betroffene sodann entscheiden, ob er seine Unterlassungs- und Schadenersatzansprüche selbst weiterverfolgen will.

Die Gutachterrolle der Datenschutzkommission über technische und organisatorische Fragen hat sich als praktisch nicht bedeutsam erwiesen und ist deshalb in der vorliegenden Bestimmung nicht mehr ausdrücklich angesprochen. Die Möglichkeit einer Nebenintervention gemäß § 17ff ZPO wurde hingegen beibehalten.

Auch die Eintragung von gerichtlichen Urteilen in das Datenverarbeitungsregister hat sich als praktisch nicht bedeutsam erwiesen, weshalb dies nicht mehr ausdrücklich in den Gesetzesentwurf aufgenommen wurde. Für die Veröffentlichung von richtungsweisenden gerichtlichen Entscheidungen scheinen die üblichen Publikationswege ausreichend.

Zu § 33 des Entwurfs (Schadenersatz):

In Umsetzung von Art. 23 Abs. 1 der Richtlinie enthält § 33 nunmehr ausdrückliche Bestimmungen über den Ersatz erlittenen Schadens. Dafür gelten zunächst die allgemeinen Bestimmungen des Schadenersatzrechts; gehaftet wird nur bei Verschulden. Für Fälle schwerwiegender rechtswidriger Datenverwendung, die ihrem Wesen nach Tatbeständen vergleichbar sind, die nach Mediengesetz zum Schadenersatz verpflichten, sieht **Abs. 1** den Ersatz immaterieller Schäden vor, wobei sich die näheren Voraussetzungen und die Höhe der Entschädigung aus den §§ 6 und 7 des Mediengesetzes ergeben. Daraus folgt, daß die Höhe der Entschädigung derzeit mit 200 000 S begrenzt ist. Da nur Fälle besonders schwerwiegender Datenschutzverletzungen zum immateriellen Schadenersatz berechtigen sollten, wurden die hier relevanten Fälle auf die Verwendung von Daten im Sinne des § 18 beschränkt; hiebei ist neben der fehlerhaften insbesondere auch die rechtsmißbräuchliche Datenverwendung Regelungsgegenstand.

Klargestellt sei, daß die Bestimmungen des DSG im Einzelfall auch als Schutzgesetz im Sinne des § 1311 ABGB greifen können. Das Grundrecht auf Datenschutz wird im übrigen auch zu den – absolut geschützten – Persönlichkeitsrechten im Sinne des § 16 ABGB zu zählen sein.

Verletzungen von Datenschutzbestimmungen erfolgen häufig außerhalb von Vertragsverhältnissen zum Geschädigten, sodaß die Regelung des § 1313a ABGB nicht zur Anwendung kommt. Auf Grund des Umstandes, daß es für den Betroffenen jedoch oft nicht möglich ist, die Arbeitsaufteilung und die daraus resultierende Verantwortlichkeit bei Datenverarbeitungsvorgängen nachzuvollziehen, erscheint es dennoch sachgemäß, die Regelung des § 1313a ABGB sinngemäß für sämtliche Haftungen aus rechtswidrigen Datenverwendungen zu übernehmen: Dem Auftraggeber und dem Dienstleister ist daher jeweils das Verhalten seiner Leute zuzurechnen, wobei der Dienstleister und seine Leute gleichzeitig "Leute des Auftraggebers" sind, sodaß die Haftung gegenüber dem Betroffenen zunächst beim Auftraggeber konzentriert wird. Allerdings kann sich der Auftraggeber von seiner Haftung gegenüber dem Betroffenen befreien, wenn er nachweist, daß der Umstand, durch den der Schaden verursacht wurde, ihm bzw. seinen Leuten nicht zur Last gelegt werden kann. Diese, in **Abs. 3** vorgesehene Beweislastumkehr zugunsten des Betroffenen setzt die zwingende Bestimmung des Art. 23 Abs. 2 der Richtlinie um.

Im übrigen gelten, etwa was Rückersatzansprüche oder die Haftung für Handlungen in Vollziehung der Gesetze betrifft, die allgemeinen Bestimmungen des bürgerlichen Rechts und

des Amtshaftungsgesetzes.

Zu § 34 des Entwurfs (Gemeinsame Bestimmungen):

Die Anwendungserfahrung, insbesondere vor der Datenschutzkommission, hat ergeben, daß die Statuierung von Verjährungsfristen **(Abs. 1)** für die Geltendmachung der Interessen der Betroffenen nach dem DSG sachlich geboten ist: Die Ermittlung von Sachverhalten, die lange zurückliegen, stößt erfahrungsgemäß auf erhebliche Schwierigkeiten und verhindert eine verläßliche Beurteilung des Vorliegens von Datenschutzverletzungen. Auch im eigenen Interesse sollten die Betroffenen daher dazu angehalten werden, behauptete Datenschutzverletzungen möglichst frühzeitig bei der Datenschutzkommission oder bei Gericht anhängig zu machen. Festzuhalten ist, daß diese besonderen Verjährungsfristen für Schadenersatzansprüche nach § 33 nicht gelten; diesbezüglich gelten die Verjährungsfristen des § 1489 ABGB, das sind drei bzw. 30 Jahre.

Gemäß § 3 des vorliegenden Entwurfes finden – in Umsetzung des Art. 4 der Richtlinie – in Österreich unter Umständen die Datenschutzregelungen eines anderen EU-Mitgliedstaates Anwendung. § 34 **Abs. 2** weist ausdrücklich darauf hin, daß auch die Verletzung ausländischen Datenschutzrechtes vor den in Österreich zuständigen Stellen anhängig gemacht werden kann, und zwar insbesondere auch im Rahmen der Kontrolltätigkeit der Datenschutzkommission nach § 30 des Entwurfs.

Durch die Statuierung der Verpflichtung zur Amtshilfe an ausländische Kontrollstellen **(Abs. 4)** – eine Verpflichtung, die in den Rechtsordnungen aller EU-Mitgliedstaaten vorzusehen ist – sollen die Vollziehungsprobleme, die sich aus der Anwendung ausländischen Rechts ergeben, verringert werden.

Zu § 35 des Entwurfs (Datenschutzkommission und Datenschutzrat):

Die Verfassungsbestimmung des Abs. 2 ist im Hinblick auf die Judikatur des VfGH (vgl. Erk. vom 1. Dezember 1993, VfSlg. 13.626) notwendig und sichert die Durchsetzbarkeit der von der Datenschutzkommission in Wahrnehmung ihrer Zuständigkeiten gesetzten Handlungen und Rechtsakte auch gegenüber den obersten Organen der Vollziehung.

Zu § 37 des Entwurfes (Weisungsfreiheit der Datenschutzkommission):

Eine Verfassungsbestimmung wird hier deshalb für notwendig erachtet, weil die Datenschutzkommission nicht nur mit Tätigkeiten der in Art. 20 Abs. 2 B-VG ausdrücklich genannten Art betraut ist: Neben der Zuständigkeit "zur Entscheidung" in oberster – und einziger – Instanz ist die Datenschutzkommission auch zu Kontrolltätigkeiten in erheblichem Ausmaß berufen (vgl. § 30). Die Weisungsfreiheit für solche Tätigkeiten ist in Art. 20 Abs. 2 nicht ausdrücklich statuiert, sodaß eine Absicherung der Weisungsfreiheit auch hinsichtlich dieser Tätigkeit der Datenschutzkommission durch Verfassungsbestimmung geboten ist.

Zu § 40 des Entwurfes (Wirkung von Bescheiden):

Hinsichtlich der bescheidmäßigen Erledigungen der Datenschutzkommission wird die generelle Möglichkeit, den Verwaltungsgerichtshof anzurufen, für die Parteien des Verfahrens durch ausdrückliche Anordnung geschaffen **(Abs. 2).** Keine Beschwerdemöglichkeit besteht allerdings bei Mandatsbescheiden nach **Abs. 1,** die der Vorstellung an die Datenschutzkommission unterliegen, da ein weiterer Rechtszug entbehrlich erscheint.

Was die Stellung der in Vollziehung der Gesetze tätigen Auftraggeber des öffentlichen Bereichs betrifft, haben sie mangels subjektiver Rechte in Verwaltungsverfahren an sich weder Parteistellung noch ein Beschwerderecht an den Verwaltungsgerichtshof (vgl. etwa sogar für den Fall der Formalpartei VwSlgNF 12.662 A). In jenen Konstellationen, in welchen jedoch im Datenschutzgesetz bei Auftraggebern des öffentlichen Bereichs die Eigenschaft als "belangte Behörde" nicht im Vordergrund steht, wie im Registrierungsverfahren und im Genehmigungsverfahren im internationalen Datenverkehr, schien es sachgerecht, auch den in Vollziehung der Gesetze tätigen Auftraggebern des öffentlichen Bereichs Parteistellung und, daran anknüpfend, das Beschwerderecht an den VwGH einzuräumen. Die Beschränkung des Beschwerderechtes an den VwGH auf diese Fälle ist insoweit systemkonform, als auch im Verfahren vor dem UVS in Beschwerden über faktische Amtshandlungen – das am ehesten mit dem Beschwerdeverfahren vor der DSK vergleichbar ist – kein Beschwerderecht der belangten Behörde an den VwGH besteht. Neben diesen rechtssystematischen Erwägungen spricht im übrigen auch das Faktum der bekannten Überlastung des VwGH gegen eine wesentliche Ausdehnung der Beschwerderechte an dieses Höchstgericht. Besondere gesetzliche Vorschriften über das Recht der Amtsbeschwerde, wie etwa § 91 SPG, sollen allerdings aufrecht bleiben.

Abs. 3 enthält eine sowohl im Hinblick auf § 68 AVG als auch im Hinblick auf den Vorrang des Gemeinschaftsrechts notwendige Regelung, nach der erteilte Genehmigungen im internationalen Datenverkehr widerrufen werden können, wenn die Voraussetzungen der Genehmigung tatsächlich weggefallen sind oder die Kommission der EU die Frage hinreichenden Schutzes bei einem konkreten Datentransfer ins Ausland nachträglich im Verfahren gemäß Art. 26 Abs. 3 Richtlinie anders beurteilt als die österreichische Datenschutzkommission.

In **Abs. 4** wird geltendes Recht – der bisherige § 37 Abs. 1 – wiederholt.

Zu § 46 des Entwurfs (Wissenschaftliche Forschung und Statistik):

Die Richtlinie 95/46/EG spricht an mehreren Stellen deutlich aus, daß eine besondere, privilegierende Stellung von wissenschaftlicher Forschung und Statistik bei der Verwendung personenbezogener Daten als sachlich gerechtfertigt angesehen wird. Dementsprechend enthält der vorliegende Entwurf erstmals eingehende datenschutzrechtliche Regelungen für diesen Bereich der Verwendung personenbezogener Daten.

Zunächst ist festzuhalten, daß § 46 nur gilt, soferne nicht spezielle gesetzliche Regelungen (wie etwa das Bundesstatistikgesetz) bestehen. (Diese müssen freilich verfassungskonform im Hinblick auf § 1 Abs. 2 sein.) Mangels solcher Regelungen gilt folgendes, wobei zwei grundsätzlich verschiedene Gebrauchssituationen zu unterscheiden sind:

– Daten werden erhoben für eine "Untersuchung", das ist ein konkretes Forschungsprojekt oder eine konkrete statistische Erhebung, bei der als Ergebnis Aussagen **in nicht personenbezogener Form** gewonnen werden sollen. Für diese Fälle sieht Abs. 1 eine privilegierte Verwendungsmöglichkeit bestimmter Daten vor (– dies betrifft insbesondere auch Daten, die beim selben Auftraggeber bereits für andere Zwecke vorhanden sind –).

– Für alle anderen Fälle gilt Abs. 2: Die "anderen Fälle" im Sinne dieser Bestimmung sind entweder Untersuchungen mit **personenbezogenen** Ergebnissen (zB Publikationen aus dem Wissenschaftsbereich der [zeitgenössischen] Geschichtsforschung) oder wissenschaftliche oder statistische Aktivitäten, die **keine konkrete Untersuchung** (Erhebung) darstellen (– das wäre zB die Führung von personenbezogenen Hilfsregistern für statistische Zwecke oder andere personenbezogene permanente Datensammlungen im Umfeld von Forschung und Statistik).

Was die Begriffe "wissenschaftliche Forschung" und "Statistik" betrifft, geht die vorliegende Regelung in Beachtung der Terminologie der Richtlinie 95/46/EG von folgendem Begriffsverständnis aus:

"Wissenschaftliche Forschung" soll nicht einen inhaltlich abgegrenzten Bereich bezeichnen – etwa in der Richtung, daß nur Grundlagenforschung erfaßt und angewandte Forschung ausgeschlossen wäre –, sondern als Bereich verstanden werden, in dem eine bestimmte Methode der Vorgangsweise, nämlich eine "wissenschaftliche", angewendet wird. Daß hiefür nicht der Ausdruck "Forschung" allein verwendet wird, ist in der Terminologie der Richtlinie begründet: Eine abweichende Begriffsbildung könnte zu Interpretationsschwierigkeiten führen.

Auch der Begriff **"Statistik"** wird dahingehend verstanden, daß es sich um methodologisch **"wissenschaftliche** Statistik" handelt, da nur unter dieser Voraussetzung eine Privilegierung sachlich zu rechtfertigen ist. Abgesehen davon soll aber dieser Begriff sowohl die sogenannte "amtliche Statistik" als auch sonstige (mit wissenschaftlichen Methoden durchgeführte) Statistik umfassen.

Zu § 47 des Entwurfs (Adreßdaten):

Diese Bestimmung wurde auf Grund der bisherigen Erfahrungen geschaffen, wonach sich ergeben hat, daß dieses Problem ohne ausdrückliche Regelung unlösbar ist. Wiederholt wurde das Bundeskanzleramt damit befaßt, daß bestimmte Betroffenenkreise aus Gründen, die durchaus im Interesse des Betroffenen oder sogar auch der Öffentlichkeit lagen, informiert oder befragt werden sollten, die Adreßdaten dieser Betroffenenkreise jedoch von jenen Stellen, die sie auf Grund anderer Datenanwendungen besitzen, nicht übermittelt werden durften, weil die Tatbestände des § 7 Abs. 2 und 3 jeweils nicht verwirklicht waren. Dasselbe gilt für jene Fälle, in welchen für Zwecke wissenschaftlicher Forschung die Adreßdaten von bestimmten Betroffenenkreisen benötigt werden, um mit ihnen in Kontakt treten zu können. Um in dieser Situation berechtigten Informationsinteressen gerecht zu werden, wird nunmehr einerseits in unbedenklichen Fällen die Verwendung von Daten gestattet, andrerseits in komplizierter gelagerten Fällen die Datenschutzkommission mit der Aufgabe betraut, im Einzelfall zu prüfen, ob eine konkrete Übermittlung von Adreßdaten eines bestimmten Betroffenenkreises die schutzwürdigen Geheimhaltungsinteressen dieser Betroffenen gefährden würde.

Festzuhalten ist, daß § 47 die Weitergabe von Adreßdaten für Marketingzwecke nicht betrifft. Für diesen Bereich ist § 268 GewO als gesetzliche Sonderbestimmung im Sinne des § 47 Abs. 1 anzuwenden.

Zu § 48 des Entwurfs (Publizistische Tätigkeit):

Die Informationsbeschaffung für Zwecke publizistischer Tätigkeit dient dem öffentlichen Informationsauftrag der Medien, worin einer der Grundpfeiler einer demokratischen Gesellschaftsordnung zu sehen ist (vgl. hiezu die ständige Judikatur des Europäischen Gerichtshofs für Menschenrechte, zB Observer und Guardian gg. VK, ÖJZ 1992/398 und Oberschlick gg Ö, ÖJZ 1997/956). Diese auf das Grundrecht auf freie Meinungsäußerung gestützte Datenverwendung hat daher einen besonderen Stellenwert gegenüber den Geheimhaltungsinteressen der Betroffenen. Freilich kann in einer Situation, in der einander gegenläufige Grundrechte gegenüberstehen, nicht davon ausgegangen werden, daß eines dieser Grundrechte Vorrang hat. Es muß vielmehr ein angemessener Interessensausgleich gesucht werden. Die Richtlinie 95/46/EG geht daher davon aus, daß Datenschutz auf "journalistische" Tätigkeit grundsätzlich Anwendung findet, allerdings mit

allen jenen Ausnahmen, die "sich als notwendig erweisen, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen" (Art. 9 RL). Die notwendigen Abweichungen dürfen vorgesehen werden

– im Bereich der "Bedingungen für die Rechtmäßigkeit" der Datenverwendung (Kapitel II der Richtlinie);

– hinsichtlich von Regelungen über die Übermittlung personenbezogener Daten in Drittländer (Kapitel IV der Richtlinie) sowie

– hinsichtlich des Kapitels VI der Richtlinie betreffend eine unabhängige datenschutzrechtliche Kontrollstelle und ihre Aufgaben.

Dementsprechend sieht § 48 vor, daß bei den **Zulässigkeitsvoraussetzungen** anstelle der §§ 7 bis 9 die Bestimmung des § 48 Abs. 2 tritt, wobei die besonderen Garantien des Mediengesetzes für den **Schutz der Rechtssphäre der Betroffenen** ausdrücklich aufrechterhalten werden (vgl. Abs. 3), sodaß die Umsetzung der Richtlinie in diesen Fragen durch das Mediengesetz erfolgt.

Terminologisch ist zu bemerken, daß die Richtlinie von "journalistischen Tätigkeiten" spricht, ohne hiefür eine Definition zu geben. Aus dem Zweck des Art. 9 Richtlinie muß nun gefolgert werden, daß unter "journalistischer Tätigkeit" nicht nur die tagesgenaue Berichterstattung der Presse oder sonstiger Medien zu verstehen ist, sondern auch Publikationen mit größerem Umfang (etwa Bücher) zu aktuellen, die Öffentlichkeit legitimerweise interessierenden Themen. Sachgerechter ist daher die Verwendung des Begriffes "publizistische Tätigkeit", wobei durch Verknüpfung mit bestimmten Berufsbildern (Medienmitarbeiter) bzw. Funktionen (Medienunternehmen, Mediendienste) eine Begriffsreduktion auf jenen Umfang erfolgt, der infolge des überragenden öffentlichen Interesses am Informationsauftrag der Medien gegenüber den datenschutzrechtlichen Geheimhaltungsinteressen zu privilegieren ist.

Zu § 49 (Automatisierte Einzelentscheidungen):

Diese Bestimmung folgt eng dem entsprechenden Text der Richtlinie. Automatisierte Entscheidungen im öffentlichen Bereich werden durch diese Bestimmung dann nicht verunmöglicht, wenn entsprechende – einfache – Rechtsschutzmöglichkeiten zur Verfügung stehen (vgl. Abs. 2 Z 3).

Für Bereiche, in denen Massenverfahren (Unzahl von gleichförmigen Erledigungen) insbesondere auch schon durch die Rechtsordnung der EU vorgezeichnet und unerläßlich sind (wie insbesondere im Bereich der hoheitlichen und privatwirtschaftsförmigen Agrarbeihilfeverfahren), soll diese Bestimmung eine ordnungsgemäße und zeitgerechte Durchführung der Verfahren nicht behindern: Sind Massenverfahren dem einschlägigen Bereich immanent, ist im hoheitlichen Bereich dem Erfordernis des Abs. 2 Z 1 schon durch den EU-rechtlichen und gesetzlichen Auftrag, diese Verfahren abzuwickeln, Genüge getan. Für den privatwirtschaftlichen Bereich ist bereits die allgemeine faktische Einräumung einer Möglichkeit des Betroffenen, seinen Standpunkt geltend zu machen, ausreichend im Sinne Abs. 2 Z 2, umsomehr als ihm darüber hinaus der Zivilrechtsweg für die Geltendmachung seiner Ansprüche offen steht.

Die in **Abs. 3** enthaltene Verpflichtung muß freilich vor dem Hintergrund der gesamten Rechtsordnung gesehen werden, dh. daß eine Verpflichtung zur Offenlegung der Entscheidungslogik nur soweit besteht, als hiedurch nicht in die Rechte anderer, insbesondere des Auftraggebers, unverhältnismäßig eingegriffen wird; letzteres wird dann anzunehmen sein, wenn zB Urheberrechte, Geschäftsgeheimnisse u. dgl. durch die Darlegung des logischen Ablaufs der Entscheidungsfindung gefährdet wären.

Zu § 50 (Informationsverbundsysteme):

Zum Zweck eines besseren Service für die Betroffenen (zB Flugbuchungssysteme), aber auch zum Zweck der genaueren Kenntnis der eine bestimmte Person betreffenden Lebensumstände haben manche Branchen aber auch die öffentliche Verwaltung (Verbrechensbekämpfung) Informationssysteme aufgebaut, bei welchen jeder Systemteilnehmer die ihm verfügbaren Informationen einspeichert und sie allen anderen Teilnehmern zur Verfügung stellt. Daß dieses Phänomen, das an sich dem Gedanken des Datenschutzes widerspricht, aus datenschutzrechtlicher Sicht äußerst relevant ist und auch extrem gefährdend sein kann, liegt auf der Hand, umsomehr als die rechtliche Zulässigkeit solcher Systeme nach der bisherigen Rechtslage in manchen Fällen nicht zweifelsfrei erscheint. Für Informationsverbundsysteme ist daher durch § 18 Abs. 2 Z 4 die Vorabkontrolle vorgesehen. Die Datenschutzkommission kann anläßlich der Registrierung auch besondere Auflagen für den Betrieb eines solchen Systems verfügen (§ 21 Abs. 2).

Der Umstand, daß dem Betroffenen bei einem Informationsverbundsystem eine Vielzahl von Auftraggebern gegenüber steht, ist für die Ausübung seiner Betroffenenrechte (5. Abschnitt des Entwurfes) nachteilig. Deshalb wird nunmehr die Bestellung eines "Betreibers" zwingend vorgeschrieben, der der erste Ansprechpartner des Betroffenen ist, falls ihm der konkrete Auftraggeber nicht bekannt ist (Art. 2 lit. d der Richtlinie eröffnet die Möglichkeit einer solchen vom Normalfall abweichenden Regelung).

Der Betreiber ist weiters für die Datensicherheit im System verantwortlich. Dies ist wesentlich, insbesondere für eine möglichst hohe Datenqualität bei jenen Informationsverbundsystemen, die eine Kontrollfunktion gegenüber den Betroffenen

bezwecken.

Das Innenverhältnis zwischen dem Betreiber und den Auftraggebern bleibt der vertraglichen Ausgestaltung überlassen; derartige Vereinbarungen können durch Eintragung im Datenverarbeitungsregister außenrelevant gemacht werden.

Zu § 51 des Entwurfs (Datenverwendung in Gewinnerzielungs- oder Schädigungsabsicht):

Die bisherige Rechtslage hat zwei gerichtlich strafbare Tatbestände vorgesehen, nämlich den "Geheimnisbruch" (§ 48 DSG) und den "unbefugten Eingriff im Datenverkehr" (§ 49 DSG).

Der Tatbestand des Geheimnisbruchs wurde als besonderes Berufsgeheimnis geschaffen für jene Personen, die "berufsmäßig mit Aufgaben der Datenverarbeitung beschäftigt" sind. Der Kreis dieser Personen war zum Zeitpunkt des Inkrafttretens des Datenschutzgesetzes im Jahr 1980 relativ eng beschränkt, sodaß die Schaffung und Sanktionierung eines besonderen Berufsgeheimnisses in der vorliegenden Form als sachgerecht angesehen werden konnte. Diese Voraussetzung liegt nicht mehr vor: Angesichts des Umstandes, daß die meisten beruflichen Tätigkeiten in der einen oder anderen Form mit der Benutzung von Datenendgeräten verbunden sind, wurde das Tatbestandselement der "berufsmäßigen Betrauung mit Aufgaben der Datenverarbeitung" heute einen Großteil aller Berufstätigen betreffen. Eine solche Ausweitung des potentiellen Täterkreises führt zu einem Kriminalisierungspotential, das ursprünglich nie beabsichtigt war. Hiezu kommt, daß der Tatbestand des § 48 insgesamt wenig spezifisch formuliert war, sodaß nahezu jede Indiskretion in Bezug auf personenbezogene Daten, die aus einer beruflichen Tätigkeit resultiert, gerichtlich strafbar gewesen wäre. Vor diesem Hintergrund scheint die Aufrechterhaltung der gerichtlichen Strafbarkeit, die ja besonders verwerflichen Handlungen vorbehalten bleiben soll, nicht gerechtfertigt. Es wurde deshalb in die Verwaltungsstrafbestimmungen des § 52 ein Tatbestand aufgenommen, der an die Verletzung des Datengeheimnisses (§ 15 des Entwurfes) anknüpft (nähere Ausführungen siehe unten).

Gerichtlich strafbar bleiben sollte jedoch die rechtswidrige Verwendung von Daten in besonders verwerflicher Absicht, nämlich in Gewinnerzielungs- oder Schädigungsabsicht. Um hiebei nicht in Konkurrenz mit anderen gerichtlichen Straftatbeständen zu gelangen (vgl. zB § 126a StGB), soll als Tathandlung die "Benützung sowie die Weitergabe von Daten, insbesonders ihre Veröffentlichung", unter Strafe gestellt werden. Die Deliktsverfolgung bedarf einer Ermächtigung durch den Verletzten.

Zu § 52 (Verwaltungsstrafbestimmung):

Die Richtlinie verlangt von der nationalen Rechtsordnung, daß sie entsprechende Sanktionen für die Ahndung von Verstößen vorsieht (Art. 24 Richtlinie). § 52 enthält daher einen gegenüber dem bisher geltenden § 50 DSG wesentlich erweiterten Katalog von Verwaltungsstraftatbeständen. Im Hinblick auf das Verletzungspotential der Straftatbestände wurde eine Abstufung des Strafrahmens eingeführt:

- **Abs. 1** enthält Tatbestände, in welchen eine Verletzung von Rechten tatsächlich stattgefunden hat;

- **Abs. 2** zählt Tatbestände auf, in welchen zwar noch keine Verletzung von Rechten des Betroffenen manifest ist, aber Unterlassungen begangen wurden, die eine Gefährdung der Rechte des Betroffenen oder zumindest eine Gefährdung der Durchsetzbarkeit dieser Rechte zur Folge hat.

Die Zurechnung der Verantwortlichkeit für Tathandlungen zu den einzelnen Organen (Mitarbeitern) eines Auftraggebers oder Dienstleisters ist durch § 9 VStG geregelt. Für Auftraggeber des öffentlichen Bereichs bedeutet dies, daß auch interne Organisationsvorschriften wie die Geschäftseinteilung oder Geschäftsordnung zur Beurteilung dieser Frage heranzuziehen sein werden.

Bisher waren die Landeshauptleute in erster Instanz als Strafbehörde zuständig. Vertreter der Länder haben demgegenüber ins Treffen geführt, daß auf Grund der derzeit vorherrschenden Zuständigkeitsverteilung den Ämtern der Landesregierungen nur mehr sehr wenige Verwaltungsstrafkompetenzen zukommen und daher kaum entsprechend ausgebildetes Personal zur Verfügung steht. Aus diesem Grunde wurde ersucht, die Verwaltungsstrafkompetenz erster Instanz den Bezirksverwaltungsbehörden zu überantworten, was mit der Formulierung des **Abs. 6** nunmehr geschieht.

Eine wesentliche Änderung gegenüber der bisherigen Rechtslage ist der Umstand, daß die Datenschutzkommission nicht mehr als Berufungsinstanz in Verwaltungsstrafverfahren zuständig ist. Dies deshalb, weil der Grundsatz des fairen Verfahrens es verbietet, daß die Datenschutzkommission einerseits Kontrollrechte ausübt (– und zwar in weit größerem Umfang als dies nach der bisherigen Rechtslage der Fall war –) und im Rahmen dieser Kontrollbefugnisse allenfalls auch Anzeige an die zuständige Strafbehörde erster Instanz erstattet und andererseits als Berufungsinstanz zur Entscheidung über diese Anzeige berufen wäre (vgl. im übrigen auch das Urteil des EGMR im Fall Bönisch gg. Ö., EuGRZ 1986/127).

Zu § 53 des Entwurfs (Befreiung von Gebühren, Verwaltungsabgaben und vom Kostenersatz):

Abweichend von der bisherigen Rechtslage ist in Aussicht genommen, keine eigene

Registrierungsgebühr vorzusehen. Dies deshalb, weil zum einen die Einhebung dieser Gebühr größeren Administrativaufwand verursacht, dem keine bedeutenden Einnahmen gegenüberstehen und weil zum anderen eine solche Gebühr der Zielrichtung eines Datenverarbeitungsregisters entgegenwirkt, da sie sich negativ auf die Bereitschaft zur Abgabe einer Meldung an das Register auswirkt. Hinzu kommt, daß sich infolge der vorgeschlagenen Registrierungsfreiheit für Standardverarbeitungen die Einnahmen aus dieser Gebühr zusätzlich verringern werden, sodaß ihr Entfall noch weniger budgetrelevant ist.

Zu den §§ 54 und 55 des Entwurfs (Informationsaustausch mit den anderen EU-Mitgliedstaaten und der Europäischen Kommission):

Die Bestimmungen der §§ 54 und 55 sind in unmittelbarer Umsetzung der Richtlinie 95/46/EG notwendig. Sie dienen einer gleichmäßigen Entscheidungspraxis in den Fällen des Datenverkehrs mit Drittstaaten durch die Behörden aller EU-Mitgliedstaaten.